
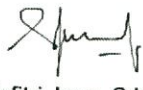





RENCANA PEMBELAJARAN SEMESTER

PROGRAM STUDI INFORMATIKA

IFA212

Issue/Revisi	: R0	Tanggal	: 25 Januari 2021
Mata Kuliah	: Pengantar Keamanan Siber	Kode MK	: IFA212
Rumpun MK	: MKMA	Semester	: 4
Dosen Pengampu	: Hendi Hermawan, S.T., M.T.I.	Bobot (sks)	: 2 sks
Dosen Pengampu	Kaprodi	Dekan	
 Hendi Hermawan, S.T., M.T.I.	 Safitri Jaya, S.Kom, M.T.I.	 Agustinus Agus Setiawan, S.T., M.T.	

RENCANA PEMBELAJARAN SEMESTER	
Capaian Pembelajaran (CP)	CPL - PRODI
	1 Mampu menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan atau implementasi ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora yang sesuai dengan bidang keahliannya.
	2 Mampu mengambil keputusan secara tepat dalam konteks penyelesaian masalah di bidang keahliannya, berdasarkan hasil analisis informasi dan data.
	3 Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri.
	4 Menguasai pengetahuan mengenai jaringan komputer secara umum maupun jaringan komputer beserta mekanisme protokol komunikasinya.
	CP-MK
1 Mampu memahami dasar-dasar agar dapat online secara aman.	
2 Mampu memahami berbagai jenis malware dan serangannya, dan bagaimana organisasi melindungi diri terhadap serangan ini.	
3 Mampu mengeksplorasi pilihan berkarir di bidang keamanan siber.	
4 Mampu menjelaskan prinsip-prinsip confidentiality, integrity, dan availability yang terkait dengan status data dan penanggulangan keamanan siber.	

RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

RENCANA PEMBELAJARAN SEMESTER	
	<p>5 Mampu menjelaskan taktik, Teknik, dan prosedur yang digunakan oleh penjahat siber.</p> <p>6 Mampu menjelaskan bagaimana teknologi, produk, dan prosedur dapat digunakan untuk melindungi kerahasiaan / confidentiality, integritas / integrity, dan memberikan ketersediaan tinggi / high availability.</p> <p>7 Mampu menjelaskan bagaimana para professional keamanan siber menggunakan teknologi, proses, dan prosedur untuk mempertahankan semua komponen jaringan.</p> <p>8 Mampu menjelaskan tujuan hukum yang terkait dengan keamanan siber.</p>
Deskripsi Singkat MK	Mata kuliah ini dirancang agar mahasiswa dapat mempertimbangkan berkarir dengan spesialisasi keamanan siber. Kuliah ini akan mengeksplorasi cara-cara agar dapat online secara aman, mempelajari berbagai jenis malware dan serangannya, mengeksplorasi karakteristik dan taktik yang digunakan oleh penjahat siber, langkah-langkah yang digunakan oleh organisasi untuk mengurangi serangan, dan meneliti peluang karir dibidang keamanan Siber.
Materi Pembelajaran/Pokok Bahasan	<p>The Need for Cybersecurity</p> <p>Attacks, Concepts and Techniques</p> <p>Protecting Your Data and Privacy</p> <p>Protecting the Organization</p> <p>Will Your Future be in Cybersecurity?</p> <p>Cybersecurity: A World of Wizard The Cybersecurity Sorcery Cube dry, Criminals, and Heroes</p> <p>Cybersecurity Threats, Vulnerabilities and Attacks</p> <p>The Art of Protecting Secrets</p> <p>The Art of Ensuring Integrity</p> <p>The Realm of Five Nines</p> <p>Fortifying the Kingdom</p> <p>Joining the Order of Cyber Hero's</p>
Pustaka	Utama
	<p>Modul Introduction to Cybersecurity v2.1, Cisco Academy</p> <p>Modul Cybersecurity Essentials 1.0, Cisco Academy</p>
	Pendukung
Media Pembelajaran	Perangkat Lunak:
	<p>Cisco Packet Tracer, Windows, Linux, Android</p>
	Perangkat Keras:
	<p>LCD Projector, Komputer, Router & Switch Cisco, Smartphone</p>
Team Teaching	-
Mata Kuliah Prasyarat	-



RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

RENCANA PEMBELAJARAN SEMESTER		
Indikator, Kriteria dan Bobot Penilaian	Tugas/Kuis	: 20%
	Praktek / Latihan	: 20%
	UTS	: 30%
	UAS / Final Project	: 30%



RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER						
Minggu ke- (1)	Sub CP-MK (Kemampuan Akhir yang Diharapkan) (2)	Indikator (3)	Kriteria & Bentuk Penilaian (4)	Metode Pembelajaran (Estimasi Waktu) (5)	Materi Pembelajaran (Pustaka) (6)	Bobot Penilaian (%) (7)
1	<ol style="list-style-type: none"> Mampu mendefinisikan karakteristik dan nilai data-data pribadi. Mampu menjelaskan mengapa data pribadi dapat menguntungkan bagi para peretas. Mampu menjelaskan jenis data yang digunakan oleh pemerintah dan organisasi. Mampu menjelaskan dampak pelanggaran keamanan. Mampu menjelaskan karakteristik dan motivasi penyerangan siber serta masalah hukum dan etika sebagai tenaga profesional keamanan siber. Mampu menjelaskan karakteristik dan tujuan perang siber. 	<ul style="list-style-type: none"> Ketepatan dalam mendefinisikan karakteristik dan nilai data-data pribadi. Ketepatan dalam menjelaskan mengapa data pribadi dapat menguntungkan bagi para peretas. Ketepatan dalam menjelaskan jenis data yang digunakan oleh pemerintah dan organisasi. Ketepatan dalam menjelaskan dampak pelanggaran keamanan. Ketepatan dalam menjelaskan karakteristik dan motivasi penyerangan siber serta masalah hukum dan etika sebagai tenaga 	<p>Kriteria: Ketepatan dan Penguasaan</p> <p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> Diskusi Test dan Evaluasi 	<p>Kuliah : TM : 1 x 50' BM : 1 x 60' BS : 1 x 60'</p> <p>Praktikum : TM : 1 x 100' BM : 1 x 70'</p>	The Need for Cybersecurity	2,86% (1,43% logbook, 1,43% praktek)



Universitas
Pembangunan Jaya

RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER						
Minggu ke- (1)	Sub CP-MK (Kemampuan Akhir yang Diharapkan) (2)	Indikator (3)	Kriteria & Bentuk Penilaian (4)	Metode Pembelajaran (Estimasi Waktu) (5)	Materi Pembelajaran (Pustaka) (6)	Bobot Penilaian (%) (7)
2	<ol style="list-style-type: none"> 1. Mampu menjelaskan cara eksploitasi kerentanan keamanan. 2. Mampu mengidentifikasi contoh kerentanan keamanan. 3. Mampu menjelaskan jenis malware dan gejalanya. 4. Mampu menjelaskan metode infiltrasi. 5. Mampu menjelaskan metode yang digunakan untuk memboikot layanan. 6. Mampu menjelaskan serangan kombinasi. 7. Mampu menjelaskan pentingnya pengurangan dampak. 	<p>profesional keamanan siber.</p> <ul style="list-style-type: none"> • Ketepatan dalam menjelaskan karakteristik dan tujuan perang siber. • Ketepatan dalam menjelaskan cara eksploitasi kerentanan keamanan. • Ketepatan dalam mengidentifikasi contoh kerentanan keamanan. • Ketepatan dalam menjelaskan jenis malware dan gejalanya. • Ketepatan dalam menjelaskan metode infiltrasi. • Ketepatan dalam menjelaskan metode yang digunakan untuk memboikot layanan. • Ketepatan dalam menjelaskan serangan kombinasi. • Ketepatan dalam menjelaskan 	<p>Kriteria: Ketepatan dan Penguasaan</p> <p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> • Diskusi • Test dan Evaluasi 	<p>Kuliah : TM : 1 x 50' BM : 1 x 60' BS : 1 x 60'</p> <p>Praktikum : TM : 1 x 100' BM : 1 x 70'</p>	<p>Attacks, Concepts and Techniques</p>	<p>2,86% (1,43% logbook, 1,43% praktek)</p>



RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER						
Minggu ke- (1)	Sub CP-MK (Kemampuan Akhir yang Diharapkan) (2)	Indikator (3)	Kriteria & Bentuk Penilaian (4)	Metode Pembelajaran (Estimasi Waktu) (5)	Materi Pembelajaran (Pustaka) (6)	Bobot Penilaian (%) (7)
3	<ol style="list-style-type: none"> Mampu mengaktifkan dan memperbaharui firewall. Mampu menggunakan antivirus dan antispyware. Mampu mengelola system operasi dan browser. Mampu melindungi semua perangkat. 	<p>pentingnya pengurangan dampak.</p> <ul style="list-style-type: none"> Ketepatan dalam mengaktifkan dan memperbaharui firewall. Ketepatan dalam menggunakan antivirus dan antispyware. Ketepatan dalam mengelola system operasi dan browser. Ketepatan dalam melindungi semua perangkat. 	<p>Kriteria: Ketepatan dan Penguasaan</p> <p>Bentuk Penilaian: <ul style="list-style-type: none"> Diskusi Test dan Evaluasi </p>	<p><u>Kuliah</u> : TM : 1 x 50' BM : 1 x 60' BS : 1 x 60'</p> <p><u>Praktikum</u> : TM : 1 x 100' BM : 1 x 70'</p>	Protecting Your Data and Privacy	2,86% (1,43% logbook, 1,43% praktek)
4	<ol style="list-style-type: none"> Mampu mengidentifikasi fungsi CSIRT dalam Cisco. Mampu menjelaskan tujuan buku panduan keamanan. Mampu mengidentifikasi alat bantu yang digunakan untuk pencegahan dan deteksi insiden. Mampu mendefinisikan IDS dan IPS. 	<ul style="list-style-type: none"> Ketepatan dalam mengidentifikasi fungsi CSIRT dalam Cisco. Ketepatan dalam menjelaskan tujuan buku panduan keamanan. Ketepatan dalam mengidentifikasi alat bantu yang digunakan untuk pencegahan dan deteksi insiden. 	<p>Kriteria: Ketepatan dan Penguasaan</p> <p>Bentuk Penilaian: <ul style="list-style-type: none"> Diskusi Test dan Evaluasi </p>	<p><u>Kuliah</u> : TM : 1 x 50' BM : 1 x 60' BS : 1 x 60'</p> <p><u>Praktikum</u> : TM : 1 x 100' BM : 1 x 70'</p>	Protecting the Organization	2,86% (1,43% logbook, 1,43% praktek)



RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

Minggu ke- (1)	Sub CP-MK (Kemampuan Akhir yang Diharapkan) (2)	Indikator (3)	Kriteria & Bentuk Penilaian (4)	Metode Pembelajaran (Estimasi Waktu) (5)	Materi Pembelajaran (Pustaka) (6)	Bobot Penilaian (%) (7)
5	<ol style="list-style-type: none"> Mampu menjelaskan masalah hukum dalam bidang keamanan siber. Mampu menjelaskan etika-etika dalam keamanan siber. Mampu menjelaskan etika yang dihadapi tenaga profesional keamanan siber. 	<ul style="list-style-type: none"> Ketepatan dalam mendefinisikan IDS dan IPS. Ketepatan dalam menjelaskan masalah hukum dalam bidang keamanan siber. Ketepatan dalam menjelaskan etika-etika dalam keamanan siber. Ketepatan dalam menjelaskan etika yang dihadapi tenaga profesional keamanan siber. 	<p>Kreteria: Ketepatan</p> <p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> Diskusi Test dan Evaluasi 	<p><u>Kuliah</u> :</p> <p>TM : 1 x 50' BM : 1 x 60' BS : 1 x 60'</p> <p><u>Praktikum</u> :</p> <p>TM : 1 x 100' BM : 1 x 70'</p>	<p>Will Your Future be in Cybersecurity?</p>	<p>2,86% (1,43% logbook, 1,43% praktek)</p>
6	<ol style="list-style-type: none"> Mampu menjelaskan karakteristik umum yang terdiri dari dunia keamanan siber Mampu membedakan karakteristik kejahatan cyber dan profesional Mampu membandingkan bagaimana ancaman keamanan siber memengaruhi individu, bisnis, dan organisasi. Mampu menjelaskan faktor-faktor yang 	<ul style="list-style-type: none"> Ketepatan dalam menjelaskan karakteristik umum yang terdiri dari dunia keamanan siber. Ketepatan dalam membedakan karakteristik kejahatan cyber dan profesional. Ketepatan dalam membandingkan bagaimana ancaman keamanan siber memengaruhi individu, bisnis, dan organisasi. 	<p>Kreteria: Ketepatan</p> <p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> Diskusi Test dan Evaluasi 	<p><u>Kuliah</u> :</p> <p>TM : 1 x 50' BM : 1 x 60' BS : 1 x 60'</p> <p><u>Praktikum</u> :</p> <p>TM : 1 x 100' BM : 1 x 70'</p>	<p>Cybersecurity: A World of Wizardry, Criminals, and Heroes</p>	<p>2,86% (1,43% logbook, 1,43% praktek)</p>



Universitas
Pembangunan Jaya

RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER						
Minggu ke- (1)	Sub CP-MK (Kemampuan Akhir yang Diharapkan) (2)	Indikator (3)	Kriteria & Bentuk Penilaian (4)	Metode Pembelajaran (Estimasi Waktu) (5)	Materi Pembelajaran (Pustaka) (6)	Bobot Penilaian (%) (7)
7	<p>menyebabkan penyebaran dan pertumbuhan kejahatan dunia maya.</p> <p>5. Mampu menjelaskan organisasi dan upaya yang dilakukan untuk memperluas tenaga kerja keamanan siber.</p> <p>1. Mampu menjelaskan bagaimana prinsip kerahasiaan, integritas, dan ketersediaan terkait dengan status data dan penanggulangan keamanan siber.</p> <p>2. Mampu menjelaskan tiga dimensi McCumber Cube.</p> <p>3. Mampu menjelaskan prinsip kerahasiaan, integritas, dan ketersediaan.</p> <p>4. Mampu membedakan tiga status data.</p>	<ul style="list-style-type: none"> • Ketepatan dalam menjelaskan faktor-faktor yang menyebabkan penyebaran dan pertumbuhan kejahatan dunia maya. • Ketepatan dalam menjelaskan organisasi dan upaya yang dilakukan untuk memperluas tenaga kerja keamanan siber. • Ketepatan dalam menjelaskan bagaimana prinsip kerahasiaan, integritas, dan ketersediaan terkait dengan status data dan penanggulangan keamanan siber. • Ketepatan dalam menjelaskan tiga dimensi McCumber Cube. • Ketepatan dalam menjelaskan prinsip kerahasiaan, integritas, dan ketersediaan. 	<p>Kriteria: Ketepatan</p> <p>Bentuk Penilaian: • Diskusi • Test dan Evaluasi</p>	<p><u>Kuliah</u> : TM : 1 x 50' BM : 1 x 60' BS : 1 x 60'</p> <p><u>Praktikum</u> : TM : 1 x 100' BM : 1 x 70'</p>	The Cybersecurity Sorcery Cube	2,86% (1,43% logbook, 1,43% praktek)



RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER						
Minggu ke- (1)	Sub CP-IMK (Kemampuan Akhir yang Diharapkan) (2)	Indikator (3)	Kriteria & Bentuk Penilaian (4)	Metode Pembelajaran (Estimasi Waktu) (5)	Materi Pembelajaran (Pustaka) (6)	Bobot Penilaian (%) (7)
	2. Mampu menjelaskan bagaimana teknik enkripsi melindungi kerahasiaan.	<ul style="list-style-type: none"> melindungi kerahasiaan. Ketepatan dalam menjelaskan bagaimana teknik enkripsi melindungi kerahasiaan. 	<ul style="list-style-type: none"> Diskusi Test dan Evaluasi 	Praktikum : TM : 1 x 100' BM : 1 x 70'		
	3. Mampu menjelaskan bagaimana teknik kontrol akses melindungi kerahasiaan.	<ul style="list-style-type: none"> Ketepatan dalam menjelaskan bagaimana teknik kontrol akses melindungi kerahasiaan. 				
	4. Mampu menjelaskan konsep mengaburkan data.	<ul style="list-style-type: none"> Ketepatan dalam menjelaskan bagaimana teknik kontrol akses melindungi kerahasiaan. Ketepatan dalam menjelaskan konsep mengaburkan data. 				
11	1. Mampu menjelaskan bagaimana teknologi, produk, dan prosedur digunakan untuk memastikan integritas.	<ul style="list-style-type: none"> Ketepatan dalam menjelaskan bagaimana teknologi, produk, dan prosedur digunakan untuk memastikan integritas. 	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: <ul style="list-style-type: none"> Diskusi Test dan Evaluasi 	Kuliah : TM : 1 x 50' BM : 1 x 60' BS : 1 x 60' Praktikum : TM : 1 x 100' BM : 1 x 70'	The Art of Ensuring Integrity	2,86% (1,43% logbook, 1,43% praktek)



Universitas
Pembangunan Jaya

RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER						
Minggu ke- (1)	Sub CP-MK (Kemampuan Akhir yang Diharapkan) (2)	Indikator (3)	Kriteria & Bentuk Penilaian (4)	Metode Pembelajaran (Estimasi Waktu) (5)	Materi Pembelajaran (Pustaka) (6)	Bobot Penilaian (%) (7)
12	<p>5. Mampu menjelaskan perlunya integritas database.</p> <p>1. Mampu menjelaskan bagaimana teknologi, produk, dan prosedur memberikan ketersediaan tinggi.</p> <p>2. Mampu menjelaskan konsep ketersediaan tinggi.</p> <p>3. Mampu menjelaskan bagaimana ukuran ketersediaan tinggi digunakan untuk meningkatkan ketersediaan.</p> <p>4. Mampu menjelaskan bagaimana rencana respons insiden meningkatkan ketersediaan tinggi.</p> <p>5. Mampu menjelaskan bagaimana perencanaan pemulihan bencana memainkan peran penting dalam</p>	<ul style="list-style-type: none"> • Ketepatan dalam menjelaskan tujuan sertifikat digital. • Ketepatan dalam menjelaskan perlunya integritas database. • Ketepatan dalam menjelaskan bagaimana teknologi, produk, dan prosedur memberikan ketersediaan tinggi. • Ketepatan dalam menjelaskan konsep ketersediaan tinggi. • Ketepatan dalam menjelaskan bagaimana ukuran ketersediaan tinggi digunakan untuk meningkatkan ketersediaan. • Ketepatan dalam menjelaskan bagaimana rencana respons insiden meningkatkan ketersediaan tinggi. • Ketepatan dalam menjelaskan 	<p>Kriteria: Ketepatan dan Penguasaan</p> <p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> • Diskusi • Test dan Evaluasi 	<p><u>Kuliah</u> : TM : 1 x 50' BM : 1 x 60' BS : 1 x 60'</p> <p><u>Praktikum</u> : TM : 1 x 100' BM : 1 x 70'</p>	The Realm of Five Nines	2,86% (1,43% logbook, 1,43% praktek)



RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER						
Minggu ke- (1)	Sub CP_MK (Kemampuan Akhir yang Diharapkan) (2)	Indikator (3)	Kriteria & Bentuk Penilaian (4)	Metode Pembelajaran (Estimasi Waktu) (5)	Materi Pembelajaran (Pustaka) (6)	Bobot Penilaian (%) (7)
13	<p>menerapkan ketersediaan tinggi.</p> <ol style="list-style-type: none"> Mampu menjelaskan bagaimana para profesional keamanan siber menggunakan teknologi, proses dan prosedur untuk mempertahankan semua komponen jaringan. Mampu menjelaskan bagaimana proses dan prosedur melindungi sistem. Mampu menjelaskan cara melindungi server di jaringan. Mampu menjelaskan bagaimana menerapkan langkah-langkah keamanan untuk melindungi perangkat jaringan. Mampu menjelaskan bagaimana langkah- 	<p>bagaimana perencanaan pemulihan bencana memainkan peran penting dalam menerapkan ketersediaan tinggi.</p> <ul style="list-style-type: none"> Ketepatan dalam menjelaskan bagaimana para profesional keamanan siber menggunakan teknologi, proses dan prosedur untuk mempertahankan semua komponen jaringan. Ketepatan dalam menjelaskan bagaimana proses dan prosedur melindungi sistem. Ketepatan dalam menjelaskan cara melindungi server di jaringan. Ketepatan dalam menjelaskan bagaimana menerapkan langkah-langkah keamanan 	<p>Kriteria: Ketepatan dan Penguasaan</p> <p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> Diskusi Test dan Evaluasi 	<p><u>Kuliah</u> : TM : 1 x 50' BM : 1 x 60' BS : 1 x 60'</p> <p><u>Praktikum</u> : TM : 1 x 100' BM : 1 x 70'</p>	Fortifying the Kingdom	2,86% (1,43% logbook, 1,43% praktek)



RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER							
Minggu ke- (1)	Sub CP-MK (Kemampuan Akhir yang Diharapkan) (2)	Indikator (3)	Kriteria & Bentuk Penilaian (4)	Metode Pembelajaran (Estimasi Waktu) (5)	Materi Pembelajaran (Pustaka) (6)	Bobot Penilaian (%) (7)	
	langkah keamanan fisik diterapkan untuk melindungi peralatan jaringan.	<ul style="list-style-type: none"> untuk melindungi perangkat jaringan. Ketepatan dalam menjelaskan bagaimana langkah-langkah keamanan fisik diterapkan untuk melindungi peralatan jaringan. 					
14	<ol style="list-style-type: none"> Mampu menjelaskan tujuan hukum yang terkait dengan keamanan siber. Mampu menjelaskan bagaimana domain keamanan siber digunakan dalam triad CIA. Mampu menjelaskan bagaimana etika memberikan panduan. Mampu menjelaskan cara mengambil langkah selanjutnya untuk menjadi profesional keamanan siber. 	<ul style="list-style-type: none"> Ketepatan dalam menjelaskan tujuan hukum yang terkait dengan keamanan siber. Ketepatan dalam menjelaskan bagaimana domain keamanan siber digunakan dalam triad CIA. Ketepatan dalam menjelaskan bagaimana etika memberikan panduan. Ketepatan dalam menjelaskan cara mengambil langkah selanjutnya untuk menjadi profesional keamanan siber. 	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: <ul style="list-style-type: none"> Diskusi Test dan Evaluasi 	Kuliah : TM : 1 x 50' BM : 1 x 60' BS : 1 x 60' <u>Praktikum</u> : TM : 1 x 100' BM : 1 x 70'	Joining the Order of Cyber Hero's	2,86% (1,43% logbook, 1,43% praktek)	



Universitas
Pembangunan Jaya

RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER						
Minggu ke- (1)	Sub CP-MK (Kemampuan Akhir yang Diharapkan) (2)	Indikator (3)	Kriteria & Bentuk Penilaian (4)	Metode Pembelajaran (Estimasi Waktu) (5)	Materi Pembelajaran (Pustaka) (6)	Bobot Penilaian (%) (7)
15	<ol style="list-style-type: none"> Mampu memahami permasalahan yang terdapat pada studi kasus. Mampu memecahkan masalah yang terdapat pada studi kasus. Mampu mempresentasikan solusi dari permasalahan yang telah dirumuskan. 	<ul style="list-style-type: none"> Ketepatan dalam memahami permasalahan yang terdapat pada studi kasus. Ketepatan dalam memecahkan masalah yang terdapat pada studi kasus. Ketepatan dalam mempresentasikan permasalahan yang telah dirumuskan. 	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: <ul style="list-style-type: none"> Diskusi Test dan Evaluasi 	Belajar Mandiri [BM: 1x (3x60")] Kuliah dan Diskusi [TM: 1x (1x50")] Presentasi BT: 1x(1x50") Tugas BM: 1x(3x60")		7,1
16	Evaluasi Akhir Semester: Melakukan validasi penilaian akhir dan menentukan kelulusan mahasiswa					

Catatan:

(1) TM: Tatap Muka, BT: Belajar Terstruktur, BM: Belajar Mandiri;



RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

RANCANGAN TUGAS MAHASISWA					
Mata Kuliah	Pengantar Keamanan Siber				
Kode MK	IFA212	sks:	3	Semester:	4
Dosen Pengampu	Hendi Hermawan, S.T., M.T.I.				
BENTUK TUGAS					
Final Project / UAS					
JUDUL TUGAS					
Final Project: Studi Kasus Permasalahan Keamanan Siber					
SUB CAPAIAN PEMBELAJARAN MATA KULIAH					
Memecahkan permasalahan dan memberikan solusi terkait dari keamanan siber yang sedang berkembang dimasyarakat					
DESKRIPSI TUGAS					
Final Project ini merupakan sebuah project yang mewajibkan mahasiswa untuk mencari permasalahan keamanan siber yang sedang berkembang dimasyarakat dimana dapat permasalahan tersebut dapat merugikan masyarakat baik secara pribadi maupun bagi masyarakat sekitar. Masalah yang didapat oleh mahasiswa perlu dicarikan solusinya agar dapat meminimalisir bahkan meniadakan kerugian yang ditimbulkannya.					
METODE Pengerjaan Tugas					
<ol style="list-style-type: none"> 1. Melakukan observasi terhadap permasalahan keamanan siber yang sedang berkembang dimasyarakat. 2. Melakukan analisis dari permasalahan yang diangkat untuk dicarikan solusinya. 3. Solusi yang didapat didokumentasikan dengan baik. 4. Hasil dokumentasi, dipresentasikan didepan kelas. 					
BENTUK DAN FORMAT LUARAN					
<ol style="list-style-type: none"> a. Obyek Garapan: Studi Kasus Permasalahan Keamanan Siber b. Bentuk luaran: <ol style="list-style-type: none"> 1. Dokumentasi solusi dari permasalahan yang diangkat. 					
INDIKATOR, KRITERIA DAN BOBOT PENILAIAN					
<ol style="list-style-type: none"> a. Dokumentasi (bobot 20%) b. Analisis Permasalahan (bobot 30%) c. Solusi yang ditawarkan (bobot 30%) d. Presentasi (bobot 20%) 					
JADWAL PELAKSANAAN					

RENCANA PEMBELAJARAN SEMESTER PROGRAM STUDI INFORMATIKA

RANCANGAN TUGAS MAHASISWA

Dokumentasi hasil observasi dan analisis permasalahan yang diangkat	Sebelum UTS
Dokumentasi solusi yang ditawarkan untuk memecahkan permasalahan yang diangkat	Setelah UTS
LAIN-LAIN	
-	
DAFTAR RUJUKAN	
Modul Introduction to Cybersecurity v2.1, Cisco Academy	
Modul Cybersecurity Essentials 1.0, Cisco Academy	

Jenjang/Grade	Angka/Skor	Angka Mutu	Deskripsi/Indikator Kerja
A (Sangat Baik)	A : 90.0 – 100	4	Mahasiswa terlibat sepenuhnya dalam diskusi, bermotivasi tinggi, melakukan persiapan dengan membaca materi sebelumnya, mengajukan gagasan dan pertanyaan substantif serta kritis, juga mendengarkan dan merespon secara terbuka terhadap kontribusi mahasiswa lain seraya memperlakukan sesama dengan setara dan adil
	A- : 80.00 – 89.99	3.7	
B (Baik)	B+ : 75.00 – 79.99	3.3	Mahasiswa terlibat sepenuhnya dalam diskusi, mengajukan gagasan dan pertanyaan substantif serta kritis, juga mendengarkan dan merespon secara terbuka terhadap kontribusi mahasiswa lain
	B : 70.00 – 74.99	3.0	
	B - : 65.00 – 69.99	2.7	
C (Cukup)	C+ : 60.00 - 64.99	2.3	Mahasiswa mengajukan gagasan dan pertanyaan, mendengarkan dan merespon secara terbuka terhadap kontribusi mahasiswa lain
	C : 55.00 – 59.99	2.0	
D (Kurang)	C- : 50.00 – 54.99	1.7	Mahasiswa tidak mengajukan gagasan dan pertanyaan, hanya mendengarkan dan tidak merespon secara terbuka terhadap kontribusi mahasiswa lain
	D : 40.00 – 49.99	1	
E (Sangat Kurang / Tidak Lulus)	<40.00	0	Mahasiswa tidak memenuhi kaidah – kaidah yang ditetapkan di atas