

# RENCANA PEMBELAJARAN SEMESTER (RPS) Keamanan Siber

ANDRY FAJAR ZULKARNAIN, S.ST., M. T

PROGRAM STUDI TEKNOLOGI INFORMASI

FAKULTAS TEKNIK UNIVERSITAS LAMBUNG MANGKURAT

# I. Capaian Pembelajaran Lulusan (CPL), Capaian Pembelajaran Mata Kuliah (CPMK), Sub-CPMK

## A. Capaian Pembelajaran Lulusan Prodi Sarjana Teknologi Informasi:

Sikap	
S1	Bertakwa kepada Tuhan Yang Maha Esa dan mampu menunjukkan sikap religius;
S2	Menjunjung tinggi nilai kemanusiaan dalam menjalankan tugas berdasarkan agama, moral, dan etika;
S3	Berkontribusi dalam peningkatan mutu kehidupan bermasyarakat, berbangsa, bernegara, dan kemajuan peradaban berdasarkan Pancasila;
S4	Berperan sebagai warga negara yang bangga dan cinta tanah air, memiliki nasionalisme serta rasa tanggung jawab pada negara dan bangsa;
S5	Menghargai keanekaragaman budaya, pandangan, agama, dan kepercayaan, serta pendapat atau temuan orisinal orang lain;
S6	Bekerja sama dan memiliki kepekaan sosial serta kepedulian terhadap masyarakat dan lingkungan;
S7	Taat hukum dan disiplin dalam kehidupan bermasyarakat dan bernegara;
S8	Menginternalisasi nilai, norma, dan etika akademik;
S9	Menunjukkan sikap bertanggung jawab atas pekerjaan di bidang keahliannya secara mandiri;
S10	Menginternalisasi semangat kemandirian, kejuangan, dan kewirausahaan;
S11	Memanifestasikan nilai kejiwaan WASAKA terhadap masyarakat dan lingkungannya secara berkelanjutan
Ketrampilan Umum	
U1	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;
U2	Mampu menunjukkan kinerja mandiri, bermutu, dan terukur;
U3	Mampu mengkaji implikasi pengembangan atau implementasi ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora sesuai dengan keahliannya berdasarkan kaidah, tata cara dan etika ilmiah dalam rangka menghasilkan solusi, gagasan, desain atau kritik seni;
U4	Mampu menyusun deskripsi saintifik hasil kajian tersebut di atas dalam bentuk skripsi atau laporan tugas akhir, dan mengunggahnya dalam laman perguruan tinggi;
U5	Mampu mengambil keputusan secara tepat dalam konteks penyelesaian masalah di bidang keahliannya, berdasarkan hasil analisis informasi dan data;
U6	Mampu memelihara dan mengembangkan jaringan kerja dengan pembimbing, kolega, sejawat baik di dalam maupun di luar lembaganya;
U7	

U8	Mampu bertanggung jawab atas pencapaian hasil kerja kelompok dan melakukan supervisi serta evaluasi terhadap penyelesaian pekerjaan yang ditugaskan kepada pekerja yang berada di bawah tanggung jawabnya;
U9	Mampu melakukan proses evaluasi diri terhadap kelompok kerja yang berada di bawah tanggung jawabnya, dan mampu mengelola pembelajaran secara mandiri; Mampu mendokumentasikan, menyimpan, mengamankan, dan menemukan kembali data untuk menjamin kesahihan dan mencegah plagiasi;
<b>Ketrampilan Khusus</b>	
K1	Menerapkan prinsip komputasi dan disiplin ilmu yang relevan dalam menganalisa masalah komputasi yang kompleks untuk mengidentifikasi solusi berbasis teknologi informasi
K2	Mengidentifikasi kebutuhan pengguna dalam merancang, menerapkan dan mengevaluasi solusi berbasis teknologi informasi secara tepat dan akurat
K3	Menerapkan konsep dan metode komputasi yang tepat dalam mengkonfigurasi, mengelola dan mengintegrasikan sumber daya teknologi informasi
K4	Menciptakan kerjasama yang efektif sebagai anggota atau pemimpin tim yang terlibat dalam aktivitas bidang teknologi informasi
K5	Menerapkan kemampuan berkomunikasi secara efektif dalam berbagai konteks profesional bidang teknologi informasi
K6	Menerapkan perilaku profesional sesuai prinsip hukum dan etika bidang keprofesian teknologi informasi
K7	Mengidentifikasi kebutuhan untuk menjadi wirausahawan di bidang teknologi informasi
<b>Pengetahuan</b>	
P1	Konsep teoritis matematika dan statistika secara umum
P2	Konsep teoritis algoritma dan pemrograman secara umum
P3	Konsep teoritis dan teknik infrastruktur teknologi informasi secara umum
P4	Konsep umum dan metode interaksi manusia komputer
P5	Konsep teoritis dan prinsip manajemen teknologi informasi secara mendalam
P6	Konsep umum dan teknik sistem enterprise
P7	Konsep teoritis, metode dan teknik skalabilitas dan analitik data secara mendalam
P8	Konsep umum dan prinsip keamanan siber
P9	Konsep umum dan prinsip isu sosial dan praktik profesional

## B. CPL Prodi Sarjana Teknologi Informasi yang dibebankan pada mata kuliah:

S11	Memanifestasikan nilai kejiwaan WASAKA terhadap masyarakat dan lingkungannya secara berkelanjutan
U9	Mampu mendokumentasikan, menyimpan, mengamankan, dan menemukan kembali data untuk menjamin kesahihan dan mencegah plagiasi
K3	Menerapkan konsep dan metode komputasi yang tepat dalam mengkonfigurasi, mengelola dan mengintegrasikan sumber daya teknologi informasi

P8	Konsep umum dan prinsip keamanan siber
----	--


### C. CPMK:

CPMK 1	Mampu menganalisa konsep dan teori keamanan siber
CPMK 2	Mampu menerapkan konsep dan teori keamanan siber dalam pengelolaan keamanan sistem dan jaringan

### D. Sub-CPMK:

Sub-CPMK 1	Mahasiswa mampu menganalisa konsep dasar Keamanan Siber
Sub-CPMK 2	Mahasiswa mampu menganalisa konsep Sistem Keamanan Komputer
Sub-CPMK 3	Mahasiswa mampu menganalisa konsep Manajemen Keamanan Siber
Sub-CPMK 4	Mahasiswa mampu menerapkan Program Keamanan Siber sesuai kebutuhan keamanan sistem dan jaringan
Sub-CPMK 5	Mahasiswa mampu menerapkan konsep keamanan siber pada aplikasi berbasis Web
Sub-CPMK 6	Mahasiswa mampu menganalisa konsep keamanan siber pada Sistem Operasi
Sub-CPMK 7	Mahasiswa mampu menganalisa konsep keamanan siber pada Jaringan Komputer dan Penanggulangan Keamanan
Sub-CPMK 8	Mahasiswa mampu menganalisa konsep keamanan siber pada pengelolaan basis data
Sub-CPMK 9	Mahasiswa mampu menganalisa konsep keamanan siber pada pengelolaan Cloud Computing
Sub-CPMK 10	Mahasiswa mampu menganalisa konsep privasi dalam keamanan siber
Sub-CPMK 11	Mahasiswa mampu menerapkan konsep Management and Incidents pada keamanan siber
Sub-CPMK 12	Mahasiswa mampu -menganalisa konsep Legal Issue dan Etik pada keamanan siber

## II. Rencana Pembelajaran Semester

		<b>UNIVERSITAS LAMBUNG MANGKURAT</b> <b>FAKULTAS TEKNIK</b> <b>PROGRAM STUDI TEKNOLOGI INFORMASI</b>				Kode Dokumen		
<b>RENCANA PEMBELAJARAN SEMESTER</b>								
<b>MATA KULIAH (MK)</b> <b>KEAMANAN SIBER</b>		<b>KODE</b> <b>STI4128</b>	<b>Rumpun MK</b> <b>Mata Kuliah Wajib</b>		<b>BOBOT (sks)</b>		<b>SEMESTER</b>	<b>Tgl Penyusunan</b>
					T=3	P=0	4	09 Januari 2023
<b>OTORISASI</b>		<b>Pengembang RPS</b>		<b>Koordinator RMK</b>		<b>Ketua PRODI</b>		
		Andry Fajar Zulkarnain, S.ST.,M.T				Dr.Ir.Yuslena Sari, S.Kom.,M.Kom		
<b>Capaian Pembelajaran (CP)</b>	<b>CPL-PRODI yang dibebankan pada MK</b>							
	S11	Memanifestasikan nilai kejiwaan WASAKA terhadap masyarakat dan lingkungannya secara berkelanjutan						
	U3	Mampu mengkaji implikasi pengembangan atau implementasi ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora sesuai dengan keahliannya berdasarkan kaidah, tata cara dan etika ilmiah dalam rangka menghasilkan solusi, gagasan, desain atau kritik seni;						
	K3	Menerapkan konsep dan metode komputasi yang tepat dalam mengkonfigurasi, mengelola dan mengintegrasikan sumber daya teknologi informasi						
	P8	Konsep umum dan prinsip keamanan siber						
	<b>Capaian Pembelajaran Mata Kuliah (CPMK)</b>							
	CPMK 1	Mampu menganalisa konsep dan teori keamanan siber						
	CPMK 2	Mampu menerapkan konsep dan teori keamanan siber dalam pengelolaan keamanan sistem dan jaringan						
	<b>Kemampuan akhir tiap tahapan belajar (Sub-CPMK)</b>							
	Sub-CPMK 1	Mahasiswa mampu menganalisa konsep dasar Keamanan Siber						
	Sub-CPMK 2	Mahasiswa mampu menganalisa konsep Sistem Keamanan Komputer						
	Sub-CPMK 3	Mahasiswa mampu menganalisa konsep Manajemen Keamanan Siber						
	Sub-CPMK 4	Mahasiswa mampu menerapkan Program Keamanan Siber sesuai kebutuhan keamanan sistem dan jaringan						
	Sub-CPMK 5	Mahasiswa mampu menerapkan konsep keamanan siber pada aplikasi berbasis Web						
	Sub-CPMK 6	Mahasiswa mampu menganalisa konsep keamanan siber pada Sistem Operasi						

	Sub-CPMK 7	Mahasiswa mampu menganalisa konsep keamanan siber pada Jaringan Komputer dan Penanggulangan Keamanan				
	Sub-CPMK 8	Mahasiswa mampu menganalisa konsep keamanan siber pada pengelolaan basis data				
	Sub-CPMK 9	Mahasiswa mampu menganalisa konsep keamanan siber pada pengelolaan Cloud Computing				
	Sub-CPMK 10	Mahasiswa mampu menganalisa konsep privasi dalam keamanan siber				
	Sub-CPMK 11	Mahasiswa mampu menerapkan konsep Management and Incidents pada keamanan siber				
	Sub-CPMK 12	Mahasiswa mampu -menganalisa konsep Legal Issue dan Etik pada keamanan siber				
<b>Deskripsi Singkat MK</b>	Cyber Security (CS) atau keamanan siber merupakan salah satu bidang yang saat ini sangat penting karena maraknya kejahatan yang berlaku di dunia cyber. Keamanan cyber tidak hanya sekedar keamanan dalam data dan perangkat lunak saja, namun sudah masuk pada ranah privasi dan publik. Perkembangan keamanan informasi akan selalu menjadi isu sampai kapan pun seiring dengan perkembangan teknologi informasi dan komunikasi. Isu keamanan cyber dalam hal ini dijadikan sebagai bahan untuk antisipasi terkait dengan kejahatan cyber dan mempelajari metode yang digunakan dalam pengamanan data dan informasi.					
<b>Bahan Kajian: Materi Pembelajaran</b>	<b>Prinsip Keamanan Siber</b> dengan pokok bahasan: 1. Konsep dasar dari Cyber Security 2. Standar Keamanan dan Kontrol 3. Manajemen dan Insiden 4. Legal Issue dan Etik					
<b>Pustaka</b>	<b>Utama :</b>					
	1. P. W. Singer dan Allan Friedman, (2014), Cybersecurity and Cyberwar: What Everyone Needs To Know, Oxford University Press 2. William Stallings, (2005), Cryptography and Network Security Principles and Practices, 4th Edition, Prentice Hall 3. Rhodes-Ousley, Mark. Information Security: The Complete Reference, Second Edition, . Information Security Management: Concepts and Practice. New York, McGraw-Hill, 2013.					
	<b>Pendukung :</b>					
	1.Pfleeger, C.P., Security in Computing 5th Edition, Prentice Hall, Copyright 2010 2.Whitman, Michael E. and Herbert J. Mattord. Roadmap to Information Security for IT and Infosec Managers. Boston, MA: Course Technology, 2011.					
<b>Dosen Pengampu</b>	Andry Fajar Zulkarnain, S.ST.,M.T; Eka Setya Wijaya, S.T.,M.Kom, Muhammad Alkaff, S.Kom.,M.Kom					
<b>Matakuliah syarat</b>	-					
<b>Minggu Ke-  (1)</b>	<b>Sub-CPMK  (2)</b>	<b>Indikator  (3)</b>	<b>Kriteria &amp; Bentuk Penilaian  (4)</b>	<b>Metode Pembelajaran [ Estimasi Waktu]  (5)</b>	<b>Materi Pembelajaran [Pustaka/Referensi]  (6)</b>	<b>Bobot Penilaian (%)  (7)</b>

1	<b>Sub-CPMK-1:</b> Mahasiswa mampu menganalisa konsep dasar Keamanan Siber	<ol style="list-style-type: none"> <li>1. Ketepatan dalam menguraikan konsep cyber security</li> <li>2. Ketepatan dalam menguraikan cara kerja dunia cyber</li> <li>3. Ketepatan dalam mengidentifikasi Pentingnya cyber security</li> <li>4. Ketepatan dalam menganalisa Penanggulangan serangan cyber</li> </ol>	Concept Map	<ul style="list-style-type: none"> <li>- Perception Students Have</li> <li>- Ceramah</li> <li>- <b>(TM: 2x50")</b></li> <li>- <b>Tugas 1:</b></li> <li>- Membuat concept map dari penjelasan teori</li> <li>- <b>(BM: 1x50")</b></li> </ul>	Pendahuluan: <ul style="list-style-type: none"> <li>• Definisi cyber security</li> <li>• Cara kerja dunia cyber</li> <li>• Pentingnya cyber security</li> <li>• Penanggulangan serangan cyber</li> </ul>	5
2	<b>Sub-CPMK-2:</b> Mahasiswa mampu menganalisa konsep Sistem Keamanan Komputer	<ol style="list-style-type: none"> <li>1. Ketepatan dalam menguraikan konsep Sistem Keamanan Komputer</li> <li>2. Ketepatan dalam menguraikan yang berpeluang mengganggu keamanan jaringan komputer dan cara penanggulangannya</li> </ol>	Ringkasan minimal 5 paragraf	<ul style="list-style-type: none"> <li>- Ceramah</li> <li>- Information Search</li> <li>- <b>(TM:2x50")</b></li> <li>- <b>Tugas 2:</b></li> <li>- Membuat ringkasan minimal 5 paragraf</li> <li>- <b>(BM: 1x50")</b></li> </ul>	<ul style="list-style-type: none"> <li>• Sistem Keamanan Komputer</li> <li>• Threats</li> <li>• Harm</li> <li>• Vurnerability</li> <li>• Kontrol</li> </ul>	5
3	<b>Sub-CPMK-3:</b> Mahasiswa mampu menganalisa Konsep Manajemen Keamanan Siber	<ol style="list-style-type: none"> <li>1. Ketepatan dalam menguraikan konsep Authentifikasi pada Cyber Security</li> <li>2. Ketepatan dalam menguraikan Access Control di dalam Cyber Security</li> <li>3. Ketepatan dalam menguraikan konsep Cryptography</li> </ol>	Ringkasan minimal 3 halaman	<ul style="list-style-type: none"> <li>- Ceramah</li> <li>- Jigsaw Learning</li> <li>- <b>(TM: 2x50")</b></li> <li>- <b>Tugas 3:</b></li> <li>- Membuat ringkasan hasil <i>jigsaw learning</i> minimal 3 halaman</li> <li>- <b>(BM: 1x50")</b></li> </ul>	<ul style="list-style-type: none"> <li>• Authentifikasi pada Cyber Security</li> <li>• Access Control di dalam Cyber Security</li> <li>• Cryptography</li> </ul>	10

4,5	<b>Sub-CPMK-4:</b> Mahasiswa mampu menerapkan Program Keamanan Siber sesuai kebutuhan keamanan sistem dan jaringan	<ol style="list-style-type: none"> <li>1. Ketepatan dalam menguraikan tentang Pengenalan Program Cyber Security</li> <li>2. Ketepatan dalam menerapkan Penanggulangannya</li> </ol>	Laporan minimal 2 halaman	<ul style="list-style-type: none"> <li>- Case-Study Teaching</li> <li>- Index Card Match (TM:2x(1x50"))</li> <li>- Problem-Based Learning</li> <li>- Small Group Discussion (TM:2x(1x50"))</li> <li>- <b>Tugas 4:</b> Membuat laporan hasil diskusi kelompok minimal 2 halaman (BM: 1x(1x50"))</li> <li>- Presentasi Tugas 4 (TM:1x(1x50"))</li> </ul>	<ul style="list-style-type: none"> <li>• Pengenalan Program Cyber Security</li> <li>• Unintentional (Non-malicious) Programming Oversights</li> <li>• Malicious Code – Malware</li> <li>• Penanggulangan</li> </ul>	10
6	<b>Sub-CPMK-5:</b> Mahasiswa mampu menerapkan konsep keamanan siber pada aplikasi berbasis Web	<ol style="list-style-type: none"> <li>1. Ketepatan dalam menerapkan konsep Cyber Security pada Web</li> <li>2. Ketepatan dalam menguraikan Serangan pada Browser</li> <li>3. Ketepatan dalam menerapkan Target User pada Serangan Web</li> <li>4. Ketepatan dalam menerapkan serangan pada Email</li> </ol>	Laporan minimal 2 halaman	<ul style="list-style-type: none"> <li>- Information Search (TM:1x50")</li> <li>- Problem-Based Learning (TM:1x50")</li> <li>- <b>Tugas 5:</b> Membuat laporan hasil belajar minimal 2 halaman (BM: 1x50")</li> </ul>	<ul style="list-style-type: none"> <li>• Konsep Cyber Security pada Web</li> <li>• Serangan pada Browser</li> <li>• Target User pada Serangan Web</li> <li>• Serangan pada Email</li> </ul>	10
7	<b>Sub-CPMK-6:</b> Mahasiswa mampu menganalisa konsep keamanan siber pada Sistem Operasi	<ol style="list-style-type: none"> <li>1. Ketepatan dalam menguraikan konsep Keamanan pada Sistem Operasi</li> <li>2. Ketepatan dalam menguraikan Keamanan di dalam desain sistem operasi</li> </ol>	Laporan kerja kelompok minimal 2 halaman	<ul style="list-style-type: none"> <li>- Case-Study Teaching</li> <li>- Problem-Based Learning</li> <li>- Small Group Discussion (TM:2x50")</li> <li>- <b>Tugas 6:</b> Membuat laporan kerja kelompok minimal 2 halaman</li> </ul>	<ul style="list-style-type: none"> <li>• Keamanan pada Sistem Operasi</li> <li>• Keamanan di dalam desain sistem operasi</li> <li>• Aplikasi Rootkit</li> </ul>	5



		3. Ketepatan dalam melakukan implementasi aplikasi Rootkit		(BM: 1x50")		
<b>8</b>	<b>Evaluasi Tengah Semester</b>					
<b>9, 10</b>	<b>Sub-CPMK-7:</b> Mahasiswa mampu menganalisa konsep keamanan siber pada Jaringan Komputer dan Penanggulangan Keamanan	1. Ketepatan dalam menguraikan konsep Jaringan Komputer 2. Ketepatan dalam menguraikan Ancaman untuk Komunikasi Jaringan Komputer 3. Ketepatan dalam menguraikan Keamanan Jaringan Wireless 4. Ketepatan dalam menguraikan perbedaan DoS (Denial of Service) dan DoS (Distributed Denial of Service) 5. Ketepatan dalam menguraikan konsep Kriptografi pada Keamanan Jaringan 6. Ketepatan dalam mengaplikasikan Firewalls 7. Ketepatan dalam mengidentifikasi Deteksi dan Pencegahan Sistem 8. Ketepatan dalam menguraikan konsep Manajemen Jaringan	Laporan praktikum minimal 2 halaman	- Case-Study Teaching (TM:2x(1x50")) - Problem-Based Learning - Praktikum - Small Group Discussion (TM:2x(1x50")) - <b>Tugas 8:</b> Membuat laporan hasil praktikum minimal 2 halaman (BM: 1x(1x50")) - Presentasi Tugas 8 (TM:1x(1x50"))	Cyber Security Pada Jaringan: <ul style="list-style-type: none"> <li>• Konsep Jaringan Komputer</li> <li>• Ancaman untuk Komunikasi Jaringan Komputer</li> <li>• Keamanan Jaringan Wireless</li> <li>• DoS (Denial of Service)</li> <li>• DDoS (Distributed Denial of Service)</li> </ul> Penanggulangan Keamanan <ul style="list-style-type: none"> <li>• Kriptografi pada Keamanan Jaringan</li> <li>• Firewalls</li> <li>• Deteksi dan Pencegahan Sistem</li> <li>• Manajemen Jaringan</li> </ul>	<b>10</b>
<b>11</b>	<b>Sub-CPMK-8:</b> Mahasiswa mampu menganalisa konsep keamanan siber pada pengelolaan basis data	1. Ketepatan dalam menguraikan konsep Pengenalan Database 2. Ketepatan dalam mengidentifikasi	Laporan praktikum minimal 2 halaman	- Case-Study Teaching (TM:1x50") - Problem-Based Learning	<ul style="list-style-type: none"> <li>• Pengenalan Database</li> <li>• Kebutuhan Keamanan pada Database</li> </ul>	<b>10</b>

		Kebutuhan Keamanan pada Database 3. Ketepatan dalam menguraikan tentang Keandalan dan Integritasnya 4. Ketepatan dalam mengidentifikasi Database Disclosure 5. Ketepatan dalam mengidentifikasi konsep Data Mining and Big Data		- Praktikum - Small Group Discussion (TM:1x(1x50")) - <b>Tugas 9:</b> Membuat laporan praktikum minimal 2 halaman (BM: 1x50")	• Keandalan dan Integritas • Database Disclosure • Data Mining and Big Data	
12	<b>Sub-CPMK-9:</b> Mahasiswa mampu menganalisa konsep keamanan siber pada pengelolaan Cloud Computing	1. Ketepatan dalam menguraikan konsep Konsep Cloud Computing 2. Ketepatan dalam menguraikan Perangkat dan teknik keamanan pada Cloud Computing 3. Ketepatan dalam mengidentifikasi manajemen pada Cloud Computing 4. Ketepatan dalam melakukan implementasi layanan Cloud IaaS	Laporan minimal 2 halaman	- Case-Study Teaching (TM:1x50") - Small Group Discussion (TM:1x(1x50")) <b>Tugas 10:</b> - Membuat laporan hasil diskusi minimal 2 halaman (BM: 1x50")	• Konsep Cloud Computing • Perangkat dan teknik keamanan pada Cloud Computing • Identifikasi Manajemen Cloud Computing • Layanan Cloud IaaS	10
13, 14	<b>Sub-CPMK-10:</b> Mahasiswa mampu menganalisa konsep privasi dalam keamanan siber	1. Ketepatan dalam menguraikan konsep privasi 2. Ketepatan dalam hubungan Prinsip dan Kebijakan Privasi 3. Ketepatan dalam menguraikan	Laporan praktikum minimal 2 halaman	- Case-Study Teaching (TM:2x(1x50")) - Problem-Based Learning - Praktikum - Small Group Discussion (TM:2x(1x50"))	• Konsep Privasi • Prinsip dan Kebijakan Privasi • Autentifikasi dan Privasi • Privasi pada Web	10


		Authentifikasi dan Privasi 4. Ketepatan dalam melakukan implementasi Privasi pada Web 5. Ketepatan dalam melakukan implementasi Keamanan pada Email 6. Ketepatan dalam menguraikan Dampak Privasi pada Teknologi Baru		- <b>Tugas 11:</b> Membuat laporan hasil praktikum minimal 2 halaman <b>(BM: 1x(1x50"))</b> - Presentasi Tugas 11 <b>(TM:1x(1x50"))</b>	<ul style="list-style-type: none"> <li>• Keamanan pada Email</li> <li>• Dampak Privasi pada Teknologi Baru</li> </ul>	
15	<b>Sub-CPMK-11:</b> Mahasiswa mampu menerapkan konsep Management and Incidents pada keamanan siber	1. Ketepatan dalam menguraikan konsep Rencana Keamanan Cyber Security 2. Ketepatan dalam memahami Rencana Keberlangsungan Bisnis 3. Ketepatan dalam melakukan instalasi Penanggulangan Insiden dan Analisis Resiko	Laporan praktikum minimal 2 halaman	- Case-Study Teaching <b>(TM:1x50")</b> - Problem-Based Learning - Praktikum - Small Group Discussion <b>(TM:1x(1x50"))</b> - <b>Tugas 12:</b> Membuat laporan praktikum minimal 2 halaman <b>(BM: 1x50")</b>	<ul style="list-style-type: none"> <li>• Rencana Keamanan Cyber Security</li> <li>• Rencana Keberlangsungan Bisnis</li> <li>• Penanggulangan Insiden dan Analisis Resiko</li> </ul>	5
16	<b>Sub-CPMK-12:</b> Mahasiswa mampu menganalisa konsep Legal Issue dan Etik pada keamanan siber	1. Ketepatan dalam melakukan instalasi dan implementasi Proteksi program dan data 2. Ketepatan dalam menerapkan Komputer Crime 3. Ketepatan dalam menguraikan konsep	Laporan praktikum minimal 2 halaman	- Case-Study Teaching <b>(TM:1x50")</b> - Problem-Based Learning - Praktikum - Small Group Discussion <b>(TM:1x(1x50"))</b> - <b>Tugas 13:</b>	<ul style="list-style-type: none"> <li>• Proteksi program dan data</li> <li>• Komputer Crime</li> <li>• Isue pada Keamanan Komputer</li> <li>• Cyber Warfare</li> </ul>	10

		Issue pada Keamanan Komputer 4. Ketepatan dalam menguraikan pemahaman Cyber Warfare		Membuat laporan praktikum minimal 2 halaman (BM: 1x50")		
16	Evaluasi Akhir Semester					100

**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, ketrampilan 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-CP 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. **Teknik 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

### III. SILABUS SINGKAT MATA KULIAH

		<b>UNIVERSITAS LAMBUNG MANGKURAT</b> <b>Fakultas Teknik</b> <b>Program Studi Teknologi Informasi</b>	
<b>SILABUS SINGKAT</b>			
<b>MATA KULIAH</b>	Nama	Keamanan Siber	
	Kode	STI4128	
	Kredit	3 SKS	
	Semester	4	
<b>DESKRIPSI MATA KULIAH</b>			
<p>Cyber Security (CS) atau keamanan siber merupakan salah satu bidang yang saat ini sangat penting karena maraknya kejahatan yang berlaku di dunia cyber. Keamanan cyber tidak hanya sekedar keamanan dalam data dan perangkat lunak saja, namun sudah masuk pada ranah privasi dan publik. Perkembangan keamanan informasi akan selalu menjadi isu sampai kapan pun seiring dengan perkembangan teknologi informasi dan komunikasi. Isu keamanan cyber dalam hal ini dijadikan sebagai bahan untuk antisipasi terkait dengan kejahatan cyber dan mempelajari metode yang digunakan dalam pengamanan data dan informasi.</p>			
<b>CAPAIAN PEMBELAJARAN MATA KULIAH (CPMK)</b>			
<ol style="list-style-type: none"><li>1. Mampu menganalisa konsep dan teori keamanan siber</li><li>2. Mampu menerapkan konsep dan teori keamanan siber dalam pengelolaan keamanan sistem dan jaringan</li></ol>			
<b>SUB CAPAIAN PEMBELAJARAN MATA KULIAH (Sub-CPMK)</b>			
1	Mahasiswa mampu menganalisa konsep dasar Keamanan Siber		
2	Mahasiswa mampu menganalisa konsep Sistem Keamanan Komputer		
3	Mahasiswa mampu menganalisa konsep Manajemen Keamanan Siber		
4	Mahasiswa mampu menerapkan Program Keamanan Siber sesuai kebutuhan keamanan sistem dan jaringan		
5	Mahasiswa mampu menerapkan konsep keamanan siber pada aplikasi berbasis Web		
6	Mahasiswa mampu menganalisa konsep keamanan siber pada Sistem Operasi		
7	Mahasiswa mampu menganalisa konsep keamanan siber pada Jaringan Komputer dan Penanggulangan Keamanan		
8	Mahasiswa mampu menganalisa konsep keamanan siber pada pengelolaan basis data		
9	Mahasiswa mampu menganalisa konsep keamanan siber pada pengelolaan Cloud Computing		
10	Mahasiswa mampu menganalisa konsep privasi dalam keamanan siber		
11	Mahasiswa mampu menerapkan konsep Management and Incidents pada keamanan siber		
12	Mahasiswa mampu -menganalisa konsep Legal Issue dan Etik pada keamanan siber		
<b>MATERI PEMBELAJARAN</b>			
<ol style="list-style-type: none"><li>1. Konsep dasar dari Cyber Security</li><li>2. Standar Keamanan dan Kontrol</li><li>3. Manajemen dan Insiden</li><li>4. Legal Issue dan Etik</li></ol>			
<b>PUSTAKA</b>			
<b>Utama :</b>			
<ol style="list-style-type: none"><li>1. P. W. Singer dan Allan Friedman, (2014), Cybersecurity and Cyberwar: What Everyone Needs To Know, Oxford University Press</li></ol>			

2. William Stallings, (2005), Cryptography and Network Security Principles and Practices, 4th Edition, Prentice Hal
3. Rhodes-Ousley, Mark. Information Security: The Complete Reference, Second Edition, . Information Security Management: Concepts and Practice. New York, McGraw-Hill, 2013.

**Pendukung :**

1. Pfleeger, C.P., Security in Computing 5th Edition, Prentice Hall, Copyright 2010
2. Whitman, Michael E. and Herbert J. Mattord. Roadmap to Information Security for IT and Infosec Managers. Boston, MA: Course Technology, 2011.

**PRASYARAT (Jika ada)**

-