	UNIVERSITAS AMIKOM YOGYAKARTA PROGRAM PASCASARJANA PROGRAM STUDI REGULER S2 TEKNIK INFORMATIKA	RPS-REGMTI-MKW05

RENCANA PEMBELAJARAN SEMESTER
FM-PJM-011/Rev.01/25 Jan 2022

MATA KULIAH (MK)	KODE	Rumpun MK	BOBOT (sks)		SEMESTER	Tanggal Penyusunan
Cyber Security	MKw05	KBK	T = 3	P = 0	3	18/04/2022

OTORISASI / PENGESAHAN	Dosen Pengembang RPS	Koordinator RMK	Ka PRODI

Capaian Pembelajaran	**CPL-PRODI yang dibebankan pada MK**	
	CPL-03	Mampu menyelesaikan permasalahan yang kompleks baik itu inter atau multidisipliner yang dengan menerapkan ilmu informatika dan komputer
	CPL-04	Memiliki wawasan, pengetahuan dan keilmuan yang mendalam di bidang di bidang Ilmu Komputer/Informatika, khususnya dalam ruang lingkup cyber security
	CPL-07	Mampu menganalisis, merancang dan mengimplementasikan sistem security berbasis cyber/ internet yang tepat untuk menyelesaikan masalah pada bidang tertentu
	Capaian Pembelajaran Mata Kuliah (CPMK)	
	CPMK-06	Membangun dan mengevaluasi sistem *cyber security* dalam berbagai area, termasuk yang berkaitan dengan ragam ancaman dan kerentanan, aset dan resiko, teknologi keamanan data, teknologi keamanan jaringan, atau tata kelola cyber security

	CPMK-07	Menguasai teori dan konsep yang mendasari ilmu komputer.khususnya cyber security
	CPMK-13	Menentukan pendekatan sistem cyber security yang sesuai dengan problem yang dihadapi, memilih representasi pengetahuan dan mekanisme penalarannya.
	Kemampuan akhir tiap tahapan belajar (Sub-CPMK)	
	…….	Mahasiswa mampu menjelaskan mengenai teori, konsep, metode, dan prinsip-prinsip dalam cyber security
		Mahasiswa menerapkan konsep security berikut aspek-aspeknya dalam dunia cyber saat ini
		Mahasiswa mampu mengomunikasikan ide dan hasil ekperimen secara lisan dan tertulis
	Korelasi CPMK terhadap Sub-CPMK	

	Sub-CPMK01	Sub-CPMK02	Sub-CPMK03	Sub-CPMK04	Sub-CPMK05	Sub-CPMK06
CPMK-05			V	V	V	V
CPMK-10	V	V				

Deskripsi Singkat MK	Mata Kuliah ini memberikan pengetahuan kepada mahasiswa mengenai cyber security yang melingkupi prinsip-prinsipnya, melakukan perencanaan, perancangan model, infrastruktur dan aplikasi cyber security	
Bahan Kajian : Materi Pembelajaran	Konsep dan arsitektur cyber security, keamanan jaringan dan internet, ragam ancaman siber dan konsep ancaman dan kerentanan Teknologi keamanan data dan konten, teknologi keamanan sistem operasi dan aplikasi (termasuk ragam keamanan sistem berbasis web), teknologi keamanan jaringan dan teknologi keamanan infrastruktur kritis (minggu 2-4) Cyber security governance, ISO 27001, forensik digital, aspek legal cyber security dan Investigation Incident (minggu 5-7) Review Paper, Ide Aplika serta Perancangan dan simulasi (minggu 10-12) Implementasi, Pengujian, Optimasi dan Penyusunan artikel siap publikasi	
Pustaka	**Utama :**	
	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf	
	Pendukung :	

	3. E.Wheeler,2011,“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, Syngress 4. Gurjar, L.R., 2009, Cyber securities and Cyber Terrorism, Vardhaman Mahaveer Open 5. HM Government, Cyber Essentials Scheme Requirements for basic technical protection from cyber attacks, 2014 Online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/ Cyber_Essentials_Requirements.pdf 6. Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.) 7. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018
Dosen Pengampu	Dr. R. M. Agung Harimurti, M. Kom
Matakuliah syarat	-

	Kemampuan akhir tiap tahapan belajar (Sub-CPMK)	**Penilaian**		**Bentuk Pembelajaran; Metode Pembelajaran; Penugasan Mahasiswa; [Estimasi Waktu]**		**Materi Pembelajaran [Pustaka]**	**Bobot Penilaian (%)**
		Indikator	**Kriteria & Teknik**				
(1)	**(2)**	**(3)**	**(4)**	**Luring (5)**	**Daring(6)**	**(7)**	**(8)**
1	Mahasiswa mampu menjelaskan konsep dasar dan perkembangan cyber security	Mampu memahami konsep dasar dan perkembangan cyber security	Baik, cukup, kurang	- Ceramah	- Ceramah	Ceramah, diskusi, presentasi (Ref 1 dan Ref 4)	**2**
2	Mahasiswa mampu menjelaskan Tren Global terhadap Ancaman dan Serangan Siber	Mampu memahami Tren Global terhadap Ancaman dan Serangan Siber	Baik, cukup, kurang	Ceramah	Ceramah	Ceramah, diskusi, presentasi (Ref 1, Ref 4, Ref 5)	**3**
3	Mahasiswa mampu menjelaskan konsep dan ragam elemen dan aspek dalam cyber security	Mampu menterjemahkan dan meresensi buku cyber security (Ref 4) dan menjelaskannya secara lisan dalam bentuk presentasi	Baik, cukup, kurang	Seminar	Seminar	Hasil karya mahasiswa individu/ kelompok	**5**
4	Mahasiswa mampu menjelaskan konsep dan penerapan *security risk, policy, and governance*	Mampu memahami konsep dan penerapan *security risk, policy, and governance*	Baik, cukup, kurang	Ceramah	- Ceramah	Ceramah, diskusi, presentasi (Ref 1 dan Ref 3)	**2**
5	Mahasiswa mampu menjelaskan konsep	Mampu memahami konsep *Information*	Baik, cukup, kurang	Ceramah	Ceramah	Ceramah, diskusi, presentasi (Ref 1 dan Ref 3)	**3**

	Kemampuan akhir tiap tahapan belajar (Sub-CPMK)	Penilaian		Bentuk Pembelajaran; Metode Pembelajaran; Penugasan Mahasiswa; [Estimasi Waktu]		Materi Pembelajaran [Pustaka]	Bobot Penilaian (%)
		Indikator	Kriteria & Teknik				
(1)	(2)	(3)	(4)	Luring (5)	Daring(6)	(7)	(8)
	Information Classification and Privacy	*Classification and Privacy*					
6	Mahasiswa mampu menjelaskan ragam ancaman serangan siber	Mampu mensimulasikan ragam ancaman siber dalam bentuk presentasi	Baik, cukup, kurang	Seminar	Seminar	Hasil karya mahasiswa individu/ kelompok	**5**
7	Mahasiswa mampu menjelaskan konsep dan penerapan teknologi keamanan data	Mampu memahami konsep dan penerapan teknologi keamanan data	Baik, cukup, kurang	Ceramah	Ceramah	Ceramah, diskusi, presentasi (Ref 1 dan Ref 6)	**2**
8	UTS (Ujian Tengah Semester) : materi pertemuan 2-7						
9	Mahasiswa mampu menjelaskan konsep dan penerapan teknologi keamanan jaringan	Mampu memahami konsep dan penerapan teknologi keamanan jaringan	Baik, cukup, kurang		-	Ceramah, diskusi, presentasi (Ref 1 dan Ref 5)	**3**
10	Mahasiswa mampu mengoperasikan pengamanan berbasis data dan jaringan	Mampu mensimulasikan ragam pengamanan berbasis data dan jaringan dalam bentuk presentasi	Baik, cukup, kurang	Seminar	- Seminar	Hasil karya mahasiswa individu/ kelompok	**5**
11	Mahasiswa mampu menjelaskan konsep dan penerapan methodology dan aspek legal cyber security	Mampu memahami konsep dan penerapan methodology dan aspek legal cyber security	Baik, cukup, kurang	Ceramah	- Ceramah	Ceramah, diskusi, presentasi (Ref 1, Ref 2 dan Ref 7)	**2**
12	Mahasiswa mampu menjelaskan standar dan strategi keamanan	Mampu memahami standar dan strategi keamanan informasi	Baik, cukup, kurang	Ceramah	Ceramah	Ceramah, diskusi, presentasi (Ref 1, Ref 2 dan Ref 7)	**3**

	Kemampuan akhir tiap tahapan belajar (Sub-CPMK)	Penilaian		Bentuk Pembelajaran; Metode Pembelajaran; Penugasan Mahasiswa; [Estimasi Waktu]		Materi Pembelajaran [Pustaka]	Bobot Penilaian (%)
		Indikator	Kriteria & Teknik				
(1)	(2)	(3)	(4)	Luring (5)	Daring(6)	(7)	(8)
	informasi						
13	Mahasiswa mampu merancang ragam pemodelan cyber security	Mampu menerapkan ragam pemodelan cyber security dalam bentuk presentasi	Baik, cukup, kurang	Seminar	Seminar	- Hasil karya mahasiswa individu/ kelompok	**15**
14	Mahasiswa mampu merancang ragam pemodelan cyber security (II)	Mampu menerapkan ragam pemodelan cyber security dalam bentuk presentasi	Baik, cukup, kurang	Seminar	Seminar	- Hasil karya mahasiswa individu/ kelompok	
15	Mahasiswa mampu membuat publikasi ilmiah cyber security siap submitt	Mampu memahami dan menulis publikasi ilmiah cyber security siap di submitt	Baik, cukup, kurang	Seminar	Seminar	- Hasil karya mahasiswa individu/ kelompok	**20**
16	**UAS (Ujian Akhir Semester) : materi pertemuan 10 dan 14**						

Teknik Penilaian CPMK

CPL	MK	CPMK	MBKM	Partisipasi (Kuis) %	Tugas Teori %	Tugas Praktikum %	Unjuk Kerja (Presentasi) %	Tes Tulis (UTS) %	Tes Tulis (UAS) %	Tes Lisan (Tugas Kelompok) %	Total %
Mampu menyelesaikan permasalahan yang kompleks dalam cyber security, baik	Teknologi keamanan data dan konten, teknologi keamanan sistem operasi dan aplikasi	Membangun dan mengevaluasi sistem *cyber security* dalam berbagai area, termasuk yang berkaitan		1	2	2	5	5	5	5	30

itu inter atau multidisipliner yang dengan menerapkan ilmu informatika dan komputer	(termasuk ragam keamanan sistem berbasis web), teknologi keamanan jaringan dan teknologi keamanan infrastruktur kritis (minggu 2-4) Cyber security governance, ISO 27001, forensik digital, aspek legal cyber security dan Investigation Incident (minggu 5-7)	dengan ragam ancaman dan kerentanan, aset dan resiko, teknologi keamanan data, teknologi keamanan jaringan, atau tata kelola cyber security									
Memiliki wawasan, pengetahuan dan keilmuan yang mendalam di bidang di bidang Ilmu Komputer/Informatika, khususnya dalam ruang lingkup cyber security	Konsep dan arsitektur cyber security, keamanan jaringan dan internet, ragam ancaman siber dan konsep ancaman dan kerentanan	Menguasai teori dan konsep yang mendasari ilmu komputer.khususnya cyber security		1	2	2	3,5	5	5	3,5	20
Mampu menganalisis, merancang dan mengimplementasikan sistem security	Review Paper, Ide Aplika serta Perancangan dan simulasi (minggu 10-12)	Menentukan pendekatan sistem cyber security yang sesuai dengan problem yang dihadapi,		-	-	-	5	10	20	15	50

berbasis cyber/ internet yang tepat untuk menyelesaikan masalah pada bidang tertentu	Implementasi, Pengujian, Optimasi dan Penyusunan artikel siap publikasi	memilih representasi pengetahuan dan mekanisme penalarannya.									