



# **DOKUMEN KURIKULUM**

## **PROGRAM STUDI SARJANA TERAPAN REKAYASA KEAMANAN SIBER**

### **POLITEKNIK NEGERI CILACAP**

 Jalan Dr. Sutomo No.1 Sidakaya - Cilacap

 [www.pnc.ac.id](http://www.pnc.ac.id)

 (0282) – 537992

 [sekretariat@pnc.ac.id](mailto:sekretariat@pnc.ac.id)

## **TIM PENYUSUN**

### **Ketua**

Nama : Abdul Rohman Supriyono, S.T., M.Kom.  
NIP/NIDN : - / 0615058407

### **Anggota**

Nama : Muhammad Nur Faiz, S.Kom., M.Kom.  
NIP/NIDN : 199303242019031011 / 0624039301

Nama : Oman Somantri, S.Kom., M.Kom.  
NIP/NIDN : 198506272019031006 / 0627068503

Nama : Linda Perdana Wanti, S.Kom., M.Kom.  
NIP/NIDN : 198810102019032020 / 0610108801

Nama : Ratih Hafsarah Maharrani, S.Kom., M.Kom.  
NIP/NIDN : 198509172019032015 / 0017098504

	<b>POLITEKNIK NEGERI CILACAP</b> Jalan Dr. Soetomo No. 1, Sidakaya, Cilacap Telepon: (0282) 533329, Fax: (0282) 537992 Laman: www.pnc.ac.id	<b>Nomor:</b> <b>KPT.2.RKS.D4</b>
	<b>DOKUMEN KURIKULUM</b>	Revisi : 01 Halaman : 40

Proses	Penanggung Jawab			Tanggal
	Nama	Jabatan	Tanda Tangan	
Perumus	Abdul Rohman Supriyono	Koordinator Program Studi		8/5 - 23
Pemeriksa	Cahyo Trileksono	Pengelola P4MP		12/5 - 23
Persetujuan	Bayu Aji Girawan	Wakil Direktur I		19/5 - 23
Penetapan	Riyadi Purwanto	Direktur		20/5 - 23
Pengendalian	Artdhita Fajar Pratiwi	Kepala P4MP		20/7 - 23

## DAFTAR ISI

<b>TIM PENYUSUN</b> .....	<b>II</b>
<b>DAFTAR ISI</b> .....	<b>IV</b>
<b>KATA PENGANTAR</b> .....	<b>VI</b>
I. IDENTITAS PROGRAM STUDI .....	1
II. LANDASAN KURIKULUM .....	1
2.1. Universitas Value .....	1
2.2. Landasan filosofi.....	2
2.3. Landasan Historis.....	3
2.4. Landasan Hukum (Yuridis) .....	6
III. VISI, MISI DAN TUJUAN PENDIDIKAN .....	7
3.1. Visi, Misi dan Tujuan Pendidikan PNC.....	7
3.2. Visi, Misi dan Tujuan Pendidikan Jurusan .....	8
3.3. Visi, Misi dan Tujuan Pendidikan Program Studi .....	9
IV. EVALUASI KURIKULUM DAN PENELUSURAN LULUSAN .....	10
4.1. Penelusuran Lulusan.....	10
4.2. Evaluasi Kurikulum .....	10
V. PROFIL LULUSAN DAN RUMUSAN CAPAIAN PEMBELAJARAN LULUSAN .....	11
5.1. Profil Lulusan .....	11
5.2. Perumusan Capaian Pembelajaran Lulusan (CPL).....	12
5.3. Matrik hubungan Profil Lulusan dengan CPL dan Mata kuliah .....	15
VI. PENETAPAN BAHAN KAJIAN .....	18
6.1. Bahan kajian .....	18
6.2. Matrik hubungan CPL dan bahan kajian .....	19
VII. PEMBENTUKAN MATA KULIAH DAN PENENTUAN BOBOT SKS.....	26
7.1. Pembentukan Mata Kuliah .....	26
7.2. Penentuan bobot sks.....	29
7.3. Matrik hubungan Profil Lulusan dengan Mata kuliah .....	31
VIII. ORGANISASI MATA KULIAH .....	33
IX. DAFTAR SEBARAN MATA KULIAH TIAP SEMESTER .....	37
X. RENCANA PEMBELAJARAN SEMSTER (RPS) .....	39



## **KATA PENGANTAR**

Puji syukur kami panjatkan kehadirat Tuhan Yang Maha Kuasa, karena atas rahmat dan pertolonganNya kami dapat menyelesaikan penyusunan Kurikulum Berdasarkan Standar Nasional Perguruan Tinggi untuk Program Studi Rekayasa Keamanan Siber di Politeknik Negeri Cilacap.

Ucapan terima kasih kami sampaikan kepada pimpinan Politeknik Negeri Cilacap yang sudah mendorong kami untuk mengembangkan kurikulum di Program Studi Rekayasa Keamanan Siber. Ucapan terimakasih yang sama kami sampaikan juga kepada Kepala P4MP yang sudah membantu terlaksananya Penyusunan kurikulum berdasarkan KKNi dan SN Dikti.

Kepada Tim Pengembangan Kurikulum dan seluruh staf Dosen Program Studi Rekayasa Keamanan Siber yang telah bekerja dan memberikan sumbangan pemikiran dalam penyusunan Kurikulum ini, kami ucapkan terimah kasih.

Cilacap, 08 Agustus 2022

Tim Penyusun Kurikulum

Program Studi Rekayasa Keamanan Siber

## I. IDENTITAS PROGRAM STUDI

Nama Perguruan Tinggi (PT)	:	POLITEKNIK NEGERI CILACAP
Jurusan	:	TEKNIK INFORMATIKA
Program Studi	:	REKAYASA KEAMANAN SIBER
Status Akreditasi	:	TERAKREDITASI MINIMUM
Jenjang Pendidikan	:	DIPLOMA 4 (D4) / SARJANA TERAPAN
Gelar Lulusan	:	S.Tr.Kom

## II. LANDASAN KURIKULUM

### 2.1. Universitas Value

Tata nilai dari Politeknik Negeri Cilacap (PNC) adalah: *Building Skill for The Future* artinya mempunyai karakter tinggi vokasi yang mengutamakan keunggulan profesionalisme, keahlian, kedisiplinan dan *link and match* dengan mitra atau mitra usaha.

PNC merupakan lembaga pendidikan yang menjadi sarana bagi bangsa Indonesia dalam meningkatkan kualitas sumber daya manusia, sehingga memiliki peran sangat penting dalam mewujudkan bangsa yang maju dan mandiri, sejahtera lahir dan batin. Oleh karena itu PNC harus menyelenggarakan pendidikan yang makin bermutu, tanggap terhadap kebutuhan pembangunan serta pemerataan pendidikan dan memiliki rasa penuh tanggung jawab terhadap masa depan bangsa dan negara.

Dalam menjalankan fungsi dan misinya PNC selalu:

1. Memegang teguh pada pengembangan, pengkajian dan penerapan Ilmu Pengetahuan, Teknologi (IPTEK) dan Seni ke dalam kehidupan bermasyarakat;
2. Aspirasi untuk meningkatkan berfungsinya IPTEK dalam kehidupan industri dan masyarakat;
3. Bersikap untuk selalu mengabdikan diri kepada masyarakat dan memelopori pembangunan.

Dalam menjalankan fungsi, misi dan jati diri PNC berpedoman pada wawasan berikut:

1. PNC mempunyai jiwa kepeloporan dalam perkembangan teknologi dan perkembangan pendidikan vokasi di tanah air;
2. PNC menjunjung tinggi azas profesionalisme dan mengandalkan mutu dan efisiensi sebagai modal keberhasilan;

3. PNC berupaya untuk mengelola kegiatan secara melembaga dan terpadu sehingga didapat hasil yang optimal;
4. PNC bersikap konsisten terhadap tujuan pendidikan yang telah digariskan, tetapi peka dan luwes terhadap dinamika perubahan tuntutan jaman dan lingkungannya;
5. PNC berwawasan kewirausahaan dalam mengelola potensi yang dimiliki sehingga menghasilkan manfaat yang maksimal bagi pertumbuhan institusi khususnya dan pembangunan nasional umumnya;
6. PNC menentukan arah pengembangan yang berorientasi kepada tuntutan masyarakat (*Link*) dan menerapkannya melalui pengembangan teknologi yang relevan (*Match*).

Berdasarkan misi, jati diri dan wawasan tersebut, PNC harus dapat melaksanakan kewajiban sebagai lembaga pendidikan tinggi vokasi dalam upaya mencerdaskan kehidupan bangsa.

Selanjutnya PNC harus selalu menanamkan tekad untuk memberikan pengabdian yang terbaik bagi pertumbuhan bangsa. Seiring dengan itu fungsi pendidikan yang hingga sekarang diselenggarakan secara melembaga harus dikembangkan dalam rangka menegakan kemandirian PNC agar pelaksanaan kewajiban dan pengabdian terbaik diatas dapat diselenggarakan dengan lebih efektif dan terukur.

## **2.2. Landasan filosofi**

Landasan filosofis pada pengembangan kurikulum Program Studi Sarjana Terapan Rekayasa Keamanan Siber, didasarkan atas berbagai filosofi seperti idealisme, realisme, pragmatisme, konstruktivisme dan nasionalisme, dengan pemikiran sebagai berikut:

- a. Model pendidikan dalam Program Studi Rekayasa Keamanan Siber menjunjung tinggi nilai-nilai sosial, ketaqwaan, perikemanusiaan, martabat, keadilan, dan demokrasi sesuai dengan ketentuan Pancasila dan Undang-undang;
- b. Manusia Indonesia sebagai makhluk Tuhan memiliki fitrah ilahi yang baik, mampu untuk belajar dan berlatih untuk memperoleh pengetahuan, keterampilan, dan membentuk sikap cerdas, cendekia, dan mandiri;
- c. Model pendidikan dalam Program Studi Rekayasa Keamanan Siber membangun manusia Indonesia seutuhnya yang Pancasila; bertaqwa kepada Tuhan Yang



- Maha Esa, berperikemanusiaan, bermartabat, berkeadilan, demokratis, dan menjunjung tinggi nilai-nilai sosial;
- d. Model pendidikan dalam Program Studi Rekayasa Keamanan Siber membekali mahasiswa dengan pengetahuan, keterampilan, dan sikap yang progresif agar dapat eksis dan berjaya dalam kehidupannya;
  - e. Kurikulum pembelajaran Program Studi Rekayasa Keamanan Siber dikembangkan dalam model pembelajaran yang berpusat pada mahasiswa (*student centered learning*), dimana mahasiswa berperan secara aktif dalam mengembangkan pengetahuan baik *soft skill* maupun *hard skill* terkait bidang keilmuan dalam bidang rekayasa keamanan siber;
  - f. Program Studi Rekayasa Keamanan Siber membekali mahasiswa dengan pengetahuan dan keterampilan sesuai bidang ilmu agar dapat eksis dan mandiri dalam kehidupannya;
  - g. Model pendidikan dalam Program Studi Rekayasa Keamanan Siber memperhatikan karakteristik dan kebutuhan mahasiswa, kebutuhan masyarakat, kemajuan IPTEKS, dan kultur budaya bangsa Indonesia;
  - h. Dosen sebagai pendidik memiliki kompetensi profesional yang meliputi kompetensi sosial, pedagogis, kepribadian dan keahlian yang sesuai dengan bidang keilmuannya dan bekerja secara professional.

### **2.3. Landasan Historis**

Ijin operasional Program Studi Sarjana Terapan Rekayasa Keamanan Siber berdasarkan Surat Keputusan Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia Nomor 59/D/OT/2022 tentang Izin Pembukaan Program Studi Rekayasa Keamanan Siber Program Sarjana Terapan Pada Politeknik Negeri Cilacap di Kabupaten Cilacap. Oleh karena itu, pengembangan pendidikan Sarjana Terapan Rekayasa Keamanan Siber merupakan bagian integral dari program pengembangan tenaga pendidik di Indonesia, yang bertujuan mendidik para peserta didik menjadi tenaga profesional, terampil dan ahli sehingga dapat melaksanakan tugas secara optimal, baik secara mandiri maupun dalam kerjasama tim.

Sesuai dengan ketentuan yang tercantum dalam Standar Nasional Pendidikan Tinggi (SN-DIKTI), sebagaimana diatur dalam Permenristekdikti Nomor 44 Tahun 2015 Pasal 1, menyatakan kurikulum adalah seperangkat rencana dan pengaturan mengenai capaian pembelajaran lulusan, bahan kajian, proses, dan penilaian yang digunakan

sebagai pedoman penyelenggaraan Program Studi sebagai bentuk akuntabilitas penyelenggaraan program terhadap para pemangku kepentingan. Standar Nasional Pendidikan Tinggi adalah satuan standar yang meliputi Standar Nasional Pendidikan, ditambah dengan Standar Nasional Penelitian, Standar Nasional Pengabdian kepada Masyarakat. Standar Nasional Pendidikan adalah kriteria minimal tentang pembelajaran pada jenjang pendidikan di perguruan tinggi di seluruh wilayah hukum Negara Kesatuan Republik Indonesia.

Kurikulum pendidikan tinggi merupakan program untuk menghasilkan lulusan, sehingga program tersebut seharusnya menjamin agar lulusannya memiliki kualifikasi yang setara dengan kualifikasi yang disepakati dalam KKNi. Konsep yang dikembangkan Direktorat Jenderal Pembelajaran dan Kemahasiswaan selama ini, dalam menyusun kurikulum dimulai dengan menetapkan profil lulusan yang dijabarkan menjadi rumusan kompetensinya. Dengan adanya KKNi rumusan kemampuan dinyatakan dalam istilah “capaian pembelajaran” (terjemahan dari *learning outcomes*), dimana kompetensi tercakup di dalamnya atau merupakan bagian dari capaian pembelajaran (CP). Penggunaan istilah kompetensi yang digunakan dalam pendidikan tinggi (DIKTI) selama ini setara dengan capaian pembelajaran yang digunakan dalam KKNi, tetapi karena di dunia kerja penggunaan istilah kompetensi diartikan sebagai kemampuan yang sifatnya lebih terbatas, terutama yang terkait dengan uji kompetensi dan sertifikat kompetensi, maka selanjutnya dalam kurikulum pernyataan “kemampuan lulusan” digunakan istilah capaian pembelajaran. Disamping hal tersebut, didalam kerangka kualifikasi di dunia internasional, untuk mendeskripsikan kemampuan setiap jenjang kualifikasi digunakan istilah “*learning outcomes*”.

Urgensi pendidikan dalam jangka pendek diarahkan kepada pemenuhan kebutuhan nasional dalam pembangunan bangsa dan negara pada setiap kehidupan sesuai dengan keahlian yang ada. Untuk menjawab kebutuhan masyarakat, pendidikan Sarjana Terapan Rekayasa Keamanan Siber berorientasi pada pengadaan tenaga dan peningkatan mutu tenaga profesional dibidang rekayasa keamanan siber. Hal ini sebagai akibat semakin majunya ilmu pengetahuan dan teknologi informasi khususnya dibidang keamanan siber. Oleh karena itu, penyelenggaraan program Sarjana Terapan Rekayasa Keamanan Siber harus menyesuaikan diri dengan kemajuan, perkembangan, dan kebutuhan industri yang terjadi yakni bersifat kreatif dan inovatif.

Kurikulum Sarjana Terapan Rekayasa Keamanan Siber mengacu pada Standar Nasional Pendidikan Tinggi (SN DIKTI) sesuai jenjang Kerangka Kualifikasi Nasional Indonesia (KKNI) yang merupakan kerangka penjenjangan capaian pembelajaran (*learning outcome*) untuk menyetarakan output bidang pendidikan formal, non formal dan informal. Dalam rangka menyiapkan lulusan yang tangguh dalam menghadapi perubahan sosial, budaya, dunia kerja, dan teknologi yang semakin berkembang dengan pesat di era revolusi industri 4.0, kompetensi mahasiswa harus semakin diperkuat sesuai dengan perkembangan yang ada. Diperlukan adanya *link and match* antara lulusan pendidikan tinggi bukan hanya dengan dunia usaha dan dunia industri saja tetapi juga dengan masa depan yang semakin cepat mengalami perubahan. Berdasarkan hal tersebut Kementerian Pendidikan dan Kebudayaan telah memberlakukan kebijakan baru dibidang pendidikan tinggi melalui program “Merdeka Belajar–Kampus Merdeka (MBKM)” yang saat ini mulai diterapkan oleh perguruan tinggi. Kebijakan Kemdikbud tersebut berkaitan dengan pemberian kebebasan bagi mahasiswa untuk mengikuti kegiatan pembelajaran selama maksimum tiga semester belajar di luar Program Studi dan kampusnya. Kebijakan MBKM memberikan kesempatan kepada mahasiswa untuk mendapatkan pengalaman belajar yang lebih luas dan kompetensi baru melalui beberapa kegiatan pembelajaran di antaranya pertukaran pelajar, magang/praktik kerja, riset, proyek independen, kegiatan wirausaha, proyek kemanusiaan, mengajar di sekolah, dan proyek di desa/kuliah kerja nyata tematik. Selain itu, mahasiswa juga diberikan kebebasan untuk mengikuti kegiatan belajar di luar program studinya di dalam perguruan tinggi yang sama dengan bobot sks tertentu. Semua kegiatan tersebut dapat dilakukan oleh mahasiswa dengan dibimbing dosen dan diperlukan adanya perjanjian kerja sama jika dilakukan bersama pihak di luar Program Studi.

Kurikulum berbasis capaian yang dikembangkan Program Studi Sarjana Terapan Rekayasa Keamanan Siber akan diorientasikan untuk menghasilkan lulusan berkualitas dengan mengimplementasikan program MBKM. Kerjasama dengan mitra juga akan melibatkan dosen dalam pembimbingan maupun aktivitas alademik untuk peningkatan kompetensinya. Inovasi pembelajaran juga harus dilakukan untuk membekali mahasiswa dengan keterampilan memecahkan permasalahan, berpikir kritis, kolaborasi, komunikasi, dan kepeduliannya melalui berbagai metode pembelajaran inovatif di antaranya pembelajaran pemecahan kasus dan pembelajaran kelompok berbasis proyek. Kurikulum ini merupakan kurikulum yang memaparkan profil lulusan, capaian

pembelajaran, bahan kajian dan kedalaman serta distribusi mata kuliah yang disepakati memiliki beban belajar paling sedikit 144 SKS.

#### **2.4. Landasan Hukum (Yuridis)**

Dasar hukum dan peraturan perundangan yang melandasi di dalam penyusunan kurikulum Program Studi Sarjana Terapan Rekayasa Keamanan Siber, sebagai berikut:

- a. Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 158, Tambahan Lembaran Negara Republik Indonesia Nomor 5336);
- b. Peraturan Presiden No. 8 Tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia (KKNI);
- c. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 73 Tahun 2013 tentang Penerapan Kerangka Kualifikasi Nasional Indonesia Bidang Pendidikan Tinggi;
- d. Peraturan Pemerintah Nomor 4 Tahun 2014 tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 16, Tambahan Lembaran Negara Republik Indonesia Nomor 5500);
- e. Peraturan Menteri Pendidikan dan Kebudayaan No. 102 Tahun 2014 tentang Pendirian, Organisasi, dan Tata Kerja Politeknik Negeri Cilacap;
- f. Peraturan Menteri Riset, Teknologi, dan Pendidikan Tinggi Republik Indonesia Nomor 62 Tahun 2016 tentang Sistem Penjaminan Mutu Pendidikan Tinggi;
- g. Peraturan Menteri Riset, Teknologi, dan Pendidikan Tinggi Republik Indonesia Nomor 7 Tahun 2017 tentang Statuta Politeknik Negeri Cilacap;
- h. Keputusan Direktur Politeknik Negeri Cilacap Nomor 0762/PL.43/DT/2018 tentang Tata Cara Penulisan Nomor Pokok Mahasiswa (NPM) dan Kode Mata Kuliah Program Diploma dan Sarjana;
- i. Keputusan Menteri Riset, Teknologi, dan Pendidikan Tinggi No. 123 Tahun 2019 tentang Magang dan Pengakuan Satuan Kredit Semester Magang Industri untuk Program Sarjana dan Sarjana Terapan;
- j. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi;
- k. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 5 Tahun 2020 tentang Akreditasi Program Studi dan Perguruan Tinggi;
- l. Buku Panduan Merdeka Belajar-Kampus Merdeka Tahun 2020;

- m. Buku Panduan Penyusunan Kurikulum Pendidikan Tinggi di Era Industri 4.0 untuk Mendukung Merdeka Belajar-Kampus Merdeka Tahun 2020.
- n. Peraturan Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi Nomor 32 Tahun 2021 tentang Penamaan Program Studi pada Perguruan Tinggi (Berita Negara Republik Indonesia Tahun 2021 Nomor 1059);
- o. Keputusan Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia Nomor 59/D/OT/2022 tentang Izin Pembukaan Program Studi Rekayasa Keamanan Siber Program Sarjana Terapan Pada Politeknik Negeri Cilacap di Kabupaten Cilacap;
- p. Keputusan Direktur Jenderal Pendidikan Vokasi Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Nomor 27/D/M/2022 tentang Daftar Nama Program Studi Jenis Pendidikan Tinggi Vokasi;
- q. Keputusan Direktur Politeknik Negeri Cilacap Nomor 195/PL43/HK.02/2022 Tentang Penetapan Rencana Strategis (RENSTRA) 2020 – 2024 Politeknik Negeri Cilacap Edisi Revisi 2.

### **III. VISI, MISI DAN TUJUAN PENDIDIKAN**

#### **3.1. Visi, Misi dan Tujuan Pendidikan PNC**

Visi, Misi dan Tujuan Pendidikan PNC tertuang dalam peraturan Menteri Riset, Teknologi, Dan Pendidikan Tinggi nomor 7 tahun 2017 tentang Statuta Politeknik Negeri Cilacap. Visi, Misi dan Tujuan Pendidikan PNC sesuai dengan arah, pengembangan dan penguatan pendidikan tinggi vokasi pada Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi serta kondisi, aspirasi masyarakat dan perkembangan industri. Rumusan Visi, Misi, dan Tujuan Pendidikan PNC adalah sebagai berikut:

##### **3.1.1. Visi Pendidikan PNC**

Dalam rangka pemantapan eksistensi sebagai perguruan tinggi vokasi, maka PNC menetapkan visi: *“Menjadi perguruan tinggi vokasi yang unggul dan berkontribusi bagi masyarakat”*.

##### **3.1.2. Misi Pendidikan PNC**

Sebagai upaya untuk mewujudkan visi di atas, maka PNC menetapkan beberapa misi sebagai berikut:

- 1) Menyelenggarakan Pendidikan Vokasi berbasis teknologi yang bermutu, bermoral dan berkeadilan sosial;

- 2) Menyelenggarakan penelitian dasar dan/atau terapan, serta menyebarluaskan hasil penelitian;
- 3) Menyelenggarakan kegiatan pengabdian untuk membantu meningkatkan taraf hidup masyarakat; dan
- 4) Membentuk jiwa kewirausahaan berbasis teknologi (*technopeneurship*).

### **3.1.3. Tujuan Pendidikan PNC**

Semangat mewujudkan visi dan misi memerlukan kejelasan arah tujuan. Tujuan ini akan menjadi *outcome* dari pelaksanaan tugas dan fungsi tridharma perguruan tinggi oleh PNC, yang dirumuskan sebagai berikut:

- 1) Menghasilkan lulusan yang kompeten di bidang teknologi sesuai dengan standar nasional pendidikan tinggi;
- 2) Menghasilkan penelitian yang dapat diterapkan dan bermanfaat bagi masyarakat;
- 3) Menghasilkan kegiatan yang bermanfaat bagi peningkatan taraf hidup masyarakat; dan
- 4) Menghasilkan lulusan yang berjiwa kewirausahaan

### **3.2. Visi, Misi dan Tujuan Pendidikan Jurusan**

Visi, Misi dan Tujuan Pendidikan Jurusan Teknik Informatika sesuai dengan arah, pengembangan dan penguatan pendidikan PNC, yang tertuang pada Keputusan Direktur Politeknik Negeri Cilacap Nomor 195/PL43/HK.02/2022 Tahun 2012 tentang Penetapan Rencana Strategis (RENSTRA) 2020 – 2024 Politeknik Negeri Cilacap Revisi 2. Rumusan Visi, Misi, dan Tujuan Jurusan Teknik Informatika adalah sebagai berikut:

#### **3.2.1. Visi Jurusan**

Dalam rangka pengelolaan terhadap pelaksanaan Pendidikan Jurusan Teknik Informatika, maka Jurusan Teknik Informatika menetapkan visi: "*Menjadi Jurusan yang unggul dalam pengkajian dan penerapan IPTEK pada bidang Informatika dan mampu berkontribusi bagi masyarakat di tingkat nasional*".

#### **3.2.2. Misi Jurusan**

Sebagai upaya untuk mewujudkan visi di atas, maka Jurusan Teknik Informatika menetapkan beberapa misi sebagai berikut:

- 1) Menyelenggarakan Pendidikan Vokasi berbasis teknologi pada bidang informatika yang bermutu, bermoral dan berkeadilan sosial;
- 2) Menyelenggarakan penelitian dasar dan/atau terapan bidang informatika, serta menyebarluaskan hasil penelitian;

- 3) Menyelenggarakan kegiatan pengabdian untuk membantu meningkatkan taraf hidup masyarakat; dan
- 4) Membentuk jiwa kewirausahaan berbasis teknologi (*technopeneurship*).

### **3.2.3. Tujuan Jurusan**

Semangat mewujudkan visi dan misi memerlukan kejelasan arah tujuan. Tujuan ini akan menjadi *outcome* dari pelaksanaan tugas dan fungsi tridharma perguruan tinggi oleh Jurusan, yang dirumuskan sebagai berikut:

- 1) Menghasilkan lulusan yang kompeten di bidang teknologi sesuai dengan standar nasional pendidikan tinggi;
- 2) Menghasilkan penelitian bidang informatika yang dapat diterapkan dan bermanfaat bagi masyarakat;
- 3) Menghasilkan kegiatan yang bermanfaat bagi peningkatan taraf hidup masyarakat; dan
- 4) Menghasilkan lulusan yang berjiwa kewirausahaan.

### **3.3. Visi, Misi dan Tujuan Pendidikan Program Studi**

Visi, Misi dan Tujuan Pendidikan Program Studi Rekayasa Keamanan Siber sesuai dengan arah, pengembangan dan penguatan pendidikan Jurusan Teknik Informatika. Rumusan Visi, Misi, dan Tujuan Program Studi Rekayasa Keamanan Siber adalah sebagai berikut:

#### **3.3.1 Visi Program Studi**

Menjadi Program Studi sarjana terapan yang berkualitas, beretika, adaptif, dan inovatif serta bermitra erat dengan industri dan masyarakat dibidang rekayasa keamanan siber pada tahun 2027.

#### **3.3.2 Misi Program Studi**

- 1) Menyelenggarakan pendidikan sarjana terapan bidang rekayasa keamanan siber untuk menghasilkan lulusan yang berkualitas, beretika, adaptif, dan inovatif pada rekayasa keamanan siber;
- 2) Melaksanakan penelitian terapan yang relevan dan berkolaborasi erat dengan masyarakat serta industri;
- 3) Melaksanakan kegiatan pengabdian kepada masyarakat melalui penerapan ilmu dan teknologi rekayasa keamanan siber; dan
- 4) Menjalin kerjasama dengan industri dan dunia usaha baik nasional maupun internasional dalam bidang rekayasa keamanan siber.

### **3.3.3 Tujuan Program Studi**

- 1) Menghasilkan lulusan Sarjana Terapan bidang rekayasa keamanan siber yang berkualitas, beretika, adaptif, dan inovatif;
- 2) Menghasilkan karya penelitian dan karya pengabdian kepada masyarakat bidang keamanan siber maupun multidisiplin bagi kelompok UMKM, industri, institusi daerah, pendidikan, dan masyarakat;
- 3) Menghasilkan kerjasama bidang keamanan siber dengan kelompok UMKM, industri, institusi daerah, pendidikan, dan masyarakat dalam rangka terjalin peran DUDI dalam pembelajaran, internship, penelitian kontekstual; dan
- 4) Mewujudkan kepakaran bidang teknologi terapan diakui secara nasional maupun internasional.

## **IV. EVALUASI KURIKULUM DAN PENELUSURAN LULUSAN**

### **4.1. Penelusuran Lulusan**

Program Studi Rekayasa Keamanan Siber didirikan pada tahun 2022, sehingga sampai dengan pelaksanaan Penyusunan Kurikulum ini belum menghasilkan lulusan karena mahasiswa yang ada saat ini baru menempuh perkuliahan sebanyak 1 semester.

### **4.2. Evaluasi Kurikulum**

Kegiatan Penyusunan Kurikulum Program Studi Rekayasa Keamanan Siber ini merupakan suatu langkah tindak lanjut dari Kebijakan baru Kementerian Pendidikan dan Kebudayaan yaitu program “Merdeka Belajar–Kampus Merdeka (MBKM)” yang saat ini mulai diterapkan oleh perguruan tinggi. Kebijakan Kemdikbud tersebut berkaitan dengan pemberian kebebasan bagi mahasiswa untuk mengikuti kegiatan pembelajaran selama maksimum tiga semester belajar di luar Program Studi dan kampusnya. Selain itu Perguruan Tinggi juga dituntut untuk menyusun target dan mengembangkan program untuk pencapaian Indeks Kinerja Utama (IKU) sesuai Keputusan Menteri Pendidikan dan Kebudayaan Nomor 754/P/2020 tentang Indikator Kinerja Utama Perguruan Tinggi Negeri Dan Lembaga Layanan Pendidikan Tinggi di Lingkungan Kementerian Pendidikan dan Kebudayaan telah mendorong perguruan tinggi untuk menyusun program kegiatan berorientasi pencapaian IKU yang di dalamnya juga mencantumkan kinerja Perguruan Tinggi dalam melaksanakan MBKM.

Dalam melakukan kegiatan penyusunan kurikulum ini, Program Studi ditantang dalam mengembangkan kurikulum yang adaptif dan mampu menyesuaikan diri dengan



perkembangan zaman yang semakin pesat tanpa keluar dari tujuan dalam menghasilkan lulusan sesuai dengan capaian pembelajaran yang telah ditentukan. Di samping itu, dalam implementasi kebijakan MBKM dibutuhkan adanya kolaborasi dan kerja sama dengan mitra ataupun pihak lain yang berkaitan dengan bidang keilmuannya dan turut serta dalam mendukung capaian pembelajaran yang diinginkan.

## **V. PROFIL LULUSAN DAN RUMUSAN CAPAIAN PEMBELAJARAN LULUSAN**

### **5.1. Profil Lulusan**

Kurikulum Program Studi Rekayasa Keamanan Siber disusun sebagai jembatan utama bagi terwujudnya visi misi Program Studi yang tercermin dalam profil lulusan. Sesuai capaian pembelajaran dan Peta Okupasi Nasional Keamanan Siber (PONKS), serta disesuaikan dengan level KKNi setidaknya memiliki kualifikasi setara dengan jenjang/level 6. Maka dari itu, profil lulusan dari Program Studi Rekayasa Keamanan Siber adalah sebagai berikut:

1. Lulusan mampu melakukan pengujian keamanan aplikasi sebelum implementasi;
2. Lulusan mampu membuat laporan pelanggaran keamanan dan/atau temuan keamanan;
3. Lulusan memiliki kemampuan dan keterampilan dalam menindaklanjuti ancaman keamanan dalam suatu organisasi;
4. Lulusan dapat mengoperasikan fitur keamanan perangkat jaringan yang meliputi sistem operasi, perangkat lunak, dan perangkat keras;
5. Lulusan memiliki kemampuan merancang jaringan komputer, mengimplementasikan, mengelola dan mengujinya sesuai dengan prinsip keamanan informasi untuk melindungi aset informasi yang dimiliki oleh organisasi;
6. Lulusan memiliki kemampuan etika profesionalitas, integritas, jujur dan bertanggung jawab terhadap peran yang diemban;
7. Lulusan mampu bekerja pada berbagai industri swasta maupun pemerintah yang membutuhkan pengamanan data dan sistem;
8. Lulusan memiliki kemampuan kerja tim, kepemimpinan, berfikir kritis, komunikasi, dan kolaborasi serta jiwa entrepreneurship.

Adapun untuk prospek lulusan dari program studi Rekayasa Keamanan Siber dicantumkan pada Tabel 1:

**Tabel 1** Prospek Lulusan dan Deskripsinya

Prospek Lulusan		Deskripsi Prospek Lulusan
PL1	Cyber Security Analyst	Seseorang yang memiliki kemampuan dan keterampilan bertugas untuk melaksanakan prosedur-prosedur dan perintah dari pejabat di atasnya pada pusat operasi keamanan
PL2	Vulnerability Assessment Analyst	Seseorang yang memiliki kemampuan dan keahlian untuk melakukan assessment terhadap celah keamanan dalam sebuah sistem pada sebuah organisasi.
PL3	Network Security Administrator	Seseorang yang memiliki kemampuan dan keahlian untuk menganalisa ancaman keamanan baik dari dalam maupun luar jaringan dan mengembangkan kebijakan keamanan yang diperlukan sesuai kebijakan keamanan yang berlaku.

### **5.2. Perumusan Capaian Pembelajaran Lulusan (CPL)**

Sesuai ketentuan yang tercantum dalam Standar Nasional Pendidikan Tinggi (SN DIKTI) Nomor 3 tahun 2020, setiap Program Studi wajib dilengkapi dengan target capaian pembelajaran sebagai bentuk akuntabilitas penyelenggaraan program terhadap para pemangku kepentingan. Capaian Pembelajaran Lulusan Program Studi selain merupakan rumusan tujuan pembelajaran yang hendak dicapai dan harus dimiliki oleh semua lulusannya, juga merupakan pernyataan mutu lulusan. Oleh karena itu, Program Studi berkewajiban untuk memiliki rumusan CPL yang dapat dipertanggungjawabkan baik isi, kelengkapan deskripsi sesuai dengan ketentuan dalam SN DIKTI, serta kesetaraan level kualifikasinya dengan Kerangka Kualifikasi Nasional Indonesia (KKNI). Karena merupakan rumusan tujuan pendidikan dan pernyataan mutu lulusan, perumusan CPL merupakan bagian yang tidak terpisahkan dari pengembangan kurikulum Program Studi. Manfaat CPL selain untuk mengarahkan pengelola Program Studi agar mencapai target mutu lulusan, juga memberikan informasi kepada masyarakat tentang pernyataan mutu lulusan Program Studi di perguruan tinggi. Dasar hukum CPL dinyatakan di dalam Peraturan Presiden Nomor 8 Tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia (KKNI) yaitu kerangka penjenjangan kualifikasi kompetensi yang dapat menyandingkan, menyetarakan, dan mengintegrasikan antara bidang pendidikan dan bidang pelatihan kerja serta pengalaman kerja dalam rangka pemberian pengakuan kompetensi kerja sesuai dengan struktur pekerjaan di berbagai sektor (pasal 1 ayat 1). Selanjutnya di dalam pasal 1 ayat 2 peraturan tersebut, CPL

dinyatakan sebagai kemampuan yang diperoleh melalui internalisasi pengetahuan, sikap, keterampilan, kompetensi, dan akumulasi pengalaman kerja.

SN DIKTI yang diatur dalam Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 adalah satuan standar yang meliputi Standar Nasional Pendidikan, ditambah dengan Standar Nasional Penelitian, dan Standar Nasional Pengabdian Kepada Masyarakat. Peraturan tersebut merupakan landasan hukum untuk merumuskan CPL, terutama ketentuan yang tercantum dalam salah satu standar yakni Standar Kompetensi Lulusan (SKL). SKL merupakan kriteria minimal tentang kualifikasi kemampuan lulusan yang mencakup sikap, pengetahuan, dan ketrampilan yang dinyatakan dalam rumusan capaian pembelajaran. Adapun CP Lulusan Program Studi Rekayasa Keamanan Siber diuraikan pada Tabel 2.

**Tabel 2** Capaian Pembelajaran Lulusan Program Studi

No. CPL	Deskripsi Capaian Pembelajaran Lulusan
<b>ASPEK SIKAP</b> [ <i>Sesuai Lampiran Permendikbud Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi</i> ]	
CPLS1	Bertakwa kepada Tuhan Yang Maha Esa dan mampu menunjukkan sikap religius;
CPLS2	Menjunjung tinggi nilai kemanusiaan dalam menjalankan tugas berdasarkan agama, moral, dan etika;
CPLS3	Berkontribusi dalam peningkatan mutu kehidupan bermasyarakat, berbangsa, bernegara, dan kemajuan peradaban berdasarkan Pancasila;
CPLS4	Berperan sebagai warga negara yang bangga dan cinta tanah air, memiliki nasionalisme serta rasa tanggungjawab pada negara dan bangsa;
CPLS5	Menghargai keanekaragaman budaya, pandangan, agama, dan kepercayaan, serta pendapat atau temuan orisinal orang lain;
CPLS6	Bekerja sama dan memiliki kepekaan sosial serta kepedulian terhadap masyarakat dan lingkungan;
CPLS7	Taat hukum dan disiplin dalam kehidupan bermasyarakat dan bernegara;
CPLS8	Menginternalisasi nilai, norma, dan etika akademik;
CPLS9	Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri;
CPLS10	Menginternalisasi semangat kemandirian, kejuangan, dan kewirausahaan.
<b>ASPEK KETRAMPILAN UMUM</b> [ <i>Sesuai Lampiran Permendikbud Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi</i> ]	
CPLKU11	Mampu menerapkan pemikian logis, kritis, inovatif, bermutu, dan terukur dalam melakukan pekerjaan yang spesifik di bidang keahliannya serta sesuai dengan standar kompetensi kerja bidang yang bersangkutan;
CPLKU12	Mampu menunjukkan kinerja mandiri, bermutu, dan terukur;
CPLKU13	Mampu mengkaji kasus penerapan ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora sesuai dengan bidang keahliannya

No. CPL	Deskripsi Capaian Pembelajaran Lulusan
	dalam rangka menghasilkan prototype, prosedur baku, desain atau karya seni, menyusun hasil kajiannya dalam bentuk kertas kerja, spesifikasi desain, atau esai seni, dan mengunggahnya dalam laman perguruan tinggi;
CPLKU14	Mampu menyusun hasil kajian tersebut di atas dalam bentuk kertas kerja, spesifikasi desain, atau esai seni, dan mengunggahnya dalam laman perguruan tinggi;
CPLKU15	Mampu mengambil keputusan secara tepat berdasarkan prosedur baku, spesifikasi desain, persyaratan keselamatan dan keamanan kerja dalam melakukan supervisi dan evaluasi pada pekerjaannya;
CPLKU16	Mampu memelihara dan mengembangkan jaringan kerja sama dan hasil kerja sama di dalam maupun di luar lembaganya;
CPLKU17	Mampu bertanggungjawab atas pencapaian hasil kerja kelompok dan melakukan supervisi dan evaluasi terhadap penyelesaian pekerjaan yang ditugaskan kepada pekerja yang berada di bawah tanggungjawabnya;
CPLKU18	Mampu melakukan proses evaluasi diri terhadap kelompok kerja yang berada dibawah tanggung jawabnya, dan mampu mengelola pembelajaran secara mandiri; dan
CPLKU19	Mampu mendokumentasikan, menyimpan, mengamankan, dan menemukan kembali data untuk menjamin kesahihan dan mencegah plagiasi.
<b>ASPEK KETRAMPILAN KHUSUS</b>	
CPLKK20	Mampu menerapkan konsep matematika terapan, dasar rekayasa dalam pelaksanaan pekerjaan, dan penyelesaian masalah dibidang keamanan siber dengan mengacu standar nasional atau internasional;
CPLKK21	Mampu menerapkan konsep pemrograman, algoritma dan logika sistem serta mampu melakukan konfigurasi perangkat jaringan dalam menyelesaikan pekerjaan dan permasalahan yang berkaitan dengan keamanan siber, informasi, sistem dan jaringan;
CPLKK22	Mampu berkomunikasi secara efektif baik lisan dan tulisan serta mampu mendokumentasikan dengan benar setiap pekerjaan yang dilakukan sesuai prosedur yang berlaku;
CPLKK23	Mampu bekerja dengan prinsip dan tata cara kerja yang efektif dan efisien dan berbasis pada Keselamatan dan Kesehatan Kerja, dan Lingkungan (K3L);
CPLKK24	Mampu mengikuti perkembangan teknologi terutama berkaitan dengan keamanan siber, serta memiliki sikap, etika yang sesuai dengan norma dan peraturan perundangan yang berlaku dalam keamanan siber;
CPLKK25	Mampu melaksanakan kebijakan keamanan siber dengan berlandaskan hukum dan etika;
CPLKK26	Mampu menerapkan konsep keamanan pengembangan perangkat lunak web dan <i>mobile</i> ;
CPLKK27	Mampu menerapkan konsep dalam melakukan mitigasi terkait keamanan informasi, sistem dan jaringan yang sedang atau telah terjadi berdasarkan tata kelola keamanan siber;
CPLKK28	Mampu mengikuti perkembangan teknologi mutakhir dalam bidang keamanan siber, ancaman dan model serangan terbaru, malware dan celah keamanan;
CPLKK29	Mampu merancang, mengimplementasikan, dan mengevaluasi program peningkatan kepedulian serta kesadaran dan pelatihan terkait keamanan siber;

No. CPL	Deskripsi Capaian Pembelajaran Lulusan
CPLKK30	Mampu mengidentifikasi, mendefinisikan, serta menganalisa permasalahan dalam pencegahan, diagnosa, pelacakan serta penanganan suatu insiden, permasalahan atau celah keamanan terkait keamanan informasi, sistem dan jaringan yang sedang atau telah terjadi dengan kepatuhan terhadap regulasi keamanan siber.
<b>ASPEK PENGETAHUAN</b>	
CPLP31	Menguasai konsep dasar rekayasa dalam melaksanakan pekerjaan dan penyelesaian masalah di bidang Keamanan Siber dengan mengacu standar nasional atau internasional;
CPLP32	Menguasai prinsip dan teknik berkomunikasi secara lisan dan tulisan menggunakan bahasa nasional dan internasional;
CPLP33	Menguasai pengetahuan, prinsip dan tata cara kerja yang efektif dan efisien dan berbasis pada keselamatan dan kesehatan kerja, dan lingkungan (K3L);
CPLP34	Menguasai dasar hukum dan etika dalam domain keamanan siber untuk menentukan legalitas cakupan batasan kerja;
CPLP35	Menguasai pengetahuan tentang perkembangan teknologi mutakhir dalam bidang keamanan siber;
CPLP36	Menguasai pengetahuan dalam mengidentifikasi, mendefinisikan dan mengimplementasikan, merencanakan dan mengevaluasi aplikasi, algoritma dan logika sistem serta konfigurasi keamanan informasi, sistem, dan jaringan;
CPLP37	Menguasai konsep dalam melakukan mitigasi, diagnosa, pelacakan serta penanganan suatu insiden, permasalahan atau celah keamanan terkait keamanan informasi, sistem dan jaringan yang sedang atau telah terjadi berdasarkan tata kelola keamanan siber.

### 5.3. Matrik hubungan Profil Lulusan dengan CPL dan Mata kuliah

#### 5.3.1 Hubungan Profil Lulusan dengan CPL

Capaian pembelajaran yang mencakup empat aspek (sikap, keterampilan umum, keterampilan khusus, dan pengetahuan) seperti yang dideskripsikan di atas telah dirumuskan sesuai dengan profil lulusan Program Studi Rekayasa Keamanan Siber. Capaian pembelajaran dan kaitanya dengan profil lulusan dijabarkan secara rinci dalam Tabel 3 berikut.

**Tabel 3.** Matrik hubungan Profil dan CPL

Deskripsi CPL Prodi		PL1	PL2	PL3
CPLS1	Bertakwa kepada Tuhan Yang Maha Esa dan mampu menunjukkan sikap religius;	V	V	V
CPLS2	Menjunjung tinggi nilai kemanusiaan dalam menjalankan tugas berdasarkan agama, moral, dan etika;	V	V	V
CPLS3	Berkontribusi dalam peningkatan mutu kehidupan bermasyarakat, berbangsa, bernegara, dan kemajuan peradaban berdasarkan Pancasila;	V	V	V

Deskripsi CPL Prodi		PL1	PL2	PL3
CPLS4	Berperan sebagai warga negara yang bangga dan cinta tanah air, memiliki nasionalisme serta rasa tanggungjawab pada negara dan bangsa;	V	V	V
CPLS5	Menghargai keanekaragaman budaya, pandangan, agama, dan kepercayaan, serta pendapat atau temuan orisinal orang lain;	V	V	V
CPLS6	Bekerja sama dan memiliki kepekaan sosial serta kepedulian terhadap masyarakat dan lingkungan;	V	V	V
CPLS7	Taat hukum dan disiplin dalam kehidupan bermasyarakat dan bernegara;	V	V	V
CPLS8	Menginternalisasi nilai, norma, dan etika akademik;	V	V	V
CPLS9	Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri;	V	V	V
CPLS10	Menginternalisasi semangat kemandirian, kejuangan, dan kewirausahaan.	V	V	V
CPLKU11	Mampu menerapkan pemikiran logis, kritis, inovatif, bermutu, dan terukur dalam melakukan pekerjaan yang spesifik di bidang keahliannya serta sesuai dengan standar kompetensi kerja bidang yang bersangkutan;	V	v	v
CPLKU12	Mampu menunjukkan kinerja mandiri, bermutu, dan terukur;	v	v	V
CPLKU13	Mampu mengkaji kasus penerapan ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora sesuai dengan bidang keahliannya dalam rangka menghasilkan prototype, prosedur baku, desain atau karya seni, menyusun hasil kajiannya dalam bentuk kertas kerja, spesifikasi desain, atau esai seni, dan mengunggahnya dalam laman perguruan tinggi;	V	V	v
CPLKU14	Mampu menyusun hasil kajian tersebut di atas dalam bentuk kertas kerja, spesifikasi desain, atau esai seni, dan mengunggahnya dalam laman perguruan tinggi;	V	V	v
CPLKU15	Mampu mengambil keputusan secara tepat berdasarkan prosedur baku, spesifikasi desain, persyaratan keselamatan dan keamanan kerja dalam melakukan supervisi dan evaluasi pada pekerjaannya;	V	V	v
CPLKU16	Mampu memelihara dan mengembangkan jaringan kerja sama dan hasil kerja sama di dalam maupun di luar lembaganya;	v	v	V
CPLKU17	Mampu bertanggungjawab atas pencapaian hasil kerja kelompok dan melakukan supervisi dan evaluasi terhadap penyelesaian pekerjaan yang ditugaskan kepada pekerja yang berada di bawah tanggungjawabnya;	v	V	v
CPLKU18	Mampu melakukan proses evaluasi diri terhadap kelompok kerja yang berada dibawah tanggung jawabnya, dan mampu mengelola pembelajaran secara mandiri; dan	v	V	v
CPLKU19	Mampu mendokumentasikan, menyimpan, mengamankan, dan menemukan kembali data untuk menjamin kesahihan dan mencegah plagiasi.	v	v	V
CPLKK20	Mampu menerapkan konsep matematika terapan, dasar rekayasa dalam pelaksanaan pekerjaan, dan penyelesaian masalah dibidang keamanan siber dengan mengacu standar nasional atau internasional;			V

Deskripsi CPL Prodi		PL1	PL2	PL3
CPLKK21	Mampu menerapkan konsep pemrograman, algoritma dan logika sistem serta mampu melakukan konfigurasi perangkat jaringan dalam menyelesaikan pekerjaan dan permasalahan yang berkaitan dengan keamanan siber, informasi, sistem dan jaringan;			V
CPLKK22	Mampu berkomunikasi secara efektif baik lisan dan tulisan serta mampu mendokumentasikan dengan benar setiap pekerjaan yang dilakukan sesuai prosedur yang berlaku;	V	V	
CPLKK23	Mampu bekerja dengan prinsip dan tata cara kerja yang efektif dan efisien dan berbasis pada Keselamatan dan Kesehatan Kerja, dan Lingkungan (K3L);	V	V	
CPLKK24	Mampu mengikuti perkembangan teknologi terutama berkaitan dengan keamanan siber, serta memiliki sikap, etika yang sesuai dengan norma dan peraturan perundangan yang berlaku dalam keamanan siber;		V	
CPLKK25	Mampu melaksanakan kebijakan keamanan siber dengan berlandaskan hukum dan etika;	V	V	
CPLKK26	Mampu menerapkan konsep keamanan pengembangan perangkat lunak web dan <i>mobile</i> ;		V	
CPLKK27	Mampu menerapkan konsep dalam melakukan mitigasi terkait keamanan informasi, sistem dan jaringan yang sedang atau telah terjadi berdasarkan tata kelola keamanan siber;		V	V
CPLKK28	Mampu mengikuti perkembangan teknologi mutakhir dalam bidang keamanan siber, ancaman dan model serangan terbaru, malware dan celah keamanan;	V	V	
CPLKK29	Mampu merancang, mengimplementasikan, dan mengevaluasi program peningkatan kepedulian serta kesadaran dan pelatihan terkait keamanan siber;	V	V	V
CPLKK30	Mampu mengidentifikasi, mendefinisikan, serta menganalisa permasalahan dalam pencegahan, diagnosa, pelacakan serta penanganan suatu insiden, permasalahan atau celah keamanan terkait keamanan informasi, sistem dan jaringan yang sedang atau telah terjadi dengan kepatuhan terhadap regulasi keamanan siber.	V	V	V
CPLP31	Menguasai konsep dasar rekayasa dalam melaksanakan pekerjaan dan penyelesaian masalah di bidang Keamanan Siber dengan mengacu standar nasional atau internasional;	V	V	
CPLP32	Menguasai prinsip dan teknik berkomunikasi secara lisan dan tulisan menggunakan bahasa nasional dan internasional;	V	V	
CPLP33	Menguasai pengetahuan, prinsip dan tata cara kerja yang efektif dan efisien dan berbasis pada keselamatan dan kesehatan kerja, dan lingkungan (K3L);		V	V
CPLP34	Menguasai dasar hukum dan etika dalam domain keamanan siber untuk menentukan legalitas cakupan batasan kerja;	V	V	
CPLP35	Menguasai pengetahuan tentang perkembangan teknologi mutakhir dalam bidang keamanan siber;	V	V	
CPLP36	Menguasai pengetahuan dalam mengidentifikasi, mendefinisikan dan mengimplementasikan, merencanakan dan mengevaluasi aplikasi, algoritma dan logika sistem serta konfigurasi keamanan informasi, sistem, dan jaringan;	V	V	V
CPLP37	Menguasai konsep dalam melakukan mitigasi, diagnosa, pelacakan serta penanganan suatu insiden, permasalahan	V	V	V

Deskripsi CPL Prodi		PL1	PL2	PL3
	atau celah keamanan terkait keamanan informasi, sistem dan jaringan yang sedang atau telah terjadi berdasarkan tata kelola keamanan siber.			

## VI. PENETAPAN BAHAN KAJIAN

Bahan kajian ditetapkan berdasarkan CPL dan/atau menggunakan *Body of Knowledge* (BoK) suatu prodi, yang kemudian digunakan untuk pembentukan matakuliah baru, dan evaluasi serta rekonstruksi terhadap mata kuliah lama atau yang sedang berjalan. Bahan kajian diambil dari peta keilmuan (rumpun ilmu) yang menjadi ciri Program Studi atau dari khasanah keilmuan yang akan dibangun oleh Program Studi.

### 6.1. Bahan kajian

Bahan kajian diambil dari peta keilmuan (rumpun ilmu) yang menjadi ciri Program Studi atau dari khasanah keilmuan yang akan dibangun oleh Program Studi. Bahan kajian juga ditambahkan dengan bidang manajemen dan teknologi informasi yang untuk dipilih berdasarkan analisis kebutuhan dunia kerja/ profesi yang akan ditekuni oleh lulusan Rekayasa Keamanan Siber seperti yang terdapat pada Tabel 4.

**Tabel 4.** Bahan Kajian

No. BK	Bahan Kajian
BK1	Risk Management and Governance / Manajemen Risiko dan Tata Kelola
BK2	Law and Regulation / Hukum dan Peraturan
BK3	Malware and Attack Technologies / Malware dan Teknologi Serangan
BK4	Security Operations and Incident Management / Operasi Keamanan dan Manajemen Insiden
BK5	Forensics / Forensika
BK6	Cryptography / Kriptografi
BK7	Operating Systems and Virtualisation Security / Sistem Operasi dan Keamanan Virtualisasi
BK8	Software Security / Keamanan Perangkat Lunak
BK9	Web and Mobile Security / Keamanan Web dan Perangkat Bergerak
BK10	Network Security / Keamanan Jaringan
BK11	Social and Humanities / Sosial dan Humaniora



## 6.2. Matrik hubungan CPL dan bahan kajian

Setelah Penyusunan Bahan Kajian, maka dilakukan penyusunan matrik hubungan antara Capaian Pembelajaran Lulusan dengan Bahan Kajian seperti terdapat pada Tabel 5.

**Tabel 5.** Matrik hubungan CPL dengan Bahan Kajian

No. CPL	Capaian Pembelajaran Lulusan	BK 1	BK 2	BK 3	BK 4	BK 5	BK 6	BK 7	BK 8	BK 9	BK 10	BK 11
<b>ASPEK SIKAP</b>												
CPLS1	Bertakwa kepada Tuhan Yang Maha Esa dan mampu menunjukkan sikap religius;	V	V									V
CPLS2	Menjunjung tinggi nilai kemanusiaan dalam menjalankan tugas berdasarkan agama, moral, dan etika;	V	V		V	V						V
CPLS3	Berkontribusi dalam peningkatan mutu kehidupan bermasyarakat, berbangsa, bernegara, dan kemajuan peradaban berdasarkan Pancasila;	V	V		V	V						V
CPLS4	Berperan sebagai warga negara yang bangga dan cinta tanah air, memiliki nasionalisme serta rasa tanggungjawab pada negara dan bangsa;	V	V		V							V
CPLS5	Menghargai keanekaragaman budaya, pandangan, agama, dan kepercayaan, serta pendapat atau temuan orisinal orang lain;	V	V						V	V	V	V
CPLS6	Bekerja sama dan memiliki kepekaan sosial serta kepedulian terhadap masyarakat dan lingkungan;	V	V		V	V				V		V
CPLS7	Taat hukum dan disiplin dalam kehidupan	V	V		V	V			V	V	V	

No. CPL	Capaian Pembelajaran Lulusan	BK 1	BK 2	BK 3	BK 4	BK 5	BK 6	BK 7	BK 8	BK 9	BK 10	BK 11
	bermasyarakat dan bernegara;											
CPLS8	Menginternalisasi nilai, norma, dan etika akademik;	V	V		V	V			V	V	V	V
CPLS9	Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri;	V	V		V				V	V	V	V
CPLS10	Menginternalisasi semangat kemandirian, kejuangan, dan kewirausahaan.	V	V		V							V
<b>ASPEK KETRAMPILAN UMUM</b>												
CPLKU11	Mampu menerapkan pemikian logis, kritis, inovatif, bermutu, dan terukur dalam melakukan pekerjaan yang spesifik di bidang keahliannya serta sesuai dengan standar kompetensi kerja bidang yang bersangkutan;	V	V	V	V	V	V		V	V		V
CPLKU12	Mampu menunjukkan kinerja mandiri, bermutu, dan terukur;	V	V		V				V	V	V	V
CPLKU13	Mampu mengkaji kasus penerapan ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora sesuai dengan bidang keahliannya dalam rangka menghasilkan prototype, prosedur baku, desain atau karya seni, menyusun hasil kajiannya dalam bentuk kertas kerja, spesifikasi desain, atau esai seni, dan mengunggahnya dalam laman perguruan tinggi;	V	V		V	V	V		V	V	V	
CPLKU14	Mampu menyusun hasil kajian tersebut di	V	V		V	V			V	V	V	

No. CPL	Capaian Pembelajaran Lulusan	BK 1	BK 2	BK 3	BK 4	BK 5	BK 6	BK 7	BK 8	BK 9	BK 10	BK 11
	atas dalam bentuk kertas kerja, spesifikasi desain, atau esai seni, dan mengunggahnya dalam laman perguruan tinggi;											
CPLKU15	Mampu mengambil keputusan secara tepat berdasarkan prosedur baku, spesifikasi desain, persyaratan keselamatan dan keamanan kerja dalam melakukan supervisi dan evaluasi pada pekerjaannya;	V	V		V	V			V	V	V	
CPLKU16	Mampu memelihara dan mengembangkan jaringan kerja sama dan hasil kerja sama di dalam maupun di luar lembaganya;	V	V		V				V	V	V	V
CPLKU17	Mampu bertanggungjawab atas pencapaian hasil kerja kelompok dan melakukan supervisi dan evaluasi terhadap penyelesaian pekerjaan yang ditugaskan kepada pekerja yang berada di bawah tanggungjawabnya;	V	V		V	V			V	V	V	V
CPLKU18	Mampu melakukan proses evaluasi diri terhadap kelompok kerja yang berada dibawah tanggung jawabnya, dan mampu mengelola pembelajaran secara mandiri; dan	V	V		V	V			V	V	V	V
CPLKU19	Mampu mendokumentasikan, menyimpan, mengamankan, dan menemukan kembali data untuk menjamin	V	V		V	V						V

No. CPL	Capaian Pembelajaran Lulusan	BK 1	BK 2	BK 3	BK 4	BK 5	BK 6	BK 7	BK 8	BK 9	BK 10	BK 11
	kesahihan dan mencegah plagiasi.											
<b>ASPEK KETRAMPILAN KHUSUS</b>												
CPLKK20	Mampu menerapkan konsep matematika terapan, dasar rekayasa dalam pelaksanaan pekerjaan, dan penyelesaian masalah dibidang keamanan siber dengan mengacu standar nasional atau internasional;	V	V	V	V		V		V	V		V
CPLKK21	Mampu menerapkan konsep pemrograman, algoritma dan logika sistem serta mampu melakukan konfigurasi perangkat jaringan dalam menyelesaikan pekerjaan dan permasalahan yang berkaitan dengan keamanan siber, informasi, sistem dan jaringan;			V		V		V	V	V		V
CPLKK22	Mampu berkomunikasi secara efektif baik lisan dan tulisan serta mampu mendokumentasikan dengan benar setiap pekerjaan yang dilakukan sesuai prosedur yang berlaku;	V	V		V	V						V
CPLKK23	Mampu bekerja dengan prinsip dan tata cara kerja yang efektif dan efisien dan berbasis pada Keselamatan dan Kesehatan Kerja, dan Lingkungan (K3L);	V	V		V	V		V	V	V	V	
CPLKK24	Mampu mengikuti perkembangan teknologi terutama berkaitan dengan keamanan siber, serta memiliki sikap, etika yang sesuai dengan	V	V	V	V	V			V	V	V	

No. CPL	Capaian Pembelajaran Lulusan	BK 1	BK 2	BK 3	BK 4	BK 5	BK 6	BK 7	BK 8	BK 9	BK 10	BK 11
	norma dan peraturan perundangan yang berlaku dalam keamanan siber;											
CPLKK25	Mampu melaksanakan kebijakan keamanan siber dengan berlandaskan hukum dan etika;	V	V		V	V			V	V		V
CPLKK26	Mampu menerapkan konsep keamanan pengembangan perangkat lunak web dan <i>mobile</i> ;						V		V	V		
CPLKK27	Mampu menerapkan konsep dalam melakukan mitigasi terkait keamanan informasi, sistem dan jaringan yang sedang atau telah terjadi berdasarkan tata kelola keamanan siber;	V			V				V	V	V	
CPLKK28	Mampu mengikuti perkembangan teknologi mutakhir dalam bidang keamanan siber, ancaman dan model serangan terbaru, malware dan celah keamanan;	V		V	V		V		V	V	V	
CPLKK29	Mampu merancang, mengimplementasikan, dan mengevaluasi program peningkatan kepedulian serta kesadaran dan pelatihan terkait keamanan siber;	V	V		V			V	V	V	V	
CPLKK30	Mampu mengidentifikasi, mendefinisikan, serta menganalisa permasalahan dalam pencegahan, diagnosa, pelacakan serta penanganan suatu insiden, permasalahan atau celah keamanan	V	V	V	V	V	V		V	V		V

No. CPL	Capaian Pembelajaran Lulusan	BK 1	BK 2	BK 3	BK 4	BK 5	BK 6	BK 7	BK 8	BK 9	BK 10	BK 11
	terkait keamanan informasi, sistem dan jaringan yang sedang atau telah terjadi dengan kepatuhan terhadap regulasi keamanan siber.											
<b>ASPEK PENGETAHUAN</b>												
CPLP31	Menguasai konsep dasar rekayasa dalam melaksanakan pekerjaan dan penyelesaian masalah di bidang Keamanan Siber dengan mengacu standar nasional atau internasional;	V			V			V	V	V	V	
CPLP32	Menguasai prinsip dan teknik berkomunikasi secara lisan dan tulisan menggunakan bahasa nasional dan internasional;	V	V		V							V
CPLP33	Menguasai pengetahuan, prinsip dan tata cara kerja yang efektif dan efisien dan berbasis pada keselamatan dan kesehatan kerja, dan lingkungan (K3L);	V	V	V	V	V	V	V	V	V		V
CPLP34	Menguasai dasar hukum dan etika dalam domain keamanan siber untuk menentukan legalitas cakupan batasan kerja;	V	V		V			V	V	V	V	
CPLP35	Menguasai pengetahuan tentang perkembangan teknologi mutakhir dalam bidang keamanan siber;	V	V		V	V		V	V	V	V	V
CPLP36	Menguasai pengetahuan dalam mengidentifikasi, mendefinisikan dan mengimplementasikan, merencanakan dan mengevaluasi aplikasi,	V	V	V	V	V	V		V	V		V

No. CPL	Capaian Pembelajaran Lulusan	BK 1	BK 2	BK 3	BK 4	BK 5	BK 6	BK 7	BK 8	BK 9	BK 10	BK 11
	algoritma dan logika sistem serta konfigurasi keamanan informasi, sistem, dan jaringan;											
CPLP37	Menguasai konsep dalam melakukan mitigasi, diagnosa, pelacakan serta penanganan suatu insiden, permasalahan atau celah keamanan terkait keamanan informasi, sistem dan jaringan yang sedang atau telah terjadi berdasarkan tata kelola keamanan siber.	V	V	V	V	V	V	V	V	V		V





No. Mata Kuliah	Nama Mata Kuliah	CPLS1	CPLS2	CPLS3	CPLS4	CPLS5	CPLS6	CPLS7	CPLS8	CPLS9	CPLS10	CPLKU11	CPLKU12	CPLKU13	CPLKU14	CPLKU15	CPLKU16	CPLKU17	CPLKU18	CPLKU19	CPLKK20	CPLKK21	CPLKK22	CPLKK23	CPLKK24	CPLKK25	CPLKK26	CPLKK27	CPLKK28	CPLKK29	CPLKK30	CPLP31	CPLP32	CPLP33	CPLP34	CPLP35	CPLP36	CPLP37															
MK16	Bahasa Inggris	v	v	v	v	v	v	v	v	v	v									v																																	
MK17	Sistem Basis Data	v	v	v	v	v	v	v	v	v	v	v	v	v																													v										
MK18	Prak. Jaringan Komputer	v	v	v	v	v	v	v	v	v	v	v	v	v																														v									
MK19	Prak. Sistem Basis Data	v	v	v	v	v	v	v	v	v	v	v	v	v																														v									
MK20	Administrasi Sistem Komputer dan Jaringan	v	v	v	v	v	v	v	v	v	v	v	v	v																														v	v								
MK21	Keamanan Data dan Informasi	v	v	v	v	v	v	v	v	v	v	v	v	v																														v	v	v	v						
MK22	Kriptografi	v	v	v	v	v	v	v	v	v	v	v	v	v																															v	v	v						
MK23	Arsitektur Keamanan	v	v	v	v	v	v	v	v	v	v	v	v	v																																v	v	v					
MK24	Keamanan Jaringan	v	v	v	v	v	v	v	v	v	v	v	v	v																																v	v	v					
MK25	Etika Profesi	v	v	v	v	v	v	v	v	v	v																																				v	v					
MK26	Prak. Administrasi Sistem Komputer dan Jaringan	v	v	v	v	v	v	v	v	v	v	v	v	v																																	v	v	v				
MK27	Prak. Arsitektur Keamanan	v	v	v	v	v	v	v	v	v	v	v	v	v																																		v	v	v			
MK28	Prak. Keamanan Jaringan	v	v	v	v	v	v	v	v	v	v	v	v	v																																		v	v				
MK29	Keamanan Basis Data	v	v	v	v	v	v	v	v	v	v	v	v	v																																		v	v	v			
MK30	Pemrograman Keamanan Web	v	v	v	v	v	v	v	v	v	v	v	v	v																																		v	v	v			
MK31	Probabilitas dan Statistika	v	v	v	v	v	v	v	v	v	v																																							v			
MK32	Kewarganegaraan	v	v	v	v	v	v	v	v	v	v																																							v			
MK33	Agama	v	v	v	v	v	v	v	v	v	v																																								v		
MK34	Pemrograman Perangkat Bergerak	v	v	v	v	v	v	v	v	v	v	v	v	v																																				v			
MK35	Prak. Keamanan Basis Data	v	v	v	v	v	v	v	v	v	v	v	v	v																																			v	v	v		
MK36	Prak. Pemrograman Keamanan Web	v	v	v	v	v	v	v	v	v	v	v	v	v																																				v	v	v	
MK37	Prak. Pemrograman Perangkat Bergerak	v	v	v	v	v	v	v	v	v	v	v	v	v																																					v		
MK38	Komunikasi Bahasa Inggris	v	v	v	v	v	v	v	v	v	v																																							v			
MK39	Penetrasi Testing	v	v	v	v	v	v	v	v	v	v	v	v	v																																				v	v	v	
MK40	Bahasa Indonesia	v	v	v	v	v	v	v	v	v	v																																										
MK41	Pengujian Perangkat Lunak	v	v	v	v	v	v	v	v	v	v	v	v	v																																				v	v	v	v
MK42	Keamanan Perangkat Bergerak	v	v	v	v	v	v	v	v	v	v	v	v	v																																					v	v	v

No. Mata Kuliah	Nama Mata Kuliah	CP LS 1	CP LS 2	CP LS 3	CP LS 4	CP LS 5	CP LS 6	CP LS 7	CP LS 8	CP LS 9	CP LS 10	CP LK U 1 1	CP LK U 1 2	CP LK U 1 3	CP LK U 1 4	CP LK U 1 5	CP LK U 1 6	CP LK U 1 7	CP LK U 1 8	CP LK U 1 9	CP LK K 2 0	CP LK K 2 1	CP LK K 2 2	CP LK K 2 3	CP LK K 2 4	CP LK K 2 5	CP LK K 2 6	CP LK K 2 7	CP LK K 2 8	CP LK K 2 9	CP LK K 3 0	CP LP 3 1	CP LP 3 2	CP LP 3 3	CP LP 3 4	CP LP 3 5	CP LP 3 6	CP LP 3 7					
MK43	Keamanan Web dan Cloud	v	v	v	v	v	v	v	v	v	v	v	v	v	v							v				v	v	v	v	v	v	v							v	v	v		
MK44	Keamanan Sistem Siber-Fisik	v	v	v	v	v	v	v	v	v	v	v	v	v	v							v		v	v	v	v	v	v	v	v	v				v			v	v	v		
MK45	Forensik Digital	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v				v	v	v				v	v			v	v	v	v					v	v	v	v		
MK46	Prak. Penetrasi Testing	v	v	v	v	v	v	v	v	v	v	v	v	v	v				v		v				v	v			v	v	v	v	v	v					v	v	v	v	
MK47	Prak. Pengujian Perangkat Lunak	v	v	v	v	v	v	v	v	v	v	v	v	v	v				v		v				v	v	v	v	v	v	v	v	v					v	v	v	v		
MK48	Prak. Forensik Digital	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v				v	v	v				v	v			v	v	v	v					v	v	v	v		
MK49	Magang Industri	v	v	v	v	v	v	v	v	v	v	v	v		v		v	v	v	v				v	v	v	v									v	v						
MK50	Proyek Keamanan Siber	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v			v	v	v	v	v	v	v	v	v	v				v			v	v	v		
MK51	Audit dan Tata Kelola Keamanan Siber	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v			v	v	v	v	v			v	v	v	v	v			v	v	v	v	v		
MK52	Kepemimpinan dan Manajemen Proyek	v	v	v	v	v	v	v	v	v	v				v	v	v	v	v					v	v												v	v					
MK53	Kewirausahaan	v	v	v	v	v	v	v	v	v	v		v				v	v	v					v																			
MK54	Manajemen Risiko TI	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v					v		v	v	v										v					
MK55	Metode Penelitian	v	v	v	v	v	v	v	v	v	v			v										v													v						
MK56	Manajemen Bisnis	v	v	v	v	v	v	v	v	v	v													v																			
MK57	Prak. Audit dan Tata Kelola Keamanan Siber	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v			v	v	v	v			v	v	v	v	v	v			v	v	v	v	v		
MK58	Prak. Manajemen Bisnis	v	v	v	v	v	v	v	v	v	v														v																		
MK59	Tugas Akhir	v	v	v	v	v	v	v	v	v	v	v	v	v	v											v	v	v	v	v	v	v	v	v			v	v	v	v	v	v	
MK60	Bahasa Inggris Dunia Kerja	v	v	v	v	v	v	v	v	v	v		v				v	v																			v						

## 7.2. Penentuan bobot sks

Penentuan Bobot SKS dilakukan dengan cara mengelompokan matakuliah berdasarkan bahan kajian yang sudah disusun kemudian menentukan sks dari matakuliah bersangkutan baik teori maupun praktek. Bobot SKS dalam kurikulum Program Studi Rekayasa Keamanan Siber tercantum dalam Tabel 7.

**Tabel 7.** Bobot sks mata kuliah

No	Bahan Kajian	Mata Kuliah	SKS	
			Teori	Praktek/ Praktikum
1	Risk Management and Governance / Manajemen Risiko dan Tata Kelola	MK2	2	
		MK10		2
		MK12	2	
		MK22	3	
		MK24	2	
		MK25	2	
		MK28		2
		MK41	2	
		MK45	2	
		MK47		2
		MK48		2
		MK51	2	
		MK54	2	
MK57		3		
2	Law and Regulation / Hukum dan Peraturan	MK12	2	
		MK25	2	
3	Malware and Attack Technologies / Malware dan Teknologi Serangan	MK2	2	
		MK10		2
		MK21	3	
		MK24	2	
		MK28		2
		MK39	2	
		MK43	2	
		MK45	2	
		MK46		2
		MK48		2
		MK51	2	
MK57		3		
4	Security Operations and Incident Management / Operasi Keamanan dan Manajemen Insiden	MK2	2	
		MK10		2
		MK21	3	
		MK22	3	
		MK39	2	
		MK45	2	
MK46		2		

No	Bahan Kajian	Mata Kuliah	SKS	
			Teori	Praktek/ Praktikum
		MK48		2
		MK51	2	
		MK54	2	
		MK57		3
5	Forensics / Forensika	MK45	2	
		MK48		2
6	Cryptography / Kriptografi	MK2	2	
		MK3	2	
		MK10		2
		MK21	3	
		MK22	3	
		MK23	2	
		MK24	2	
		MK27		2
		MK28		2
		MK30	2	
		MK36		2
		MK42	2	
		MK43	2	
		MK44	2	
7	Operating Systems and Virtualisation Security / Sistem Operasi dan Keamanan Virtualisasi	MK2	2	
		MK10		2
		MK23	2	
		MK24	2	
		MK27		2
		MK28		2
		MK43	2	
MK44	2			
8	Software Security / Keamanan Perangkat Lunak	MK3	2	
		MK7	2	
		MK9		2
		MK12	2	
		MK13	2	
		MK17	2	
		MK18		2
		MK19		2
		MK24	2	
		MK28		2
		MK29	2	
		MK30	2	
MK35		2		
MK36		2		
9		MK7	2	
		MK9		2

No	Bahan Kajian	Mata Kuliah	SKS	
			Teori	Praktek/ Praktikum
	Web and Mobile Security / Keamanan Web dan Perangkat Bergerak	MK21	3	
		MK22	3	
		MK29	2	
		MK30	2	
		MK34	2	
		MK35		2
		MK36		2
		MK37		2
		MK39	2	
		MK41	2	
		MK42	2	
		MK43	2	
		MK46		2
		MK47		2
10	Network Security / Keamanan Jaringan	MK21	3	
		MK23	2	
		MK24	2	
		MK27		2
		MK28		2
		MK30	2	
		MK34	2	
		MK36		2
		MK42	2	
MK43	2			
11	Social and Humanities / Sosial dan Humaniora	MK3	2	
		MK12	2	
		MK25	2	

### 7.3. Matrik hubungan Profil Lulusan dengan Mata kuliah

Matrik hubungan profil lulusan dengan mata kuliah dapat dilihat pada Tabel 8.

**Tabel 8.** Matrik hubungan profil dan mata kuliah

No	Mata Kuliah	PL1	PL2	PL3
1	Arsitektur dan Organisasi Komputer			V
2	Sistem Operasi			V
3	Pengantar Keamanan Siber	V	V	V
4	Struktur dan Literasi Data	V	V	
5	Kalkulus	V	V	
6	Pancasila	V	V	V
7	Algoritma Pemrograman	V	V	

No	Mata Kuliah	PL1	PL2	PL3
8	Prak. Arsitektur dan Organisasi Komputer			V
9	Prak. Algoritma Pemrograman	V	V	
10	Prak. Sistem Operasi			V
11	Matematika Diskrit	V	V	
12	Hukum Keamanan Siber	V	V	V
13	Jaringan Komputer			V
14	Pengantar Teknologi Informasi	V	V	V
15	Kecerdasan Buatan		V	
16	Bahasa Inggris	V	V	V
17	Sistem Basis Data		V	V
18	Prak. Jaringan Komputer			V
19	Prak. Sistem Basis Data		V	V
20	Administrasi Sistem Komputer dan Jaringan		V	V
21	Keamanan Data dan Informasi	V	V	V
22	Kriptografi		V	V
23	Arsitektur Keamanan			V
24	Keamanan Jaringan			V
25	Etika Profesi	V	V	V
26	Prak. Administrasi Sistem Komputer dan Jaringan			V
27	Prak. Arsitektur Keamanan	V	V	V
28	Prak. Keamanan Jaringan	V	V	V
29	Keamanan Basis Data		V	V
30	Pemrograman Keamanan Web			V
31	Probabilitas dan Statistika	V	V	
32	Kewarganegaraan	V	V	
33	Agama		V	V
34	Pemrograman Perangkat Bergerak		V	V
35	Prak. Keamanan Basis Data	V	V	
36	Prak. Pemrograman Keamanan Web	V	V	V
37	Prak. Pemrograman Perangkat Bergerak	V	V	V
38	Komunikasi Bahasa Inggris	V	V	
39	Penetrasi Testing		V	
40	Bahasa Indonesia		V	
41	Pengujian Perangkat Lunak	V	V	

No	Mata Kuliah	PL1	PL2	PL3
42	Keamanan Perangkat Bergerak	V	V	
43	Keamanan Web dan Cloud	V	V	
44	Keamanan Sistem Siber-Fisik	V	V	
45	Forensik Digital	V	V	V
46	Prak. Penetrasi Testing	V	V	V
47	Prak. Pengujian Perangkat Lunak	V	V	V
48	Prak. Forensik Digital	V	V	V
49	Magang Industri	V	V	V
50	Proyek Keamanan Siber	V	V	
51	Audit dan Tata Kelola Keamanan Siber		V	
52	Kepemimpinan dan Manajemen Proyek	V	V	V
53	Kewirausahaan	V	V	V
54	Manajemen Risiko TI	V	V	V
55	Metode Penelitian	V	V	V
56	Manajemen Bisnis	V	V	V
57	Prak. Audit dan Tata Kelola Keamanan Siber	V	V	
58	Prak. Manajemen Bisnis	V	V	
59	Tugas Akhir	V	V	V
60	Bahasa Inggris Dunia Kerja	V	V	V

## VIII. ORGANISASI MATA KULIAH

Tahapan penyusunan struktur kurikulum dalam bentuk organisasi matrik mata kuliah per semester dilakukan dengan memperhatikan hal-hal sebagai berikut:

- a. Tahapan pembelajaran mata kuliah yang direncanakan dalam usaha memenuhi capaian pembelajaran lulusan;
- b. Ketepatan letak mata kuliah yang disesuaikan dengan keruntutan tingkat kemampuan dan integrasi antar mata kuliah baik secara vertikal maupun horisontal;
- c. Beban belajar mahasiswa secara normal antara 8–10 jam per hari per minggu yang setara dengan beban 17-21 sks per semester.
- d. Proses penyusunannya melibatkan seluruh dosen Program Studi dan selanjutnya ditetapkan oleh Program Studi.

**Tabel 9.** Matrik organisasi mata kuliah prodi Rekayasa Keamanan Siber

SMT	SKS	MATA KULIAH DALAM PRODI										MK-MBKM				
												DALAM PT	PT LAIN	NON-PT		
VIII	8	Tugas Akhir				Bahasa Inggris Dunia Kerja										
VII	20	Audit dan Tata Kelola Keamanan Siber	Kepemimpinan dan Manajemen Proyek	Kewirausahaan	Manajemen Risiko TI	Metode Penelitian	Manajemen Bisnis	Prak. Audit dan Tata Kelola Keamanan Siber	Prak. Manajemen Bisnis				MBKM Pertukaran Mahasiswa (sesuai sks mata kuliah)	MBKM Kewirausahaan (6-10 sks) - Pertukaran Mahasiswa (sesuai sks mata kuliah) - Penelitian/Riset (20 sks)	MBKM Kewirausahaan (6-10 sks) - Penelitian/Riset (20 sks)	
VI	22	Proyek Keamanan Siber													Magang Industri	
V	20	Penetrasi Testing	Bahasa Indonesia	Pengujian Perangkat Lunak	Keamanan Perangkat Bergerak	Keamanan Web dan Cloud	Keamanan Sistem Siber-Fisik	Forensik Digital	Prak. Penetrasi Testing	Prak. Pengujian Perangkat Lunak	Prak. Forensik Digital					
IV	21	Keamanan Basis Data	Pemrograman Keamanan Web	Probabilitas dan Statistika	Kewarganegaraan	Agama	Pemrograman Perangkat Bergerak	Prak. Keamanan Basis Data	Prak. Pemrograman Keamanan Web	Prak. Pemrograman Perangkat Bergerak	Komunikasi Bahasa Inggris					
III	20	Administrasi Sistem Komputer dan Jaringan	Keamanan Data dan Informasi	Kriptografi	Arsitektur Keamanan	Keamanan Jaringan	Etika Profesi	Prak. Administrasi Sistem Komputer dan Jaringan	Prak. Arsitektur Keamanan	Prak. Keamanan Jaringan						




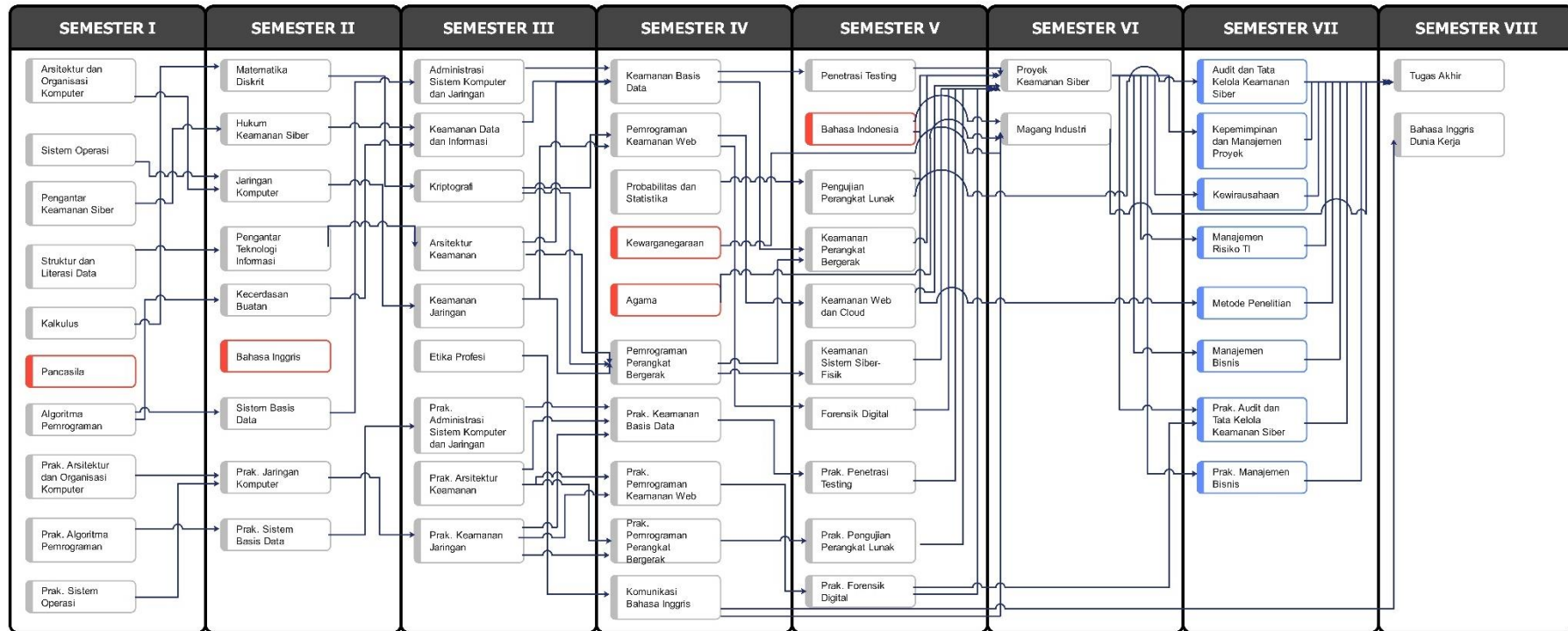
SMT	SKS	MATA KULIAH DALAM PRODI										MK-MBKM		
												DALAM PT	PT LAIN	NON-PT
II	20	Matematika Diskrit	Hukum Keamanan Siber	Jaringan Komputer	Pengantar Teknologi Informasi	Kecerdasan Buatan	Bahasa Inggris	Sistem Basis Data	Prak. Jaringan Komputer	Prak. Sistem Basis Data				
I	20	Arsitektur dan Organisasi Komputer	Sistem Operasi	Pengantar Keamanan Siber	Struktur dan Literasi Data	Kalkulus	Pancasila	Algoritma Pemrograman	Prak. Arsitektur dan Organisasi Komputer	Prak. Algoritma Pemrograman	Prak. Sistem Operasi			
JML	151													

Keterangan:

	: Matakuliah Wajib Umum
	: Matakuliah Wajib Program Studi
	: Matakuliah MBKM

Gambar 10. Peta Kurikulum Program Studi Rekayasa Keamanan Siber

<b>PETA KURIKULUM PRODI.</b> <b>REKAYASA KEAMANAN SIBER</b> <a href="https://jti.pnc.ac.id/siber">https://jti.pnc.ac.id/siber</a>	<b>V.1.0.</b>	 <b>REKAYASA KEAMANAN SIBER</b> POLITEKNIK NEGERI CILACAP
	<b>2022</b>	



**Keterangan:**

Replace your title here! Matakuliah Wajib Umum

Replace your title here! Matakuliah Wajib Program Studi

Replace your title here! Matakuliah MBKM

## IX. DAFTAR SEBARAN MATA KULIAH TIAP SEMESTER

Sebaran mata kuliah tiap semester dimaksudkan untuk mendistribusikan mata kuliah yang ada di Program Studi kedalam tiap semester yang disesuaikan dengan beban belajar mahasiswa untuk mencapai profil lulusan yang dimiliki Program Studi. Adapun sebaran mata kuliah tiap semester Program Studi Rekayasa Keamanan Siber dapat dilihat seperti pada Tabel 11.

**Tabel 11.** Sebaran mata kuliah tiap semester

SEMESTER I				
No	Kode MK	Mata Kuliah	Bobot SKS	
			Teori	Praktek/ Praktikum
1	0910012	Arsitektur dan Organisasi Komputer	2	
2	0910022	Sistem Operasi	2	
3	0910032	Pengantar Keamanan Siber	2	
4	0910042	Struktur dan Literasi Data	2	
5	0910052	Kalkulus	2	
6	0000032	Pancasila	2	
7	0910062	Algoritma Pemrograman	2	
8	0911072	Prak. Arsitektur dan Organisasi Komputer		2
9	0911082	Prak. Algoritma Pemrograman		2
10	0911092	Prak. Sistem Operasi		2
<b>Jumlah Beban Studi</b>			<b>14</b>	<b>6</b>

SEMESTER II				
No	Kode MK	Mata Kuliah	Bobot SKS	
			Teori	Praktek/ Praktikum
1	0920103	Matematika Diskrit	3	
2	0920112	Hukum Keamanan Siber	2	
3	0920122	Jaringan Komputer	2	
4	0920132	Pengantar Teknologi Informasi	2	
5	0920143	Kecerdasan Buatan	3	
6	0000052	Bahasa Inggris	2	
7	0920152	Sistem Basis Data	2	
8	0921162	Prak. Jaringan Komputer		2
9	0921172	Prak. Sistem Basis Data		2
<b>Jumlah Beban Studi</b>			<b>16</b>	<b>4</b>

SEMESTER III				
No	Kode MK	Mata Kuliah	Bobot SKS	
			Teori	Praktek/ Praktikum
1	0930182	Administrasi Sistem Komputer dan Jaringan	2	
2	0930193	Keamanan Data dan Informasi	3	
3	0930203	Kriptografi	3	

<b>SEMESTER III</b>				
No	Kode MK	Mata Kuliah	Bobot SKS	
			Teori	Praktek/ Praktikum
4	0930212	Arsitektur Keamanan	2	
5	0930222	Keamanan Jaringan	2	
6	0930232	Etika Profesi	2	
7	0931242	Prak. Administrasi Sistem Komputer dan Jaringan		2
8	0931252	Prak. Arsitektur Keamanan		2
9	0931262	Prak. Keamanan Jaringan		2
<b>Jumlah Beban Studi</b>			<b>14</b>	<b>6</b>

<b>SEMESTER IV</b>				
No	Kode MK	Mata Kuliah	Bobot SKS	
			Teori	Praktek/ Praktikum
1	0940272	Keamanan Basis Data	2	
2	0940282	Pemrograman Keamanan Web	2	
3	0940292	Probabilitas dan Statistika	2	
4	0000042	Kewarganegaraan	2	
5	0000012	Agama	2	
6	0940302	Pemrograman Perangkat Bergerak	2	
7	0941312	Prak. Keamanan Basis Data		2
8	0941322	Prak. Pemrograman Keamanan Web		2
9	0941332	Prak. Pemrograman Perangkat Bergerak		2
10	0941342	Komunikasi Bahasa Inggris		2
<b>Jumlah Beban Studi</b>			<b>13</b>	<b>8</b>

<b>SEMESTER V</b>				
No	Kode MK	Mata Kuliah	Bobot SKS	
			Teori	Praktek/ Praktikum
1	0950352	Penetrasi Testing	2	
2	0000022	Bahasa Indonesia	2	
3	0950362	Pengujian Perangkat Lunak	2	
4	0950372	Keamanan Perangkat Bergerak	2	
5	0950382	Keamanan Web dan Cloud	2	
6	0950392	Keamanan Sistem Siber-Fisik	2	
7	0950402	Forensik Digital	2	
8	0951412	Prak. Penetrasi Testing		2
9	0951422	Prak. Pengujian Perangkat Lunak		2
10	0951432	Prak. Forensik Digital		2
<b>Jumlah Beban Studi</b>			<b>14</b>	<b>6</b>

SEMESTER VI				
No	Kode MK	Mata Kuliah	Bobot SKS	
			Teori	Praktek/ Praktikum
1	09614420	Magang Industri		20
2	0961453	Proyek Keamanan Siber		3
<b>Jumlah Beban Studi</b>				<b>23</b>

SEMESTER VII				
No	Kode MK	Mata Kuliah	Bobot SKS	
			Teori	Praktek/ Praktikum
<b>PILIHAN MBKM DI DALAM PT</b>				
1	0970462	Audit dan Tata Kelola Keamanan Siber	2	
2	0970473	Kepemimpinan dan Manajemen Proyek	3	
3	0000062	Kewirausahaan	2	
4	0970482	Manajemen Risiko TI	2	
5	0970492	Metode Penelitian	2	
6	0970503	Manajemen Bisnis	3	
7	0971513	Prak. Audit dan Tata Kelola Keamanan Siber		3
8	0971523	Prak. Manajemen Bisnis		3
<b>Jumlah Beban Studi</b>			<b>14</b>	<b>6</b>
<b>PILIHAN MBKM DI LUAR PT</b>				
1	09715320	Penelitian/Riset		20
2	09715410	Kewirausahaan		6 – 10
<b>Jumlah Beban Studi</b>				<b>26 – 30</b>

SEMESTER VIII				
No	Kode MK	Mata Kuliah	Bobot SKS	
			Teori	Praktek/ Praktikum
1	0981556	Tugas Akhir		6
2	0980562	Bahasa Inggris Dunia Kerja	2	
<b>Jumlah Beban Studi</b>			<b>2</b>	<b>6</b>

## X. RENCANA PEMBELAJARAN SEMSTER (RPS)

Penyusunan RPS dilakukan dengan memegang prinsip: 1) RPS adalah dokumen program pembelajaran yang dirancang untuk menghasilkan lulusan yang memiliki kemampuan sesuai CPL yang ditetapkan, sehingga harus dapat ditelusuri keterkaitan dan kesesuaian dengan konsep kurikulumnya; 2) Rancangan dititik beratkan pada bagaimana memandu mahasiswa belajar agar memiliki kemampuan sesuai dengan CP kepentingan kegiatan dosen mengajar; 3) Pembelajaran yang dirancang adalah pembelajaran yang berpusat pada mahasiswa (*student centred learning* disingkat SCL);

4) RPS wajib ditinjau dan disesuaikan secara berkala dengan perkembangan ilmu pengetahuan dan teknologi.

Rencana Pembelajaran Semester telah disusun sesuai dengan SN-Dikti Pasal 12 yang memuat: a) nama Program Studi, nama dan kode mata kuliah, semester, sks, nama dosen pengampu; b) capaian pembelajaran lulusan yang dibebankan pada mata kuliah; c) kemampuan akhir yang direncanakan pada tiap tahap pembelajaran untuk memenuhi capaian pembelajaran lulusan; d) bahan kajian yang terkait dengan kemampuan yang akan dicapai; e) metode pembelajaran; f) waktu yang disediakan untuk mencapai kemampuan pada tiap tahap pembelajaran; g) pengalaman belajar mahasiswa yang diwujudkan dalam deskripsi tugas yang harus dikerjakan oleh mahasiswa selama satu semester; h) kriteria, indikator, dan bobot penilaian; dan i) daftar referensi yang digunakan.