



KURIKULUM KURSUS DAN PELATIHAN KEAMANAN KOMPUTER JENJANG IV

Berbasis

Kerangka Kualifikasi Nasional Indonesia

Indonesian Qualification Framework



**DIREKTORAT PEMBINAAN KURSUS DAN PELATIHAN
DIREKTORAT JENDERAL PENDIDIKAN ANAK USIA DINI DAN
PENDIDIKAN MASYARAKAT
KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
2018**

KATA PENGANTAR

Puji dan syukur kami panjatkan kehadiran Tuhan Yang Maha Esa, karena berkat rahmat dan hidayah-Nya tim penyusun telah melewati berbagai tahapan dalam proses pembuatan Kurikulum Kursus dan Pelatihan berdasarkan Standar Kompetensi Lulusan (SKL) yang berbasis Kerangka Kualifikasi Nasional Indonesia (KKNI). Kurikulum ini diharapkan dapat diimplementasikan oleh Lembaga Kursus dan Pelatihan (LKP) dalam penyelenggaraan proses pembelajaran kursus dan pelatihan.

Kami mengucapkan terima kasih kepada penyusun yang telah mencurahkan pikiran, waktu dan tenaganya, sehingga kurikulum ini dapat diselesaikan dengan baik. Kami juga mengharapkan masukan atau saran yang konstruktif dari berbagai pihak sebagai bahan pertimbangan untuk menyempurnakannya di masa mendatang.

Jakarta, Desember 2018
Direktur,

Dr. Yusuf Muhyiddin, M.Pd
NIP 195901051986021001

DAFTAR ISI

	Halaman
DAFTAR ISI	ii
I. PENDAHULUAN	1
A. Latar Belakang	1
B. Tujuan	2
C. Dasar Hukum	3
D. Ruang Lingkup	3
II. KURIKULUM BERBASIS KERANGKA KUALIFIKASI NASIONAL INDONESIA (KKNI)	6
A. Profil Lulusan	6
B. Capaian Pembelajaran	6
C. Bahan Kajian	8
D. Daftar Modul	12
E. Rencana Pembelajaran Kursus dan Pelatihan (RPKP)	16
III. PENUTUP	33

I. PENDAHULUAN

A. Latar Belakang

Kerangka Kualifikasi Nasional Indonesia (KKNI) secara khusus dikembangkan untuk menjadi suatu rujukan nasional untuk meningkatkan mutu dan daya saing bangsa Indonesia di sektor sumber daya manusia. Pencapaian setiap tingkat kualifikasi sumber daya manusia Indonesia berhubungan langsung dengan tingkat capaian pembelajaran baik yang dihasilkan melalui sistem pendidikan maupun sistem pelatihan kerja yang dikembangkan dan diberlakukan secara nasional. Oleh karena itu upaya peningkatan mutu dan daya saing bangsa akan sekaligus pula memperkuat jati diri bangsa Indonesia.

KKNI merupakan salah satu langkah untuk mewujudkan mutu dan jati diri bangsa Indonesia dalam sektor sumber daya manusia yang dikaitkan dengan program pengembangan sistem pendidikan dan pelatihan secara nasional. Setiap tingkat kualifikasi yang dicakup dalam KKNI memiliki makna dan kesetaraan dengan capaian pembelajaran yang dimiliki setiap insan pekerja Indonesia dalam menciptakan hasil karya dan kontribusi yang bermutu di bidang pekerjaannya masing-masing.

Pada jalur pendidikan nonformal, salah satu infrastruktur yang penting dalam mencapai keselarasan mutu dan penjenjangan kualifikasi antara lulusan dari institusi penyelenggara kursus dan pelatihan dengan deskripsi kompetensi kerja yang diharapkan oleh pengguna lulusan adalah dokumen Standar Kompetensi Lulusan (SKL). Terkait dengan kepentingan yang strategis dan telah kuat aspek hukumnya, SKL disusun sebagai pelaksanaan amanah PP No. 32 Tahun 2013 tentang perubahan PP No. 19 Tahun 2005 tentang Standar Nasional Pendidikan, dan Permendiknas No. 47 Tahun 2010 tentang Standar Kompetensi Lulusan Kursus. Pada Tahun 2009, dokumen SKL untuk 16 bidang telah selesai disusun dan ditetapkan oleh Mendiknas tahun 2010. Selanjutnya, SKL 10

bidang kursus telah berhasil disusun tahun 2010 dan ditetapkan tahun 2012. Dengan terbitnya Peraturan Presiden No. 8 tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia, maka SKL yang telah disusun tersebut perlu dikaji keselarasannya dengan kualifikasi pada KKNI.

Kurikulum disusun sebagai pedoman pembelajaran bagi peserta didik pada lembaga kursus dan pelatihan. untuk mengembangkan kurikulum dalam pembelajaran kursus dan pelatihan perlu disusun kurikulum berbasis KKNI yang berguna untuk perencanaan, pelaksanaan, penilaian hasil, dan pengawasan pembelajaran kursus dan pelatihan dalam rangka menghasilkan lulusan yang bermutu.

B. Tujuan

1. Umum

Secara umum program kursus dan pelatihan keamanan komputer ini bertujuan untuk menghasilkan lulusan yang memiliki penguasaan, pengetahuan faktual, kemampuan kerja, serta memiliki hak dan tanggung jawab dalam bidang keamanan sistem komputer yang dibutuhkan sesuai bidang kerja jenjang empat, menerapkan pengetahuan standar dalam pengamanan sistem komputer meliputi pengamanan akses, basis data dan jaringan, serta memelihara dan melakukan pembaharuan terhadap pengamanan yang dilakukan terhadap sistem komputer sesuai dengan spesifikasi standar yang telah ditentukan.

2. Khusus

Secara khusus program kursus dan pelatihan keamanan komputer ini bertujuan untuk menghasilkan lulusan yang kompeten sebagai berikut:

- 1) Mampu memahami dan menjawab kebutuhan organisasi / perusahaan / lembaga terkait keamanan komputer.

- 2) Mampu melaksanakan tugas instalasi keamanan komputer meliputi:
 - a. Instalasi keamanan pada sistem operasi di sisi server dan pengguna (klien).
 - b. Konfigurasi keamanan jaringan.
 - c. Konfigurasi keamanan pada basis data.
- 3) Mampu melaksanakan pembaharuan otentikasi hak akses pada server dan perangkat jaringan secara berkala.
- 4) Mampu melaksanakan tugas pemeliharaan keamanan komputer.
- 5) Membuat laporan faktual secara tertulis terkait insiden keamanan sesuai format yang baku.

C. Dasar Hukum

1. Undang-Undang No. 20 Tahun 2003 tentang Sistem Pendidikan Nasional.
2. Peraturan Pemerintah No. 13 Tahun 2015 tentang Perubahan Kedua Atas Peraturan Pemerintah No. 19 Tahun 2005 tentang Standar Nasional Pendidikan.
3. Peraturan Presiden No. 8 Tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia.
4. Peraturan Menteri Pendidikan dan Kebudayaan No. 131 Tahun 2014 tentang Standar Kompetensi Lulusan Kursus dan Pelatihan.
5. Pedoman Penyusunan Kurikulum Kursus dan Pelatihan Tahun 2014.

D. Ruang Lingkup

1. Kurikulum dan pembelajaran

- a. Jenjang program kursus
Program kursus dan pelatihan keamanan komputer pemula ini merupakan jenjang IV KKNI, secara umum diharapkan

peserta mampu mengerjakan pekerjaan secara mandiri yang bersifat sederhana dan berulang-ulang.

b. Output lulusan

Program kursus dan pelatihan ini dirancang untuk membekali peserta didik agar memiliki penguasaan faktual, kemampuan kerja serta memiliki hak dan tanggung jawab dalam bidang sistem keamanan komputer sesuai kebutuhan, meliputi:

- i. Menerapkan prinsip keamanan untuk sistem operasi, basis data dan jaringan,
- ii. Melakukan pembaruan dan perawatan sistem keamanan komputer.

c. Jumlah durasi belajar

Durasi yang diperlukan peserta untuk mengikuti pelatihan keamanan komputer level pemula ini adalah 168 jam, terdiri dari 62 jam teori dan 106 jam praktik, dalam waktu \pm 3 bulan. 1 jam pelatihan = 45 menit.

d. Bobot bahan kajian

Bobot pelatihan keamanan komputer level IV adalah 107.

e. Perbandingan antara teori dan praktik

Perbandingan bobot teori dan praktik adalah 1:2.

2. Pendidik atau instruktur

Pendidik atau instruktur memiliki kualifikasi akademik minimal D4/S1 atau kualifikasi akademik dibawahnya yang memiliki kompetensi satu tingkat di atas keamanan komputer pemula serta memiliki pengalaman minimal 3 tahun di bidang pekerjaan keamanan komputer.

3. Sarana dan prasarana

Alat dan peralatan yang menunjang kegiatan pelatihan keamanan komputer pemula, antara lain:

- a. Perangkat keras
- b. Perangkat lunak
- c. Modul

d. Buku *operation & maintenance manual*

Prasarana yang menunjang pembelajaran, antara lain:

- a. Ruang teori
- b. Ruang praktik
- c. Ruang instruktur
- d. Ruang administrasi
- e. Ruang penyimpanan alat dan peralatan (*tools*)

II. KURIKULUM BERBASIS KERANGKA KUALIFIKASI NASIONAL INDONESIA

A. Profil Lulusan

Lulusan program kursus dan pelatihan keamanan komputer tingkat pemula ini menjadi administrator keamanan komputer (*network security*).

B. Capaian Pembelajaran

PARAMETER DESKRIPSI CAPAIAN PEMBELAJARAN KHUSUS BIDANG KEAMANAN KOMPUTER TINGKAT PEMULA SESUAI KKNI JENJANG IV	
SIKAP DAN TATA NILAI	<p>Membangun dan membentuk karakter dan kepribadian manusia Indonesia yang:</p> <ol style="list-style-type: none"> 1. Bertaqwa kepada Tuhan Yang Maha Esa. 2. Memiliki moral, etika dan kepribadian yang baik di dalam menyelesaikan tugasnya. 3. Berperan sebagai warga negara yang bangga dan cinta tanah air serta mendukung perdamaian dunia. 4. Mampu bekerja sama dan memiliki kepekaan sosial serta kepedulian yang tinggi terhadap masyarakat dan lingkungannya. 5. Menghargai keanekaragaman budaya, pandangan, kepercayaan, dan agama serta pendapat/temuan original orang lain. 6. Menjunjung tinggi penegakan hukum serta memiliki semangat untuk mendahulukan kepentingan bangsa serta masyarakat luas.
KEMAMPUAN DI BIDANG KERJA	<ol style="list-style-type: none"> 1. Mampu melaksanakan tugas instalasi keamanan komputer meliputi: <ol style="list-style-type: none"> a. Instalasi keamanan dasar pada sistem operasi disisi server dan klien; b. Mampu melakukan konfigurasi dasar keamanan jaringan; c. Konfigurasi dasar keamanan pada basis data. 2. Mampu melaksanakan tugas pemeliharaan keamanan komputer. 3. Melakukan pembaharuan otentikasi hak

	<p>akses pada server dan perangkat jaringan secara berkala.</p> <ol style="list-style-type: none"> 4. Mampu menangani serangan keamanan komputer yang bersifat <i>low attack</i>. 5. Mampu membuat laporan faktual secara tertulis terkait insiden keamanan sesuai format baku.
PENGETAHUAN YANG DIKUASAI	<p>Menguasai pengetahuan operasional yang lengkap, prinsip-prinsip serta konsep umum terkait dengan keamanan komputer jaringan yang mencakup hal-hal berikut:</p> <ol style="list-style-type: none"> 1. Mengetahui cara menyusun daftar kebutuhan untuk melakukan pemasangan topologi jaringan; 2. Mengetahui metode keamanan pada sistem operasi server; 3. Mengetahui metode keamanan pada sistem operasi klien; 4. Mengetahui metode keamanan basis data dan web; 5. Mengetahui aturan pada perangkat keamanan jaringan; 6. Mengetahui fakta jenis-jenis serangan pada komputer jaringan yang beresiko rendah; 7. Mengetahui urutan konfigurasi jaringan.
HAK DAN TANGGUNG JAWAB	<ol style="list-style-type: none"> 1. Bertanggung jawab dalam pemasangan, perawatan, dan penyelesaian masalah dasar untuk keamanan komputer sesuai dengan standar mutu. 2. Melakukan koordinasi antar anggota tim 3. Melindungi hak-hak stakeholder.

C. Bahan Kajian

BAHAN KAJIAN

Bidang Keterampilan : Keamanan Komputer

Jenjang : IV - KKNI (Teknisi Pemula)

ELEMEN KOMPETENSI	BAHAN KAJIAN	BOBOT	MODUL
Kemampuan di Bidang Kerja			
EK-K4-1 Mampu melaksanakan tugas memasang keamanan komputer.	BK-K4-1.1. Prosedur pemasangan keamanan pada sistem operasi disisi server dan klien:		MDK4-1 Konfigurasi pada keamanan komputer
	a. Konfigurasi akun pemakai	5	
	b. Konfigurasi antivirus	5	
	c. Konfigurasi kontrol akses	5	
	BK-K4-1.2. Prosedur pemasangan konfigurasi keamanan jaringan dasar pada:		MDK4-1 Konfigurasi pada keamanan komputer
	a. Hak akses jaringan	5	
	b. <i>Firewall</i>	5	
	c. <i>Virtual Private Network(VPN)</i>	5	
	d. Saluran terbuka (lapisan aplikasi, <i>transport</i> , dan <i>network</i>)	5	
	BK-K4-1.3. Prosedur konfigurasi dasar keamanan pada basis data		MDK4-1 Konfigurasi pada keamanan komputer
	a. Pembentukan akun pengguna	5	

ELEMEN KOMPETENSI	BAHAN KAJIAN	BOBOT	MODUL
	b. Pembatasan bagi pengguna untuk mengakses data	5	
	c. Pembuatan data cadangan dan pemulihan data	5	
EK-K4-2 Mampu melaksanakan tugas pemeliharaan keamanan komputer.	BK-K4-2.1. Fitur-fitur pada software antivirus	4	MDK4-2 Pemeliharaan pada keamanan komputer
	BK-K4-2.2. Fitur pencadangan konfigurasi firewall	4	MDK4-2 Pemeliharaan pada keamanan komputer
	BK-K4-2.3. Fitur pencadangan sistem operasi	4	MDK4-2 Pemeliharaan pada keamanan komputer
	BK-K4-2.4. Objek pemantauan jaringan (ketersediaan layanan jaringan, penyimpangan lalu lintas <i>broadcast</i> , <i>bottlenecks</i>)	4	MDK4-2 Pemeliharaan pada keamanan komputer
	BK-K4-2.5. Objek pemantauan server (<i>log files</i> , penggunaan memori, suhu dan penggunaan prosesor)	4	MDK4-2 Pemeliharaan pada keamanan komputer
EK-K4-3 Mampu melakukan pengecekan otentikasi hak akses secara berkala.	BK-K4-3. Kesesuaian hak akses dengan tugas dan fungsi pengguna	4	MDK4-2 Pemeliharaan pada keamanan komputer

ELEMEN KOMPETENSI	BAHAN KAJIAN	BOBOT	MODUL
EK-K4-4 Mampu menangani serangan kecil pada keamanan komputer.	BK-K4-4. Penanganan serangan komputer yang beresiko rendah yang dikeluarkan oleh lembaga internasional bidang kerentanan keamanan komputer	8	MDK4-3 Jenis-jenis dan penanggulangan serangan komputer
EK-K4-5. Mampu membuat laporan faktual secara tertulis terkait insiden keamanan sesuai format baku.	BK-K4-5. Cara penyusunan laporan faktual secara informatif dan tepat waktu	4	MDK4-4 Panduan menyusun laporan
Pengetahuan yang Dikuasai			
EK-P4-1. Mengetahui jenis dan perangkat keamanan jaringan	BK-P4-1. Nama, fungsi dan jenis perangkat keras dan perangkat lunak pada keamanan komputer	3	MDP4-1 Pengenalan Perangkat keras dan lunak pada keamanan komputer
EK-P4-2. Mengetahui metode keamanan sistem operasi untuk server	BK-P4-2. Jenis dan metode keamanan sistem operasi untuk server	2	MDP4-2 Jenis dan metode keamanan sistem operasi untuk server
EK-P4-3. Mengetahui metode keamanan pada sistem operasi klien	BK-P4-3. Jenis dan metode keamanan sistem operasi untuk klien	2	MDP4-3 Jenis dan metode keamanan sistem operasi untuk klien
EK-P4-4. Mengetahui metode keamanan basis data	BK-P4-4. Jenis dan metode keamanan basis data	2	MDP4-4 Jenis dan metode keamanan basis data

ELEMEN KOMPETENSI	BAHAN KAJIAN	BOBOT	MODUL
EK-P4-5. Mengetahui fakta jenis-jenis serangan komputer risiko rendah yang dikeluarkan oleh lembaga internasional bidang kerentanan keamanan komputer	BK-P4-5. Jenis-jenis serangan komputer risiko rendah yang dikeluarkan oleh lembaga internasional bidang kerentanan keamanan komputer	2	MDP4-5 Jenis-jenis serangan komputer
EK-P4-6. Mengetahui metode keamanan website	BK-P4-6. Jenis dan metode keamanan website	2	MDP4-6 Jenis dan metode keamanan website
EK-P4-7. Mengetahui metode keamanan pada aplikasi komputer	BK-P4-7. Jenis dan metode keamanan pada aplikasi komputer	2	MDP4-7 Jenis dan metode keamanan pada aplikasi komputer
Hak dan Tanggung Jawab			
EK-HTJ4-1. Bertanggung jawab dalam pemasangan, perawatan, dan penyelesaian masalah dasar untuk keamanan komputer sesuai dengan standar mutu	BK-HTJ4-1. Tanggungjawab Pekerjaan	2	MDHTJ4-1 Tanggung jawab Pekerjaan
EK-HTJ4-2. Melakukan koordinasi antar anggota tim	BK-HTJ4-2. Kordinasi Tim	2	MDHTJ4-2 Kordinasi Tim
EK-HTJ4-3. Melindungi hak-hak stakeholder	BK-HTJ4-3. Kerahasiaan Perusahaan	2	MDHTJ4-1 Kerahasiaan Perusahaan

D. Daftar Modul

DAFTAR MODUL

Bidang Keterampilan : Keamanan Komputer

Jenjang : IV – KKNI (Teknisi Pemula)

MODUL	BAHAN KAJIAN	BOBOT	DURASI (JAM)		
			Rincian		Total
			T	P	
MDK4-1 Konfigurasi pada keamanan komputer	BK-K4-1.1. Prosedur pemasangan keamanan pada sistem operasi disisi server dan klien:				
	a. Konfigurasi akun pemakai	5	2	6	8
	b. Konfigurasi antivirus	5	2	6	8
	c. Konfigurasi kontrol akses	5	2	6	8
	BK-K4-1.2. Prosedur pemasangan konfigurasi keamanan jaringan dasar pada:				
	a. Hak akses jaringan	5	2	10	12
	b. <i>Firewall</i>	5	2	10	12
	c. <i>Virtual Private Network(VPN)</i>	5	2	10	12
	d. Saluran terbuka (lapisan aplikasi, <i>transport</i> , dan <i>network</i>)	5	2	10	12
	BK-K4-1.3. Prosedur konfigurasi dasar keamanan pada basis data:				
	a. Pembentukan akun pengguna	5	2	6	8
	b. Pembatasan bagi pengguna untuk mengakses data	5	2	10	12

MODUL	BAHAN KAJIAN	BOBOT	DURASI (JAM)		
			Rincian		Total
			T	P	
	c. Pembuatan data cadangan dan pemulihan data	5	2	10	12
MDK4-2 Pemeliharaan pada keamanan komputer	BK-K4-2.1. Fitur-fitur pada software antivirus	4	1	1	2
	BK-K4-2.2. Fitur pencadangan konfigurasi firewall	4	1	3	4
	BK-K4-2.3. Fitur pencadangan sistem operasi	4	1	1	2
	BK-K4-2.4. Objek pemantauan jaringan (ketersediaan layanan jaringan, penyimpangan lalu lintas <i>broadcast</i> , <i>bottlenecks</i>)	4	1	3	4
	BK-K4-2.5. Objek pemantauan server (<i>log files</i> , penggunaan memori, suhu dan penggunaan prosesor)	4	1	3	4
MDK4-2 Pemeliharaan pada keamanan komputer	BK-K4-3. Kesesuaian hak akses dengan tugas dan fungsi pengguna	4	1	3	4
MDK4-3 Jenis-jenis dan penanggulangan serangan komputer	BK-K4-3. Penanggulangan serangan komputer yang beresiko rendah yang dikeluarkan oleh lembaga internasional bidang kerentanan keamanan komputer	8	2	6	8
MDK4-4 Panduan menyusun laporan	BK-K4-4. Cara penyusunan laporan faktual secara informatif dan	4	2	2	4

MODUL	BAHAN KAJIAN	BOBOT	DURASI (JAM)		
			Rincian		Total
			T	P	
	tepat waktu				
MDP4-1 Pengenalan Perangkat keras dan lunak pada keamanan komputer	BK-P4-1. Jenis dan fungsi perangkat keamanan jaringan	3	4	0	4
MDP4-2 Jenis dan metode keamanan sistem operasi untuk server	BK-P4-2. Jenis dan metode keamanan sistem operasi untuk server	2	4	0	4
MDP4-3 Jenis dan metode keamanan sistem operasi untuk klien	BK-P4-3. Jenis dan metode keamanan sistem operasi untuk klien	2	4	0	4
MDP4-4 Jenis dan metode keamanan basis data	BK-P4-4. Jenis dan metode keamanan basis data	2	4	0	4
MDP4-5 Jenis-jenis serangan komputer	BK-P4-5. Jenis-jenis serangan komputer risiko rendah yang dikeluarkan oleh lembaga internasional bidang kerentanan keamanan komputer	2	4	0	4
MDP4-6 Jenis dan metode keamanan website	BK-P4-6. Jenis dan metode keamanan website	2	4	0	4
MDP4-7 Jenis dan metode keamanan pada aplikasi komputer	BK-P4-7. Jenis dan metode keamanan pada aplikasi komputer	2	2	0	2

MODUL	BAHAN KAJIAN	BOBOT	DURASI (JAM)		
			Rincian		Total
			T	P	
MDHTJ4-1 Tanggungjawab Pekerjaan	BK-HTJ4-1. Tanggungjawab Pekerjaan	2	2	0	2
MDHTJ4-2 Kordinasi Tim	BK-HTJ4-2. Kordinasi Tim	2	2	0	2
MDHTJ4-3 Kerahasiaan Perusahaan	BK-HTJ4-3. Kerahasiaan Perusahaan	2	2	0	2
TOTAL		107	62	106	168

*Keterangan:

1 jam = 45 menit

T = Teori

P = Praktik

E. Rencana Pembelajaran Kursus dan Pelatihan (RPKP)**RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN****Bidang : Keamanan Komputer****Level : IV - KKNi****Waktu : 4 jam teori****Modul : Pengenalan Perangkat keras dan lunak pada keamanan komputer (MDP4-1)****Instruktur :**

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-1 (2 jam)	Nama, fungsi dan jenis perangkat keras dan perangkat lunak pada keamanan komputer	Teori: <ul style="list-style-type: none"> • Presentasi • Diskusi 	<ol style="list-style-type: none"> 1. Ketepatan siswa dalam mengidentifikasi nama, fungsi dan jenis perangkat keras dan perangkat lunak. 2. Diskusi tentang nama, fungsi dan jenis perangkat keras dan perangkat lunak dilakukan secara aktif dan cermat. 	3

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan Komputer
Level : IV - KKNi
Waktu : 4 jam teori
Modul : Jenis dan metode keamanan sistem operasi untuk server (MDP4-2)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-2 (4 jam)	Jenis dan metode keamanan sistem operasi untuk server	Teori: <ul style="list-style-type: none"> • Presentasi • Diskusi 	Ketepatan dalam menyebutkan metode keamanan sistem operasi untuk server.	2

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan Komputer
Level : IV - KKNi
Waktu : 4 jam teori
Modul : Jenis dan Metode keamanan sistem operasi untuk klien (MDP4-3)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-3 (4 jam)	Jenis dan metode keamanan sistem operasi untuk klien	Teori: <ul style="list-style-type: none"> • Presentasi • Diskusi 	1. Ketepatan dalam menyebutkan jenis keamanan sistem operasi untuk klien. 2. Ketepatan dalam menyebutkan metode keamanan sistem operasi untuk klien.	2

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan Komputer
Level : IV - KKNi
Waktu : 4 jam teori
Modul : Jenis dan metode keamanan basis data (MDP4-4)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-4 (4 jam)	Jenis dan metode keamanan basis data	Teori: <ul style="list-style-type: none"> • Presentasi • Diskusi 	1. Ketepatan dalam menyebutkan jenis keamanan basis data. 2. Ketepatan dalam menyebutkan metode keamanan basis data.	3

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan Komputer
Level : IV - KKNi
Waktu : 4 jam teori
Modul : Jenis-jenis serangan komputer (MDP4-5)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-5 (2 jam)	Jenis-jenis serangan komputer resiko rendah yang dikeluarkan oleh lembaga internasional bidang kerentanan keamanan komputer	Teori: <ul style="list-style-type: none"> • Presentasi • Diskusi 	1. Ketepatan dalam menyebutkan metode keamanan sistem operasi untuk server. 2. Ketepatan dalam menyebutkan jenis serangan komputer resiko rendah sesuai ketentuan lembaga internasional bidang kerentanan keamanan komputer.	2

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan Komputer
Level : IV - KKNi
Waktu : 4 jam teori
Modul : Jenis dan metode keamanan website (MDP4-6)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-6 H-7	Jenis dan metode keamanan situs web	Teori: <ul style="list-style-type: none"> • Presentasi • Diskusi 	1. Ketepatan dalam menyebutkan jenis keamanan situs web. 2. Ketepatan dalam menyebutkan metode keamanan situs web.	2

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan komputer
Level : IV - KKNi
Waktu : 2 jam teori
Modul : Jenis dan metode keamanan pada aplikasi komputer (MDP4-7)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-8 (2 jam)	Jenis dan metode keamanan pada aplikasi komputer	Teori: <ul style="list-style-type: none"> • Presentasi • Diskusi 	1. Ketepatan dalam menyebutkan jenis keamanan pada aplikasi komputer. 2. Ketepatan dalam menyebutkan metode keamanan pada aplikasi komputer.	2

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan komputer
Level : IV - KKNi
Waktu : 20 jam teori, 84 jam praktik
Modul : Konfigurasi pada keamanan komputer (MDK4-1)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
	Prosedur pemasangan keamanan pada sistem operasi di sisi server dan klien:	<ul style="list-style-type: none"> • Presentasi • Demonstrasi • Simulasi 		
H-9 H-10	a. Konfigurasi Akun pemakai		Ketepatan dalam melakukan konfigurasi akun pemakai secara berurutan	5
H-11 H-12	b. Konfigurasi antivirus		Ketepatan dalam melakukan konfigurasi antivirus secara berurutan	5
H-13 H-14	c. Konfigurasi kontrol akses		Ketepatan dalam melakukan konfigurasi kontrol akses secara berurutan	5
	Prosedur pemasangan konfigurasi keamanan jaringan dasar:	<ul style="list-style-type: none"> • Presentasi • Demonstrasi 		

H-15 H-16 H-17	a. Hak akses jaringan	<ul style="list-style-type: none"> • Simulasi 	Ketepatan dalam melakukan konfigurasi hak akses jaringan secara berurutan	5
H-18 H-19 H-20	b. Firewall		Ketepatan dalam melakukan konfigurasi firewall secara berurutan	5
H-21 H-22 H-23	c. <i>Virtual Private Network (VPN)</i>		Ketepatan dalam melakukan konfigurasi VPN secara berurutan	5
H-24 H-25 H-26	d. Saluran terbuka (lapisan aplikasi, <i>transport</i> , dan <i>network</i>)		Ketepatan dalam melakukan konfigurasi saluran terbuka secara berurutan	5
	Prosedur konfigurasi dasar keamanan pada basis data:	<ul style="list-style-type: none"> • Presentasi • Demonstrasi • Simulasi 		
H-27 H-28	a. Pembuatan akun pengguna		Ketepatan dalam melakukan konfigurasi pembuatan akun pengguna secara berurutan	5
H-29 H-30	b. Pembatasan bagi pengguna untuk mengakses data		Ketepatan dalam melakukan konfigurasi pembatasan pengguna dalam mengakses data secara berurutan	5
H-31 H-32	c. Pembuatan data cadangan dan pemulihan data		Ketepatan dalam melakukan konfigurasi pembuatan data cadangan dan pemulihan data secara berurutan	5

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan Komputer
Level : IV - KKNi
Waktu : 5 jam teori, 11 jam praktik
Modul : Pemeliharaan Pada Keamanan Komputer (MDK4-2)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-33	Fitur-fitur pada <i>software</i> antivirus	<ul style="list-style-type: none"> • Presentasi • Demonstrasi • Simulasi 	Ketepatan dalam melakukan pemindaian, pembersihan program perusak (<i>malicious software</i>) dan pembaharuan basis data antivirus secara berurutan dan benar.	4
H-34	Fitur pencadangan konfigurasi firewall	<ul style="list-style-type: none"> • Presentasi • Demonstrasi • Simulasi 	Ketepatan dalam melakukan pencadangan konfigurasi firewall secara berkala.	4
H-35	Fitur pencadangan sistem operasi	<ul style="list-style-type: none"> • Presentasi • Demonstrasi • Simulasi 	Ketepatan dalam melakukan pencadangan konfigurasi sistem operasi secara benar.	4
H-36	Objek pemantauan jaringan (ketersediaan layanan jaringan, penyimpanan	<ul style="list-style-type: none"> • Presentasi • Demonstrasi • Simulasi 	Ketepatan dalam memantau ketersediaan layanan jaringan.	4

	lalulintas <i>broadcast</i> , <i>bottleneck</i>)			
H-37	Obyek pemantauan server (<i>log files</i> , penggunaan memori, suhu dan penggunaan prosesor)	<ul style="list-style-type: none"> • Presentasi • Demonstrasi • Simulasi 	Ketepatan dalam memantau server.	4

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan komputer
Level : IV - KKNi
Waktu : 1 jam teori, 3 jam praktik
Modul : Pemeliharaan pada keamanan komputer (MDK4-2)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-38	Kesesuaian hak akses dengan tugas dan fungsi pengguna	<ul style="list-style-type: none"> • Presentasi • Demonstrasi • Simulasi 	Ketepatan dalam melakukan pengecekan otentifikasi hak akses pengguna terhadap server dan perangkat jaringan secara berurutan.	4

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan Komputer
Level : IV - KKNi
Waktu : 2 jam teori, 6 jam praktik
Modul : Jenis-jenis dan penanggulangan serangan komputer (MDK4-3)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-39 H-40	Penanggulangan serangan komputer yang beresiko rendah yang dikeluarkan oleh lembaga internasional bidang kerentanan keamanan komputer	<ul style="list-style-type: none"> • Presentasi • Demonstrasi • Simulasi 	Ketepatan dalam menangani serangan komputer resiko rendah secara berurutan.	8

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan Komputer
Level : IV - KKNi
Waktu : 2 jam teori, 2 jam praktik
Modul : Panduan menyusun laporan (MDK4-4)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-41	Cara penyusunan laporan faktual secara informatif dan tepat waktu	<ul style="list-style-type: none"> • Presentasi • Demontrasi • Simulasi 	Penyusunan laporan faktual dilakukan secara informatif dan tepat waktu.	4

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan komputer
Level : IV - KKNi
Waktu : 2 jam teori
Modul : Tanggungjawab pekerjaan (MDHTJ4-1)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-42	Tanggung jawab pekerjaan	Teori: <ul style="list-style-type: none"> • Presentasi • Diskusi 	1. Ketepatan mendelegasikan dengan jelas tanggung jawab yang harus dijalankan sesuai dengan prosedur. 2. Ketepatan mengkomunikasikan permasalahan keamanan jaringan tingkat lanjut pada tim sesuai prosedur.	2

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan komputer
Level : IV - KKNi
Waktu : 2 jam teori
Modul : Koordinasi Tim (MDHTJ4-2)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-43	Koordinasi tim	Teori: <ul style="list-style-type: none"> • Presentasi • Diskusi 	1. Menerapkan ruang lingkup masing-masing anggota tim secara sesuai. 2. Melakukan pendekatan kerjasama antar anggota tim secara benar dan tepat. 3. Memberikan umpan balik dari unjuk kerja sesuai dengan prosedur	2

RENCANA PEMBELAJARAN KURSUS DAN PELATIHAN

Bidang : Keamanan computer
Level : IV – KKNI
Waktu : 2 jam teori
Modul : Kerahasiaan Perusahaan (MDHTJ4-3)
Instruktur :

(1) HARI KE- (JAM)	(2) BAHAN KAJIAN	(3) METODE PEMBELAJARAN	(4) INDIKATOR KELULUSAN	(5) BOBOT NILAI
H-44	Kerahasiaan perusahaan	Teori: <ul style="list-style-type: none"> • Presentasi • Diskusi 	1. Menentukan integritas, kerahasiaan, keamanan dan ketersediaan informasi yang diperlukan oleh kebijakan organisasi dengan tepat. 2. Menjaga kerahasiaan dan hak kepemilikan para pemangku kepentingan dengan benar.	2

III. PENUTUP

Kurikulum berbasis kompetensi ini merupakan rangkaian rencana pembelajaran untuk dijadikan acuan dan diterapkan oleh Lembaga Kursus dan Pelatihan (LKP) dalam melaksanakan kegiatan pembelajaran pada bidang Keamanan Komputer jenjang IV.

Arah pengembangan kurikulum ini dapat disesuaikan dengan perkembangan kebutuhan dunia usaha dan industri (DUDI) dan dapat ditambahkan dengan muatan lokal sesuai dengan kebutuhan pada masing-masing LKP.

Dengan demikian, hasil yang diharapkan dari penerapan kurikulum berbasis kompetensi adalah lulusan yang memiliki kemampuan dan keterampilan pada bidang Keamanan Komputer pada jenjang IV yang memenuhi standar mutu dan mampu memenuhi kebutuhan pasar kerja, baik nasional maupun internasional.