KEMENTERIAN HUKUM REPUBLIK INDONESIA

KEPUTUSAN KEPALA BADAN PENGEMBANGAN SUMBER DAYA MANUSIA HUKUM
KEMENTERIAN HUKUM

NOMOR SDM-15.SM.02.02 TAHUN 2026

TENTANG
PEDOMAN PENYELENGGARAAN
PELATIHAN TEKNIS KEAMANAN SIBER

KEPALA BADAN PENGEMBANGAN SUMBER DAYA MANUSIA HUKUM
KEMENTERIAN HUKUM,

Menimbang :

a. bahwa dalam menyelenggarakan Pelatihan Teknis Keamanan Siber, perlu adanya Pedoman Penyelenggaraan Pelatihan.

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Keputusan Kepala Badan Pengembangan Sumber Daya Manusia Hukum Kementerian Hukum tentang Pedoman Penyelenggaraan Pelatihan Teknis Keamanan Siber

Mengingat :

1. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820);
2. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
4. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
5. Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 159);
6. Peraturan Presiden Nomor 155 tahun 2024 tentang Kementerian Hukum (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 351);
7. Peraturan Menteri Hukum Nomor 1 Tahun 2024 tentang Organisasi dan Tata Kerja Kementerian Hukum (Berita Negara Republik Indonesia Tahun 2024 Nomor 832);
8. Peraturan Menteri Hukum Nomor 35 Tahun 2025 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2025 Nomor 846);
9. Peraturan Menteri Hukum Nomor 1 Tahun 2026 tentang Pelaksanaan Pengembangan Kompetensi melalui Sistem Pembelajaran Terintegrasi di Bidang Hukum (Berita Negara Republik Indonesia Tahun 2026 Nomor 14);

10. Peraturan Menteri Hukum Republik Indonesia Nomor 2 Tahun 2026 Tentang Organisasi dan Tata Kerja Balai Pelatihan Hukum (Berita Negara Republik Indonesia Tahun 2026 Nomor 39);
11. Keputusan Menteri Hukum Nomor M.HH-8.PR.01.03 Tahun 2025 tentang Peta Jalan Pengembangan Kompetensi Sumber Daya Manusia Bidang Hukum Tahun 2025 – 2029.

MEMUTUSKAN :

Menetapkan : KEPUTUSAN KEPALA BADAN PENGEMBANGAN SUMBER DAYA MANUSIA HUKUM KEMENTERIAN HUKUM TENTANG PEDOMAN PENYELENGGARAAN PELATIHAN TEKNIS KEAMANAN SIBER.

KESATU : Penyelenggaraan Pelatihan Teknis Keamanan Siber menggunakan Model Pembelajaran Jarak Jauh, Klasikal, dan *Blended Learning*.

KEDUA : Pedoman Penyelenggaraan Pelatihan Keamanan Siber sebagaimana tercantum dalam Lampiran Keputusan ini.

KETIGA : Pedoman ini sebagai acuan dalam penyelenggaraan Pelatihan Teknis Keamanan Siber baik diselenggarakan oleh BPSDM Hukum dan atau Balai Pelatihan Hukum.

KEEMPAT : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Depok
pada tanggal 20 Februari 2026
KEPALA BADAN PENGEMBANGAN
SUMBER DAYA MANUSIA HUKUM,

GUSTI AYU PUTU SUWARDANI

Tembusan :
1. Menteri Hukum;
2. Kepala Lembaga Administrasi Negara Republik Indonesia;
3. Wakil Menteri Hukum;
4. Sekretaris Jenderal Kementerian Hukum;
5. Inspektur Jenderal Kementerian Hukum.

LAMPIRAN I
KEPUTUSAN KEPALA BPSDM HUKUM
NOMOR : SDM-15.SM.02.02 TAHUN 2026
TANGGAL : 20 FEBRUARI 2026

PEDOMAN PENYELENGGARAAN PELATIHAN TEKNIS KEAMANAN SIBER

BAB I PENDAHULUAN

A. LATAR BELAKANG

Penyelenggaraan pemerintahan saat ini sedang mengalami transformasi besar menuju Sistem Pemerintahan Berbasis Elektronik (SPBE) untuk mewujudkan tata kelola yang bersih, efektif, transparan, dan akuntabel. Namun, seiring dengan meningkatnya pemanfaatan teknologi informasi dan komunikasi, risiko dan ancaman keamanan siber terhadap infrastruktur pemerintah juga semakin kompleks.

Seiring dengan masifnya digitalisasi, lanskap ancaman siber di sektor publik juga semakin kompleks dengan munculnya berbagai pola serangan seperti malware, phishing, ransomware, hingga ancaman dari dalam (insider threat). Gangguan terhadap informasi dan dokumen elektronik tersebut tidak hanya berisiko merusak sistem, tetapi juga dapat mengganggu ketertiban umum serta melanggar hak konstitusional warga negara terkait perlindungan data pribadi. Oleh karena itu, setiap Aparatur Sipil Negara (ASN), terutama yang bertugas di bidang pengelolaan teknologi informasi dan media sosial instansi, memiliki tanggung jawab besar dalam menjaga keamanan serta integritas data publik yang dikelolanya.

Pelatihan Teknis Keamanan Siber ini diselenggarakan untuk memberikan pembekalan bagi ASN yang mengelola teknologi informasi dan media sosial untuk dapat memiliki kompetensi yang memadai tentang keamanan siber, mulai dari kemampuan manajemen identitas digital, pengamanan komunikasi data pemerintah, hingga teknik penyusunan rencana keamanan siber yang sesuai dengan standar kebijakan SPBE. Pelatihan ini juga mencakup simulasi penanganan dan pemulihan pasca-insiden untuk memastikan setiap instansi siap menghadapi gangguan siber secara terkoordinasi dan profesional.

B. TUJUAN DAN SASARAN

Pelatihan Teknis Keamanan Siber bertujuan memberikan pembekalan materi yang cukup bagi para peserta dalam menerapkan prinsip dan praktik keamanan siber untuk mendukung penyelenggaraan pemerintahan berbasis elektronik sesuai standar kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Peraturan Perundangan-Undangan yang berlaku. Adapun sasaran peserta pelatihan adalah Aparatur Sipil Negara (ASN) yang mengelola teknologi informasi dan media sosial dilingkungan Kementerian Hukum.

C. KOMPETENSI

Kompetensi yang dibangun pada Pelatihan Teknis Keamanan Siber adalah menerapkan prinsip dan praktik keamanan siber untuk mendukung penyelenggaraan pemerintahan berbasis elektronik sesuai standar kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Peraturan Perundangan-Undangan yang berlaku.

Adapun indikator keberhasilan dari pelatihan ini adalah peserta mampu:

1. Menjelaskan kebijakan pengembangan SDM serta nilai-nilai Pancasila;
2. Membangun komitmen belajar;
3. Menjelaskan konsep dasar, arah kebijakan, dan contoh penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) dalam pelayanan publik.;
4. Menjelaskan etika dan tanggung jawab ASN di lingkungan digital;
5. Menjelaskan konsep dan pentingnya keamanan siber dalam pemerintahan;
6. Mengidentifikasi jenis dan dampak ancaman siber pada instansi pemerintah;
7. Mempraktikkan pengelolaan identitas digital dan pengamanan akun ASN sesuai kebijakan keamanan yang berlaku;
8. Menjalankan prosedur pengamanan komunikasi dan data digital pemerintah;
9. Menyusun langkah-langkah penerapan keamanan siber di instansi sesuai pedoman SPBE;
10. Mensimulasikan penanganan insiden keamanan siber.

BAB II
KURIKULUM

Kurikulum Pelatihan Teknis Keamanan Siber secara keseluruhan terdiri dari 3 (tiga) Agenda Pembelajaran yang akan diberikan dalam 45 (empat puluh lima) Jam Pelajaran (JP).

A. Agenda Materi Pembelajaran

1. Agenda Materi Dasar/Wawasan

   Pada agenda materi ini peserta pelatihan dibekali pengetahuan dan pemahaman tentang Kebijakan Pengembangan SDM dan Penguatan Nilai Nilai Pancasila, serta *Building Learning Commitment* (BLC).

2. Agenda Materi Inti/Teknis

   Pada agenda materi ini peserta pelatihan dibekali pengetahuan, pemahaman dan keterampilan tentang Konsep Dasar dan Urgensi Keamanan Siber bagi ASN, Lanskap Ancaman Siber di Sektor Publik, Manajemen Identitas dan Keamanan Akun ASN, Pengamanan Komunikasi dan Data Digital Pemerintah, Penerapan Kebijakan dan SOP Keamanan Informasi Instansi, Simulasi Penanganan Insiden Keamanan Siber.

3. Agenda Materi Penunjang

   Pada agenda materi ini peserta pelatihan dibekali pengetahuan dan pemahaman tentang Pengenalan Transformasi Digital Pemerintahan dan SPBE dan Etika dan Tanggung Jawab ASN dalam Dunia Digital.

B. Ringkasan Materi Pelatihan

Penjelasan ringkasan mata pelatihan yang terdapat di masing-masing agenda pembelajaran adalah sebagai berikut:

1. Ringkasan Mata Pelatihan dalam Agenda Materi Dasar/Wawasan adalah sebagai berikut:

   a. Kebijakan Pengembangan SDM dan Penguatan Nilai-Nilai Pancasila

      1) Deskripsi Singkat

         Mata pelatihan ini membahas mengenai Kebijakan Pengembangan SDM dan Penguatan Nilai-Nilai Pancasila. Materi disajikan melalui ceramah sehingga diharapkan peserta mampu menjelaskan dasar hukum, isu aktual, arah dan strategi kebijakan pengembangan SDM dan mampu menjelaskan nilai-nilai serta implementasi pengamalan pancasila yang akan dievaluasi melalui Non Tes Penilaian Sikap.

      2) Hasil Belajar

         Setelah mengikuti pembelajaran ini, peserta mampu Setelah mengikuti pembelajaran ini, peserta mampu menjelaskan kebijakan pengembangan SDM aparatur dan nilai-nilai Pancasila.

      3) Indikator Hasil Belajar

         a) Menjelaskan dasar hukum, isu aktual, arah dan strategi kebijakan pengembangan SDM.

b) Menjelaskan nilai-nilai serta implementasi pengamalan Pancasila

4) Materi Pokok

Materi pokok pada mata pelatihan ini adalah:

a) Kebijakan Pengembangan SDM;

b) Penguatan Nilai-Nilai Pancasila;

5) Waktu

Alokasi waktu mata pelatihan ini adalah 2 Jam Pelajaran (JP).

b. *Building Learning Commitment* (BLC)

1) Deskripsi Singkat

Mata Pelatihan ini membahas Pengertian dan Proses Dinamika Kelompok, cara Membangun Kelompok Dinamis dan Kesepakatan Komitmen Belajar. Materi akan disampaikan melalui metode ceramah, curah pendapat, dan diskusi kelompok, sehingga peserta mampu menjelaskan pengertian dan proses dinamika kelompok serta dapat membangun kelompok yang dinamis serta dapat merumuskan komitmen belajar bersama yang efektif yang akan dievaluasi melalui Tes Non objektif Uraian dan Non Tes Penilaian Sikap.

2) Hasil Belajar

Setelah mengikuti pembelajaran ini, peserta mampu membangun komitmen belajar.

3) Indikator Hasil Belajar

a) Menjelaskan pengertian dan proses dinamika kelompok;

b) Membangun kelompok yang dinamis dan kesepakatan komitmen belajar bersama.

4) Materi Pokok

Materi pokok pada mata pelatihan ini adalah:

a) Pengertian dan Proses Dinamika Kelompok;

b) Kelompok Dinamis dan Kesepakatan Komitmen Belajar.

5) Waktu

Alokasi waktu mata pelatihan ini adalah 2 Jam Pelajaran (JP).

2. Ringkasan Mata Pelatihan dalam Agenda Materi Inti/Teknis adalah sebagai berikut:

a. Pengantar Keamanan Siber

1) Deskripsi Singkat

Mata pelatihan ini membahas pengertian dan prinsip dasar keamanan siber dan urgensi keamanan siber dalam penyelenggaraan pemerintahan digital. Materi akan disampaikan melalui metode ceramah dan curah pendapat, sehingga peserta mampu menjelaskan pengertian dan prinsip dasar keamanan siber dengan benar dan menjelaskan urgensi keamanan siber dalam mendukung penyelenggaraan pemerintahan digital yang akan dievaluasi melalui Tes Objektif pilihan ganda, Tes Non objektif Uraian dan Non Tes Penilaian Sikap.

2) Hasil Belajar

Setelah mengikuti pembelajaran ini, peserta mampu menjelaskan konsep dan pentingnya keamanan siber dalam pemerintahan.

3) Indikator Hasil Belajar
   a) Menjelaskan pengertian dan prinsip dasar keamanan siber;
   b) Menjelaskan urgensi keamanan siber dalam mendukung penyelenggaraan pemerintahan secara digital.
4) Materi Pokok

   Materi pokok pada mata pelatihan ini adalah:
   a) Pengertian dan prinsip dasar keamanan siber;
   b) Urgensi keamanan siber dalam penyelenggaraan pemerintahan secara digital.
5) Waktu

   Alokasi waktu mata pelatihan ini adalah 3 Jam Pelajaran (JP).

b. Lanskap Ancaman Siber di Sektor Publik
1) Deskripsi Singkat

   Mata pelatihan ini membahas Jenis dan pola ancaman siber terhadap instansi pemerintah dan Dampak serangan siber terhadap pelayanan publik. Materi disampaikan melalui metode ceramah, curah pendapat dan diskusi kelompok, sehingga peserta diharapkan dapat menjelaskan berbagai jenis dan pola ancaman siber yang dapat menyerang instansi pemerintah dan menjelaskan dampak serangan siber terhadap keberlangsungan dan kepercayaan layanan publik digital yang akan dievaluasi melalui Tes objektif pilihan ganda dan tes non objektif Uraian.
2) Hasil Belajar

   Setelah mengikuti pembelajaran ini, peserta mampu mengidentifikasi jenis dan dampak ancaman siber pada instansi pemerintah
3) Indikator Hasil Belajar
   a) Menjelaskan berbagai jenis dan pola ancaman siber yang dapat menyerang instansi pemerintah
   b) Menjelaskan dampak serangan siber terhadap keberlangsungan dan kepercayaan layanan publik digital.
4) Materi Pokok

   Materi pokok pada mata pelatihan ini adalah:
   a) Jenis dan pola ancaman siber terhadap instansi pemerintah;
   b) Dampak serangan siber terhadap pelayanan publik.
5) Waktu

   Alokasi waktu mata pelatihan ini adalah 3 Jam Pelajaran (JP).

c. Manajemen Identitas Digital dan Keamanan Akun
1) Deskripsi Singkat

   Mata pelatihan ini membahas Pengelolaan Identitas Digital, Autentikasi, dan Kontrol Akses serta Praktik terbaik dalam menjaga keamanan akun. Materi disampaikan melalui metode ceramah, curah pendapat, diskusi kelompok, studi kasus dan simulasi, sehingga Peserta mampu menjelaskan pengelolaan identitas

digital dan autentikasi serta mampu mempraktikkan prinsip autentikasi yang aman dalam penggunaan akun yang akan dievaluasi melalui Tes Objektif Pilihan Ganda, Tes Non objektif Uraian, Non Tes Unjuk Kerja dan Penilaian Sikap.

2) Hasil Belajar

Setelah mengikuti pembelajaran ini, peserta mampu mempraktikkan pengelolaan identitas digital dan pengamanan akun sesuai kebijakan keamanan yang berlaku.

3) Indikator Hasil Belajar

a) Menjelaskan Pengelolaan identitas digital dan autentikasi;

b) Mempraktikkan prinsip autentikasi yang aman dalam penggunaan akun.

4) Materi Pokok

Materi pokok pada mata pelatihan ini adalah:

a) Pengelolaan Identitas Digital, Autentikasi, dan Kontrol Akses.

b) Praktik terbaik dalam menjaga keamanan akun.

5) Waktu

Alokasi waktu mata pelatihan ini adalah 5 Jam Pelajaran (JP).

d. Pengamanan Komunikasi dan Data Digital Pemerintah

1) Deskripsi Singkat

Mata pelatihan ini membahas Pemahaman dan Penerapan Pengamanan Komunikasi dan Data Digital Pemerintah. Materi disampaikan melalui metode ceramah, curah pendapat, diskusi kelompok dan simulas sehingga Peserta mampu mampu Menjelaskan Konsep, Prinsip dan ruang lingkup perlindungan komunikasi dan data digital serta mampu menjalankan prosedur pengamanan komunikasi dan data digital pemerintah yang akan dievaluasi melalui Tes Objektif Pilihan Ganda, Tes Non objektif Uraian, Non Tes Unjuk Kerja dan Penilaian Sikap.

2) Hasil Belajar

Setelah mengikuti pembelajaran ini, peserta mampu menjalankan prosedur pengamanan komunikasi dan data digital pemerintah

3) Indikator Hasil Belajar

a) Menjelaskan Konsep, Prinsip dan ruang lingkup perlindungan komunikasi dan data digital;

b) Menjalankan prosedur pengamanan komunikasi. dan data digital.

4) Materi Pokok

Materi pokok pada mata pelatihan ini adalah:

a) Pemahaman Pengamanan Komunikasi dan Data Digital Pemerintah;

b) Penerapan pengamanan komunikasi. dan data digital.

5) Waktu

Alokasi waktu mata pelatihan ini adalah 9 Jam Pelajaran (JP).

e. Penyusunan Rencana Penerapan Keamanan Siber Pada Instansi

1) Deskripsi Singkat

Mata pelatihan ini membahas Prinsip dasar kebijakan keamanan informasi instansi dan Teknik penyusunan keamanan siber sesuai pedoman SPBE. Materi Disampaikan melalui metode ceramah, curah pendapat, diskusi kelompok dan

Insiden, sehingga peserta mampu menjelaskan prinsip dasar kebijakan keamanan informasi instansi dan mampu menerapkan langkah-langkah keamanan sesuai pedoman SPBE yang akan di evaluasi melalui Tes Objektif Pilihan Ganda, Tes Non objektif Uraian dan Non Tes Penilaian Sikap dan Produk.

2) Hasil Belajar

Setelah mengikuti pembelajaran ini, peserta diharapkan mampu menyusun langkah-langkah penerapan keamanan siber di instansi sesuai pedoman SPBE.

3) Indikator Hasil Belajar

a) Menjelaskan prinsip dasar kebijakan keamanan informasi instansi.

b) Menyusun langkah-langkah keamanan siber sesuai pedoman SPBE.

4) Materi Pokok

a) Prinsip dasar kebijakan keamanan informasi instansi;

b) Teknik penyusunan keamanan siber sesuai pedoman SPB.

5) waktu

Alokasi waktu mata pelatihan ini adalah 8 Jam Pelajaran (JP).

f. Simulasi Penanganan Insiden Keamanan Siber

1) Deskripsi Singkat

Mata pelatihan ini membahas Identifikasi dan Analisis Insiden Keamanan Siber dan Langkah Penanganan dan Pemulihan Pasca Insiden Siber. Materi Disampaikan melalui metode metode ceramah, curah pendapat, diskusi kelompok dan simulasi sehingga Peserta mampu mengidentifikasi jenis dan sumber insiden keamanan siber menggunakan metode dan alat analisis yang sesuai dan mampu melaksanakan prosedur penanganan dan pemulihan insiden siber secara terkoordinasi sesuai standar keamanan informasi yang akan dievaluasi melalui Tes Objektif Pilihan Ganda, Tes Non objektif Uraian, Non Tes Unjuk Kerja dan Penilaian Sikap.

2) Hasil Belajar

Setelah mengikuti pembelajaran ini, peserta diharapkan mampu mensimulasikan penanganan insiden keamanan siber.

3) Indikator Hasil Belajar

a) Mengidentifikasi jenis dan sumber insiden keamanan siber menggunakan metode dan alat analisis yang sesuai.

b) Melaksanakan prosedur penanganan dan pemulihan insiden siber secara terkoordinasi sesuai standar keamanan informasi.

4) Materi Pokok

a) Identifikasi dan Analisis Insiden Keamanan Siber;

b) Langkah Penanganan dan Pemulihan Pasca Insiden Siber.

5) waktu

Alokasi waktu mata pelatihan ini adalah 8 Jam Pelajaran (JP).

3. Ringkasan Mata Pelatihan dalam Agenda Penunjang adalah sebagai berikut:

a. Konsep, Kebijakan, dan Penerapan SPBE dalam Pelayanan Publik

1) Deskripsi Singkat

Mata pelatihan ini membahas Konsep Dasar dan Arah Kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE) , Manfaat transformasi digital dalam mendukung pelayanan publik, dan Penerapan SPBE dalam Pelaksanaan Tugas dan Fungsi Instansi Pemerinta. Materi akan disampaikan melalui metode ceramah, curah pendapat, dan diskusi kelompok, sehingga peserta mampu menjelaskan konsep dasar dan arah kebijakan SPBE, menguraikan manfaat transformasi digital melalui SPBE bagi pelayanan publik dan memberikan contoh penerapan SPBE di lingkup instansi yang akan dievaluasi melalui Tes Objektif pilihan ganda, Tes Non objektif Uraian dan Non Tes Penilaian Sikap.

2) Hasil Belajar

Setelah mengikuti pembelajaran ini, peserta mampu menjelaskan konsep dasar, arah kebijakan, dan contoh penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) dalam pelayanan publik..

3) Indikator Hasil Belajar

a) Menjelaskan konsep dasar dan arah kebijakan SPBE;
b) Menguraikan manfaat transformasi digital melalui SPBE bagi pelayanan publik.
c) Memberikan contoh penerapan SPBE di lingkup instansi.

4) Materi Pokok

a) Konsep Dasar dan Arah Kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE);
b) Manfaat transformasi digital dalam mendukung pelayanan publik;
c) Penerapan SPBE dalam Pelaksanaan Tugas dan Fungsi Instansi Pemerintah.

5) Waktu

Alokasi waktu mata pelatihan ini adalah 3 Jam Pelajaran (JP).

b. Etika dan Tanggung Jawab ASN dalam Dunia Digital

1) Deskripsi Singkat

Mata pelatihan ini membahas Etika dan Tanggung Jawab ASN dalam Dunia Digital dan Tanggung jawab ASN dalam menjaga keamanan dan integritas data publik. Materi akan disampaikan melalui metode ceramah dan curah pendapat, sehingga peserta mampu Menjelaskan Prinsip etika dan perilaku ASN di ruang digital dan mampu Menguraikan Tanggung jawab ASN dalam menjaga keamanan dan integritas data publik yang akan dievaluasi melalui Tes Objektif pilihan ganda, Tes Non objektif Uraian dan Non Tes Penilaian Sikap.

2) Hasil Belajar

Setelah mengikuti pembelajaran ini, peserta mampu menjelaskan etika dan tanggung jawab ASN di lingkungan digital.

3) Indikator Hasil Belajar

a) Menjelaskan Prinsip etika dan perilaku ASN di ruang digital;
b) Menguraikan Tanggung jawab ASN dalam menjaga keamanan dan integritas data publik.

4) Materi Pokok

a) Etika dan Tanggung Jawab ASN dalam Dunia Digital;

b) Tanggung jawab ASN dalam menjaga keamanan dan integritas data publik.

5) Waktu

Alokasi waktu mata pelatihan ini adalah 2 Jam Pelajaran (JP).

C. Struktur Mata Pelatihan dan JP

Struktur mata Pelatihan Teknis Keamanan Siber adalah sebagai berikut:

NO	MATA PELATIHAN	TEORI	PRAKTIK	LATIHAN	JAM PELAJARAN
I	AGENDA MATERI DASAR / WAWASAN				
1	Kebijakan Pengembangan SDM dan Penguatan Nilai-Nilai Pancasila.	2			2
2	*Building Learning Commitment* (BLC)	2			2
II.	AGENDA MATERI INTI / TEKNIS				
3	Pengantar Keamanan Siber	3			3
4	Lanskap Ancaman Siber di Sektor Publik	3			3
5	Manajemen Identitas Digital dan Keamanan Akun	3	2		5
6	Pengamanan Komunikasi dan Data Digital Pemerintah	4	5		9
7	Penyusunan Rencana Penerapan Keamanan Siber Pada Instansi	3	5		8
8	Simulasi Penanganan Insiden Keamanan Siber	2	6		8
III	AGENDA MATERI PENUNJANG				
9	Konsep, Kebijakan, dan Penerapan SPBE dalam Pelayanan Publik	3			3
10	Etika dan Tanggung Jawab ASN dalam Dunia Digital	2			2
	Total	27	18		45

D. Silabus Materi Pelatihan

Silabus materi Pelatihan Teknis Keamanan Siber adalah sebagai berikut:

NO	MATA PELATIHAN	SILABUS	JUMLAH JP
I.	AGENDA MATERI DASAR / WAWASAN		
1	Kebijakan Pengembangan SDM dan Penguatan Nilai-Nilai Pancasila.	1. Kebijakan pengembangan SDM 1.1. Pengertian dan tujuan kebijakan pengembangan SDM Aparatur; 1.2. Jenis-jenis kebijakan penyelenggaraan pengembangan kompetensi SDM aparatur di Kementerian Hukum. 2. Penguatan nilai-nilai Pancasila	2

NO	MATA PELATIHAN	SILABUS	JUMLAH JP
		2.1. Nilai-nilai Pancasila; 2.2. Implementasi nilai-nilai Pancasila.	
2	*Building Learning Commitment* (BLC)	1. Pengertian dan Proses dinamika kelompok 1.1 Pengertian dinamika kelompok; 1.2 Mengenal diri sendiri; 1.3 Mengenal orang lain. 2. Kelompok dinamis dan kesepakatan komitmen belajar 2.1. Pengertian kelompok; 2.2. Teori dan tahap pembentukan kelompok; 2.3. Pengenalan dan membangun kerjasama; 2.4. Komitmen Belajar.	2
II.	AGENDA MATERI INTI / TEKNIS		
3	Pengantar Keamanan Siber	1. Pengertian, tujuan, fungsi dan prinsip dasar keamanan siber. 1.1. Konsep dasar dan ruang lingkup keamanan siber 1.2. Tujuan dan fungsi keamanan siber dalam organisasi 1.3. Prinsip-prinsip dasar keamanan siber (kerahasiaan, integritas, ketersediaan) 2. Urgensi keamanan siber dalam penyelenggaraan pemerintahan secara digital 2.1. Tantangan dan ancaman siber dalam penyelenggaraan pemerintahan digital 2.2. Dampak pelanggaran keamanan siber terhadap layanan publik 2.3. Peran ASN dalam menjaga keamanan siber pemerintahan	3
4	Lanskap Ancaman Siber di Sektor Publik	1. Jenis dan pola ancaman siber terhadap instansi pemerintah. 1.1. Klasifikasi ancaman siber (malware, phishing, ransomware, DDoS, insider threat, dll.) 1.2. Pola dan tren serangan siber yang umum terjadi di sektor publik 1.3. Faktor penyebab kerentanan sistem pemerintahan terhadap serangan siber 2. Dampak serangan siber terhadap pelayanan publik. 2.1. Dampak serangan siber terhadap ketersediaan dan keandalan layanan publik digital 2.2. Konsekuensi kebocoran data dan kehilangan kepercayaan masyarakat	3

NO	MATA PELATIHAN	SILABUS	JUMLAH JP
		2.3. Contoh kasus serangan siber pada lembaga pemerintahan dan pelajarannya	
5	Manajemen Identitas Digital dan Keamanan Akun	1. Pengelolaan Identitas Digital, Autentikasi, dan Kontrol Akses 1.1. Konsep dan Komponen Identitas Digital ASN; 1.2. Kebijakan dan Regulasi Pengelolaan Identitas Digital ASN; 1.3. Prinsip dan Mekanisme Autentikasi yang Aman; 1.4. Manajemen Akses dan Kontrol Keamanan Akun berbasis peran (role-based access). 2. Praktik terbaik dalam menjaga keamanan akun 2.1. Pengaturan Kata Sandi yang Aman 2.2. Penerapan Multi-Factor Authentication (MFA) 2.3. Pengelolaan Perangkat dan Sesi Login 2.4. Identifikasi dan Penanganan Ancaman terhadap Akun	5
6	Pengamanan Komunikasi dan Data Digital Pemerintah	1. Pemahaman Pengamanan Komunikasi dan Data Digital Pemerintah 1.1. Konsep dan Ruang Lingkup Pengamanan Komunikasi dan Data Digital Pemerintah; 1.2. Kebijakan dan Standar Keamanan Pengamanan Komunikasi dan Data Digital; 1.3. Ancaman dan Risiko terhadap Komunikasi dan Data Digital 2. Penerapan pengamanan komunikasi. dan data digital. 2.1. Pengamanan email dinas; 2.2. Pengamanan komunikasi melalui aplikasi perpesanan dan rapat daring 2.3. Pengamanan pertukaran informasi dan dokumen digital 2.4. Pengamanan penyimpanan data pada perangkat kerja dan sistem informasi 2.5. Pencadangan (backup) dan pemulihan data	9
7	Penyusunan Rencana Penerapan Keamanan Siber Pada Instansi	1. Prinsip dasar kebijakan keamanan informasi instansi. 1.1. Konteks dan Urgensi Kebijakan Keamanan Informasi dalam SPBE 1.2. Prinsip Fundamental Keamanan Informasi	8

NO	MATA PELATIHAN	SILABUS	JUMLAH JP
		1.3. Implementasi Kebijakan Keamanan Informasi di lingkungan Kementerian Hukum 2. Teknik penyusunan keamanan siber sesuai pedoman SPBE. 1.1. Perencanaan dan Tata Kelola (Dasar Kebijakan) 1.2. Klasifikasi Data & Informasi 1.3. Manajemen Risiko SPBE 1.4. Penyusunan Kebijakan & SOP 1.5. Perlindungan Teknis Kontrol Akses (Access Control) 1.6. Enkripsi Data 1.7. Tanda Tangan Elektronik (TTE) 1.8. Operasional & Pemantauan 1.9. Backup & Recovery Data 1.10. Pemantauan & Penanganan Insiden 1.11. Audit Keamanan Berkala 1.12. Penguatan SDM	
8	Simulasi Penanganan Insiden Keamanan Siber	1. Identifikasi dan Analisis Insiden Keamanan Siber 1.1. Pengenalan jenis-jenis insiden keamanan siber 1.2. Teknik deteksi dini dan analisis sumber insiden 1.3. Penggunaan alat bantu (tools) monitoring dan log analisis 2. Langkah Penanganan dan Pemulihan Pasca Insiden Siber 1.1. Prosedur respon cepat terhadap insiden siber. 1.2. Koordinasi antar unit dalam proses mitigasi dan pemulihan. 1.3. Evaluasi insiden dan penyusunan rencana pencegahan berkelanjutan	8
III.	AGENDA MATERI PENUNJANG		
8	Konsep, Kebijakan, dan Penerapan SPBE dalam Pelayanan Publik	1. Konsep Dasar dan Arah Kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE) 1.1. Konsep dan arah kebijakan SPBE & Satu Data Indonesia. 1.2. Penerapan SPBE di Lingkungan Kementerian Hukum 2. Manfaat transformasi digital dalam mendukung pelayanan publik 2.1. Manfaat transformasi digital bagi pemerintah	3

NO	MATA PELATIHAN	SILABUS	JUMLAH JP
		2.2. Manfaat transformasi digital bagi masyarakat 3. Penerapan SPBE dalam Pelaksanaan Tugas dan Fungsi Instansi Pemerintah 3.1. Penerapan SPBE dalam manajemen dan administrasi perkantoran 3.2. Penerapan SPBE dalam pelayanan publik di lingkungan Kementerian Hukum	
9	Etika dan Tanggung Jawab ASN dalam Dunia Digital	1. Etika dan Tanggung Jawab ASN dalam Dunia Digital 1.1. Kode Etik ASN & Etika Bermedia Digital Bagi ASN 1.2. 4 Pilar Literasi Digital 2. Tanggung jawab ASN dalam menjaga keamanan dan integritas data publik. 2.1. Hak & Kewajiban ASN Di Era Digital 2.2. Perlindungan Data Pribadi (PDP) 2.3. Sanksi Disiplin dan Ancaman Pidana UU ITE	2

E. Jadwal Penyelenggaraan / *Sequence*

1. Metode Pembelajaran Klasikal

Hari 1	**Hari 2**
1. *Check-in*; 2. Pembukaan; 3. Kebijakan Pengembangan SDM dan Penguatan Nilai-Nilai Pancasila (2 JP) 4. Pengarahan Program (1 JP); 5. *Pre-Test* (1 JP);	1. *Building Learning Commitment* (BLC) (2 JP) 2. Konsep, Kebijakan, dan Penerapan SPBE dalam Pelayanan Publik (3 JP) 3. Etika dan Tanggung Jawab ASN dalam Dunia Digital (2 JP)
Hari 3	**Hari 4**
1. Konsep Dasar dan Urgensi Keamanan Siber (3 JP) 2. Lanskap Ancaman Siber di Sektor Publik (3 Jp) 3. Manajemen Identitas Digital dan Keamanan Akun (5 JP)	Pengamanan Komunikasi dan Data Digital Pemerintah (9 JP)
Hari 5	**Hari 6**
Penyusunan Rencana Penerapan Keamanan Siber Pada Instansi (8 JP)	Simulasi Penanganan Insiden Keamanan Siber (8 JP)
Hari 7	**Hari 8**
1. Ujian Komprehensif (60 Menit); 2. Ujian Praktik (6 JP)	1. Rapat Evaluasi 2. Penutupan

2. Metode Pembelajaran Jarak Jauh (PJJ)

Hari 1	Hari 2
1. Pembukaan; 2. Kebijakan Pengembangan SDM dan Penguatan Nilai-Nilai Pancasila (2 JP) 3. Pengarahan Program (1 JP); 4. *Pre-Test* (1 JP); 5. *Building Learning Commitment* (BLC) (2 JP)	1. Konsep, Kebijakan, dan Penerapan SPBE dalam Pelayanan Publik (3 JP) 2. Etika dan Tanggung Jawab ASN dalam Dunia Digital (2 JP) 3. Konsep Dasar dan Urgensi Keamanan Siber (3 JP)
Hari 3	**Hari 4**
1. Lanskap Ancaman Siber di Sektor Publik (3 Jp) 2. Manajemen Identitas Digital dan Keamanan Akun (5 JP)	Pengamanan Komunikasi dan Data Digital Pemerintah (9 JP)
Hari 5	**Hari 6**
Penyusunan Rencana Penerapan Keamanan Siber Pada Instansi (8 JP)	Simulasi Penanganan Insiden Keamanan Siber (8 JP)
Hari 7	**Hari 8**
1. Ujian Komprehensif (60 Menit); 2. Ujian Praktik (6 JP)	1. Rapat Evaluasi 2. Penutupan

3. Metode *Blended Learning*

Hari 1 (PJJ)	Hari 2 (PJJ)
1. Pengarahan Program (1 JP); 2. *Pre-Test* (1 JP); 3. Konsep, Kebijakan, dan Penerapan SPBE dalam Pelayanan Publik (3 JP)	1. Etika dan Tanggung Jawab ASN dalam Dunia Digital (2 JP) 2. Konsep Dasar dan Urgensi Keamanan Siber (3 JP)
Hari 3 (PJJ)	**Hari 4 (Klasikal)**
1. Lanskap Ancaman Siber di Sektor Publik (3 JP) 2. Manajemen Identitas Digital dan Keamanan Akun (5 JP)	1. *Check-In* 2. Pembukaan 3. Kebijakan Pengembangan SDM dan Penguatan Nilai-Nilai Pancasila (2 JP) 4. *Building Learning Commitment* (BLC) (2 JP)
Hari 5 (Klasikal)	**Hari 6 (Klasikal)**
Pengamanan Komunikasi dan Data Digital Pemerintah (9 JP)	Penyusunan Rencana Penerapan Keamanan Siber Pada Instansi (8 JP)

Hari 7 (Klasikal)	Hari 8 (Klasikal)
Simulasi Penanganan Insiden Keamanan Siber (8 JP)	1. Ujian Komprehensif (60 Menit); 2. Ujian Seminar (6 JP)
Hari 9 (Klasikal)	
1. Rapat Evaluasi 2. Penutupan	

Keterangan :

1. Ujian seminar dilakukan secara berkelompok;
2. Kegiatan pembelajaran metode otede klasikal dan PJJ 8 hari kerja. *Blended learning* 9 hari kerja (Sabtu dan Minggu Libur);
3. 1 JP = 45 Menit;

F. Media Pembelajaran

Media pembelajaran yang dipergunakan dalam proses pembelajaran virtual adalah:

a. LMS
b. Modul
c. Bahan tayang
d. Wifi / Internet
e. Zoom Meeting

BAB III
MANAJEMEN PENYELENGGARAAN PELATIHAN

A. Tahap Penyelenggaraan

Pembelajaran Pelatihan Teknis Keamanan Siber melalui 3 cara, untuk pembelajaran metode klasikal dan Jarak Jauh menggunakan 1 (satu) tahapan sedangkan untuk blended learning menggunakan 2 (tahapan), diawali dengan (PJJ) dan dilanjutkan dengan tatap muka (klasikal). Adapun metode penyampaian materinya menggunakan metode ceramah, diskusi kelompok, curah pendapat, studi kasus, roleplay, insiden dan simulasi.

B. Ruang Lingkup Manajemen Penyelenggaraan

Ruang lingkup manajemen penyelenggaraan Pelatihan Teknis Keamanan Siber meliputi:

1. Perencanaan pelaksanaan Pelatihan Keamanan Siber meliputi persiapan pelatihan, peserta, tenaga pelatihan, fasilitas dan pembiayaan;
2. Pelaksanaan Pelatihan Teknis Keamanan Siber meliputi lembaga penyelenggara pelatihan, mekanisme pelaksanaan, waktu pelaksanaan pelatihan, evaluasi, kode registrasi alumni (KRA),
3. Evaluasi Pelatihan Teknis Keamanan Siber meliputi evaluasi terhadap peserta, tenaga pengajar, penyelenggaraan pelatihan dan alumni peserta pelatihan

C. Perencanaan

1. Persiapan Pelatihan

Persiapan Pelatihan Teknis Keamanan Siber dilakukan melalui kegiatan sebagai berikut:

a. Pimpinan Lembaga Penyelenggara Pelatihan dalam hal ini BPSDM Hukum atau Balai Pelatihan Hukum merencanakan waktu pelaksanaan Pelatihan Teknis Keamanan Siber serta pembiayaannya
b. Lembaga Penyelenggara Pelatihan dalam hal ini BPSDM Hukum atau Balai Pelatihan Hukum berkoordinasi dengan Biro Kepegawaian terkait penentuan peserta Pelatihan Teknis Keamanan Siber
c. Lembaga Penyelenggara Pelatihan dalam hal ini BPSDM Hukum atau Balai Pelatihan Hukum dapat menyiapkan sarana dan prasarana pelatihan.

2. Peserta Pelatihan

a. Persyaratan Peserta

Sebelum mengikuti pelatihan, peserta harus memenuhi persyaratan sebagai berikut:

1) ASN di bidang Pengelolaan Teknologi Informasi atau media sosial instansi;
2) Memiliki latar belakang pendidikan di bidang komputer atau teknologi informasi.
3) Mendapatkan rekomendasi atau persetujuan dari pimpinan instansi yang bersangkutan;
4) Sanggup mengikuti pelatihan sampai dengan selesai;
5) Sehat jasmani dan rohani;
6) Sedang tidak dalam proses atau menjalani hukuman disiplin.

b. Jumlah Peserta

Jumlah peserta Pelatihan Teknis Keamanan Siber berjumlah 30 orang per angkatan.

c. Registrasi Peserta

Peserta melakukan registrasi melalui media pendaftaran yang ditentukan dengan melengkapi persyaratan sesuai ditetapkan.

d. Penetapan Peserta
   1) Calon peserta pelatihan berdasarkan Surat Kepala Biro Sumber Daya Manusia Sekretariat Jenderal Kementerian Hukum;
   2) Penetapan peserta dilakukan oleh Kepala BPSDM Hukum atau Kepala Balai Pelatihan Hukum.

3. Tenaga Pelatihan
   a. Jenis Tenaga Pelatihan
      1) Penceramah

         Merupakan orang yang memberikan wawasan pengetahuan dan/atau berbagi pengalaman sesuai dengan keahliannya kepada peserta.
      2) Pengajar

         Merupakan orang/tim sesuai bidang keahliannya yang memberikan informasi dan pengetahuan kepada peserta dalam suatu kegiatan pembelajaran.
      3) Pengelola dan Penyelenggara

         Merupakan pegawai ASN yang bertugas mengelola dan menyelenggarakan pelatihan.
      4) Penjamin Mutu

         Tim Penjamin Mutu Penyelenggara Pelatihan Badan Pengembangan Sumber Daya Manusia Hukum**.**
   b. Persyaratan Tenaga Pelatihan
      1) Penceramah
         a) Merupakan pejabat/pimpinan organisasi;
         b) Berpengalaman dibidang materi yang diampunya.
      2) Pengajar
         a) Widyaiswara/Pakar/Praktisi/Dosen/Pejabat struktural/JFT yang membidangi materi yang diampunya;
         b) Memiliki pengalaman teknis minimal 2 tahun pada bidang materi yang diampunya;
         c) Memiliki pengalaman mengajar.
      3) Pengelola dan Penyelenggara
         a) Memiliki sertifikat pengelola pelatihan (MOT) atau dokumen lain sejenis bagi pengelola pelatihan;
         b) Memiliki sertifikat penyelenggara (TOC) atau dokumen lain yang sejenis bagi penyelenggara pelatihan;
         c) Mendapat penugasan dari pimpinan Lembaga penyelenggara pelatihan.
      4) Penjamin Mutu

         Tim Penjamin Mutu Penyelenggara Pelatihan Badan Pengembangan Sumber Daya Manusia Hukum.

4. Fasilitas Pelatihan

   Sarana dan prasarana penyelenggaraan Pelatihan Teknis Keamanan Siber disiapkan untuk mendukung proses belajar sehingga kompetensi yang akan dibangun dapat tercapai secara efektif dan efisien.

5. Sarana Pelatihan

   Penyelenggaraan Pelatihan Teknis Keamanan Siber menggunakan sarana sebagai berikut :

   1. Kursi dan meja
   2. Komputer/Laptop
   3. Jaringan Internet
   4. *Zoom Meeting*
   5. LMS
   6. Modul / Bahan Tayang
   7. Video Pembelajaran
   8. Alat praktik/Peraga

6. Pembiayaan

   penyelenggaraan Pelatihan Teknis Keamanan Siber dibebankan oleh Lembaga Penyelenggara Pelatihan (BPSDM Hukum / Balai Pelatihan Hukum).

D. Pelaksanaan

1. Lembaga Penyelenggara Pelatihan

   Pelatihan Teknis Keamanan Siber diselenggarakan oleh :

   a. BPSDM Hukum, dan atau

   b. Balai Pelatihan Hukum

   Penyelenggara dapat bekerja sama dengan lembaga lainya yang sudah terakreditasi dalam penyelenggaraan Pelatihan Teknis Keamanan Siber.

2. Jadwal Pelaksanaan (dapat mengacu pada *Sequence*).

E. Evaluasi Pelatihan

1. Evaluasi terhadap Peserta

   Penilaian terhadap peserta meliputi evaluasi kehadiran dan sikap perilaku, ujian komprehensif, praktik dan seminar.

KOMPONEN EVALUASI PESERTA	BOBOT (%)
Pre-test	0%
Kehadiran dan Sikap Perilaku a. Dinilai oleh tenaga pengajar dengan bobot 15%; b. Dinilai oleh petugas kelas dengan bobot 5%.	20%
Ujian Komprehensif	20%
Penilaian Praktik dilakukan untuk materi a. Pengamanan Komunikasi dan Data Digital Pemerintah 10% b. Manajemen Identitas Digital dan Keamanan Akun dengan bobot 10% c. Simulasi Penanganan Insiden Keamanan Siber dengan bobot 10%	30%
Seminar: Rencana Penerapan Keamanan Siber Pada Instansi	30%

Jumlah	100%

a. Penilaian Kehadiran dan Sikap Perilaku

1) Penilaian Kehadiran dan Sikap Perilaku merupakan penilaian dari pengampu materi dan tim penyelenggara terhadap aktivitas peserta dalam mengikuti setiap sesi pembelajaran sesuai jadwal dengan bobot nilai 20%.
2) Penilaian kehadiran dan sikap perilaku dinilai oleh :
   a) tenaga pengajar dengan bobot 15%.
   b) petugas kelas dengan bobot 5%.

b. Ujian Komprehensif

Ujian Komprehensif diberikan kepada peserta untuk menilai pemahaman pada mata pelatihan agenda materi inti/teknis. Ujian Komprehensif menjadi komponen penilaian evaluasi peserta dengan bobot 20% dengan alokasi waktu 60 menit dan terdiri dari 30 soal pilihan ganda.

c. Penilaian Praktik

Penilaian praktik merupakan bentuk evaluasi yang menekankan pada kemampuan peserta dalam menerapkan pengetahuan dan keterampilan. Pengambilan penilaian praktik dilakukan saat proses pembelajaran. Penilaian Praktik dilakukan untuk materi Manajemen Identitas Digital dan Keamanan Akun dengan bobot 10%, Pengamanan Komunikasi dan Data Digital Pemerintah dengan bobot 10% dan Simulasi Penanganan Insiden Keamanan Siber dengan bobot 10%.

d. Seminar

Seminar merupakan tahap evaluasi akhir yang bertujuan untuk mengukur kemampuan peserta dalam menyusun serta mempresentasikan dokumen rencana pengamanan siber yang aplikatif bagi instansi asalnya. Seminar dilakukan secara berkelompok yang memiliki bobot penilaian sebesar 30%.

e. Rekapitulasi nilai kelulusan peserta sebagai berikut:

Dalam penilaian pelatihan ini, terdapat tiga komponen utama yaitu kehadiran & sikap perilaku, ujian komprehensif dan ujian praktik. Setiap komponen memiliki persentase penilaian yang menunjukkan bobot dalam keseluruhan evaluasi. Rekapitulasi nilai kelulusan peserta sebagai berikut

No	Nama Peserta	Kehadiran & Sikap Perilaku 20%	Ujian Komprehensif 20%	Praktik 30%	Seminar 30%	Total Nilai
1						
2						
3						

f. Remedial

Remedial diberikan kepada peserta yang belum memperoleh nilai diatas 70 pada evaluasi Ujian Komprehensif. Nilai yang diperoleh dari hasil remedial paling tinggi adalah 70,01. Bentuk dan format remedial ditentukan oleh penyelenggara pelatihan.

g. Kualifikasi Kelulusan

1) Untuk dapat dinyatakan lulus pelatihan, peserta harus memenuhi ketentuan sebagai berikut :
   a) Peserta wajib mengikuti seluruh sesi pembelajaran, kecuali apabila berhalangan dengan persetujuan penyelenggara pelatihan yang disertai surat keterangan dari Kepala Satuan Kerja;
   b) Kehadiran dalam sesi pembelajaran paling sedikit 95 % (Sembilan puluh lima persen) dari seluruh sesi pembelajaran;
   c) Memperoleh nilai rata-rata setiap komponen penilaian paling rendah kualifikasi cukup memuaskan (skor minimal 70,01).

2) Kualifikasi kelulusan peserta pelatihan ditetapkan sebagai berikut:

Kualifikasi	Skor
Sangat Memuaskan	90,01 – 100
Memuaskan	80,01 – 90
Cukup Memuaskan	70,01 – 80
Kurang Memuaskan	60,01 – 70
Tidak Memuaskan	<60

h. Sertifikat Pelatihan

Hal-hal yang berkaitan dengan sertifikat Pelatihan mengikuti ketentuan sebagai berikut:

1. Peserta yang telah menyelesaikan seluruh sesi pembelajaran dengan baik dalam pelatihan dan dinyatakan lulus, diberikan Sertifikat Pelatihan
2. Dalam hal peserta Pelatihan dinyatakan tidak lulus, diberikan surat keterangan telah mengikuti pelatihan
3. Sertifikat Pelatihan atau Surat Keterangan telah mengikuti pelatihan sebagaimana dimaksud pada point (1) dan (2) diberi nomor register dan ditandatangani oleh Kepala BPSDM Hukum

KEMENTERIAN HUKUM REPUBLIK INDONESIA

SERTIFIKAT PELATIHAN
NOMOR .....

Kementerian Hukum berdasarkan ....
..... menyatakan bahwa:

Nama	: .....
NIP	: .....
Tempat/Tanggal lahir	: .....
Pangkat/Golongan Ruang	: .....
Jabatan	: .....
Instansi/Unit kerja	: .....

Telah mengikuti.....
.....

Nama tempat, tanggal
Nama Jabatan,

(Tanda tangan dan cap)

Nama Lengkap

DAFTAR MATA PELAJARAN/PELATIHAN

I. Materi Dasar:
   1. .....
   2. .....
   3. dst.

II. Materi Inti:
   1. .....
   2. .....
   3. dst.

III. Materi Penunjang:
   1. .....
   2. .....
   3. dst.

Nama tempat, tanggal
Nama Jabatan,

(Tanda tangan dan cap)

Nama Lengkap

2. Evaluasi terhadap Penyelenggaraan

Evaluasi penyelenggaraan pelatihan dilakukan dengan mengukur kepuasan peserta terhadap :

1. Tenaga pengajar/Narasumber/Widyaiswara/Pemateri;
2. Materi Pembelajaran; dan
3. Penyelenggaraan Pelatihan

Evaluasi terhadap penyelenggaraan Pelatihan Teknis Keamanan Siber yang dilaksanakan dengan model pembelajaran klasikal / jarak jauh (PJJ) /*blended learning* mengacu kepada Keputusan Kepala Badan Pengembangan Sumber Daya Manusia Hukum dan Hak Asasi Manusia Republik Indonesia No.SDM-135.0T.02.02 Tahun 2022 Tentang Pedoman dan Instrumen Evaluasi Penyelenggaraan Pelatihan di Lingkungan Kementerian Hukum dan HAM, dengan rincian sebagai berikut :

a. Instrumen Evaluasi Pelatihan Model Pembelajaran PJJ :

No	DIMENSI	SUB DIMENSI	ITEM PERTANYAAN
1	Tenaga Pengajar/ Narasumber/ Widyaiswara/ Pemateri	Pengetahuan	Tenaga pengajar mampu menjawab pertanyaan dengan mudah dipahami di platform PJJ.
			Tenaga pengajar mampu menarik minat peserta dalam diskusi di platform pembelajaran jarak jauh (PJJ).
			Tenaga pengajar memiliki keahlian yang cukup di bidang terkait.
			Tenaga pengajar menyajikan penjelasan disertai contoh yang aplikatif dalam pekerjaan sehari-hari.
			Tenaga pengajar mampu menggunakan bahasa yang mudah dimengerti saat mengajar.
			Tenaga pengajar memiliki wawasan yang luas pada topik pembelajaran terkait.
			Penjelasan Tenaga pengajar meyakinkan dengan data yang disampaikan.
		Sikap	Tenaga pengajar mengapresiasi peserta yang open camera atau yang terlibat aktif dalam sesi pembelajaran di *platform* pembelajaran jarak jauh (PJJ).
			Saya belum menemukan hal yang baru pada materi yang disampaikan oleh Tenaga pengajar.
			Saya ingin mencari tahu lebih dalam mengenai materi yang disampaikan oleh Tenaga pengajar.
			Saya ragu untuk mengungkapkan pendapat atau bertanya saat sesi pembelajaran berlangsung.
		Perilaku	Tenaga pengajar memulai dan mengakhiri sesi tepat waktu.
			Tenaga pengajar menggunakan lebih dari 1 macam metode dalam menyampaikan materi (seperti ceramah, penggunaan aplikasi lain yang mendukung, voting, *chat box*, *games*, *quiz*, diskusi kelompok).

No	DIMENSI	SUB DIMENSI	ITEM PERTANYAAN
			Tenaga pengajar menampilkan diri dengan sesuai selama sesi pembelajaran di *platform* pembelajaran jarak jauh (PJJ).
			Tenaga pengajar memberikan pertanyaan-pertanyaan yang mengajak peserta berpartisipasi aktif dalam pembelajaran jarak jauh (PJJ).
			Metode penyampaian materi di pelatihan ini seru.
2	Materi Pembelajaran	Kelengkapan Modul Pembelajaran	Saya menerima Modul Pembelajaran yang memuat petunjuk penggunaan modul yang mudah dipahami.
			Modul Pembelajaran memuat latar belakang dilakukannya pelatihan yang mudah dipahami.
			Modul Pembelajaran memuat tujuan dan indikator hasil belajar yang jelas.
			Saya bisa menemukan garis besar dan rangkuman materi pada modul pembelajaran.
			Dalam modul pembelajaran terdapat lembar pengayaan dan latihan soal.
			Modul Pembelajaran menyertakan lembar evaluasi pembelajaran.
		Fungsi Modul Pembelajaran	Modul Pembelajaran memuat studi kasus yang relevan dengan topik pembelajaran
			Modul Pembelajaran menyediakan tempat untuk peserta memberikan pendapat atau analisis.
			Pada modul pembelajaran, terdapat sumber-sumber informasi lain yang bisa diakses terkait topik pembelajaran.
		Bahan Ajar yang Bervariasi, menarik dan atraktif	Bahan ajar yang diberikan menarik untuk disimak.
			Bahan ajar yang diberikan beragam (misalnya ppt, video, *podcas*t, artikel, dll).
		Bahan Ajar yang	Bahan ajar yang diberikan bisa membantu saya lebih paham dan terampil.

No	DIMENSI	SUB DIMENSI	ITEM PERTANYAAN
		Kontekstual	Bahan ajar yang diberikan mampu menjawab pertanyaan terkait pekerjaan sehari-hari.
			Bahan ajar memuat gambaran standar kualitas kerja yang diharapkan..
			Saya memiliki kendala dalam memahami bahan ajar yang diberikan.
3	Penyelenggaraan Pelatihan	Media dan Informasi Pelatihan	Saya mendapatkan informasi pemberitahuan resmi terkait kegiatan pelatihan yang akan diikuti.
			Penyelenggaraan pelatihan dilakukan secara mendadak.
		Administrasi dan Dokumentasi	Panitia menyediakan *link* untuk mengakses dokumentasi kegiatan pelatihan.
		Efektivitas *E-Meeting*	Kegiatan pelatihan melalui pembelajaran jarak jauh (PJJ) ini terselenggara tepat waktu sesuai jadwal.
			Materi pelatihan sesuai dengan *rundown* pelatihan yang diberikan
			Saya tidak mengalami kendala dalam menggunakan platform pembelajaran jarak jauh (PJJ).
			Saya dapat dengan mudah menggunakan fitur-fitur yang ada dalam platform pembelajaran jarak jauh (PJJ).
			Waktu *coffee break* dan ISHOMA yang diberikan kurang.
		Akses dan Jaringan Internet	Saya dapat mengikuti pembelajaran dengan baik dengan dukungan internet yang memadai.
		Kualitas Pelayanan Tim Penyelenggara	Kegiatan pelatihan ini disertai informasi yang jelas mengenai penanggung jawab yang bisa dihubungi saat terjadi kendala.
			Host memberikan respon yang efektif dalam penanganan masalah yang terjadi selama pembelajaran jarak jauh (PJJ).

b. Instrumen Evaluasi Pelatihan Model Pembelajaran Klasikal :

No	DIMENSI	SUB DIMENSI	ITEM PERTANYAAN
1	Tenaga Pengajar/ Narasumber/ Widyaiswara/ Pemateri	Pengetahuan	Menurut saya, Tenaga Pengajar menguasai topik yang dibawakan pada pelatihan ini.
			Tenaga Pengajar mampu menjawab pertanyaan dengan jelas.
			Tenaga Pengajar memiliki keahlian yang cukup terkait materi.
			Tenaga Pengajar mampu memancing diskusi pada pelatihan ini.
			Saya merasa contoh yang diberikan Tenaga Pengajar aplikatif dalam pekerjaan sehari- hari.
			Tenaga Pengajar mampu memberikan penjelasan yang meyakinkan dengan data yang disampaikan.
			Saya tidak mengalami kesulitan dalam memahami materi yang disampaikan oleh Tenaga Pengajar.
		Sikap	Saya merasa penasaran dengan materi yang disampaikan oleh Tenaga Pengajar.
			Saya merasa dihargai oleh Tenaga Pengajar.
			Saya belum menemukan inspirasi dari materi yang disampaikan oleh Tenaga Pengajar.
			Saya menghindari interaksi secara langsung dengan Tenaga Pengajar.
		Perilaku	Tenaga Pengajar memulai dan mengakhiri sesi tepat waktu.
			Tenaga Pengajar menggunakan lebih dari 1 macam metode dalam menyampaikan materi (seperti ceramah, video, artikel, games, *quiz*, diskusi kelompok).
			Tampilan Tenaga Pengajar sesuai

No	DIMENSI	SUB DIMENSI	ITEM PERTANYAAN
			dengan waktu dan tempat
			Menurut saya, cara penyampaian Tenaga Pengajar monoton.
			Tenaga Pengajar mampu memancing peserta untuk berpartisipasi aktif.
			Saya merasa Tenaga Pengajar berperilaku sopan.
2	Materi Pembelajaran	Kelengkapan Modul Pembelajaran	Saya menerima Modul Pembelajaran yang memuat petunjuk penggunaan modul yang mudah dipahami.
			Modul Pembelajaran memuat latar belakang dilakukannya pelatihan yang mudah dipahami.
			Modul Pembelajaran memuat tujuan dan indikator hasil belajar yang jelas.
			Saya bisa menemukan garis besar dan rangkuman materi pada modul pembelajaran.
			Dalam modul pembelajaran terdapat lembar pengayaan dan latihan soal.
			Modul Pembelajaran menyertakan lembar evaluasi pembelajaran.
		Fungsi Modul Pembelajaran	Modul Pembelajaran memuat studi kasus yang relevan dengan topik pembelajaran.
			Modul Pembelajaran menyediakan tempat untuk peserta memberikan pendapat atau analisis.
			Pada modul pembelajaran, terdapat sumber-sumber informasi lain yang bisa diakses terkait topik pembelajaran.
		Bahan Ajar yang Bervariasi, menarik dan atraktif	Bahan ajar yang diberikan menarik untuk disimak.
			Bahan ajar yang diberikan beragam (misalnya ppt, video, *podcast*, artikel, dll).
		Bahan Ajar yang	Saya merasa bahan ajar yang

No	DIMENSI	SUB DIMENSI	ITEM PERTANYAAN
		Kontekstual	diberikan membantu saya lebih paham dan terampil.
			Bahan ajar yang diberikan mampu menjawab pertanyaan terkait pekerjaan sehari-hari.
			Bahan ajar memuat gambaran standar kualitas kerja yang diharapkan secara teknis.
3	Penyelenggaraan Pelatihan	Media dan Informasi Pelatihan	Saya memiliki waktu yang cukup untuk mempersiapkan diri sebelum kegiatan pelatihan dimulai.
			Saya menerima informasi jadwal kegiatan pelatihan dengan lengkap.
		Konsumsi	Konsumsi yang disediakan oleh panitia memadai.
			Konsumsi yang disediakan oleh panitia bervariasi.
		Administrasi dan Dokumentasi	Tersedianya media untuk mengakses dokumentasi kegiatan pelatihan.
		Acara Penyelenggaraan	Kegiatan pelatihan ini terselenggara tepat waktu sesuai jadwal.
			Materi pelatihan sesuai dengan *rundown* pelatihan yang diberikan.
			Tenaga pengajar yang hadir sama dengan tenaga pengajar yang tertulis di *rundown* pelatihan.
		Sarana dan Prasarana	Semua alat bantu pembelajaran yang dibutuhkan berfungsi dengan baik.
			Asrama, ruang kelas, ruang makan, toilet dan prasarana lainnya layak pakai (berfungsi baik dan bersih)
			Kegiatan pelatihan berlangsung kondusif di tempat ini.
			Fasilitas olahraga, kesehatan dan tempat ibadah layak pakai (berfungsi baik dan bersih).
		Kualitas Pelayanan Tim Penyelenggara	Kegiatan Pelatihan ini disertai informasi penanggung jawab yang

No	DIMENSI	SUB DIMENSI	ITEM PERTANYAAN
			bisa dihubungi saat terjadi kendala.
			Panitia kegiatan pelatihan memberikan respon yang efektif dalam penanganan masalah yang terjadi.

c. Instrumen Evaluasi Pelatihan metode *Blended Learning*:

Untuk evaluasi pelatihan metode *Blended Learning* merupakan gabungan dari instrumen evaluasi pelatihan metode klasikal dan PJJ.

BAB IV
PENUTUP

Pedoman ini disusun sebagai panduan bagi penyelenggara Pelatihan Teknis Keamanan Siber di lingkungan BPSDM Hukum sebagai kompas operasional yang memastikan program pelatihan berjalan terstruktur, berkualitas, dan mencapai target yang diinginkan oleh *stakeholder* yang terlibat dalam penyelenggaran pelatihan ini seperti penyelenggara, tenaga pengajar maupun peserta pelatihan.

KEPALA BADAN PENGEMBANGAN
SUMBER DAYA MANUSIA HUKUM,

GUSTI AYU PUTU SUWARDANI

LAMPIRAN II
KEPUTUSAN KEPALA BPSDM HUKUM
NOMOR : SDM-15.SM.02.02 TAHUN 2026
TANGGAL : 20 FEBRUARI 2026

RANCANG BANGUN PROGRAM PELATIHAN (RBPP) &
RANCANG BANGUN PEMBELAJARAN MATA PELATIHAN (RBPMP)
PELATIHAN TEKNIS KEAMANAN SIBER
METODE PEMBELAJARAN KLASIKAL / PJJ / BLENDED LEARNING

RANCANG BANGUN PROGRAM PELATIHAN (RBPP)
PELATIHAN TEKNIS KEAMANAN SIBER

Nama Program Pelatihan	:	Pelatihan Teknis Keamanan Siber
Alokasi Waktu	:	45 JP @ 45 Menit = 2.025 menit
Deskripsi singkat	:	Pelatihan ini membekali peserta dengan kompetensi menerapkan prinsip dan praktik keamanan siber untuk mendukung penyelenggaraan pemerintahan berbasis elektronik sesuai standar kebijakan SPBE melalui pembelajaran terkait Konsep, Kebijakan, dan Penerapan SPBE dalam Pelayanan Publik, Etika dan Tanggung Jawab ASN dalam Dunia Digital, Pengantar Keamanan Siber, Lanskap Ancaman Siber di Sektor Publik, Manajemen Identitas Digital dan Keamanan Akun, Pengamanan Komunikasi dan Data Digital Pemerintah, Penyusunan Rencana Penerapan Keamanan Siber Pada Instansi, Simulasi Penanganan Insiden Keamanan Siberi. Metode pembelajaran meliputi Ceramah, Diskusi Kelompok, Studi Kasus, dan Simulasi. Adapun yang menjadi peserta adalah seluruh ASN dilingkungan Kementerian Hukum dibidang Pengelolaan Teknologi Informasi dan media sosial instansi.
Tujuan Program		
Kompetensi Dasar	:	Setelah mengikuti pelatihan peserta diharapkan mampu menerapkan prinsip dan praktik keamanan siber untuk mendukung penyelenggaraan pemerintahan berbasis elektronik sesuai standar kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Peraturan Perundangan-Undangan yang berlaku.
Indikator Keberhasilan	:	Pada akhir pelatihan Peserta dapat :

NO	INDIKATOR KEBERHASILAN	MATA PELATIHAN	POKOK BAHASAN	METODE	EVALUASI	ESTIMASI WAKTU
KELOMPOK MATERI DASAR / WAWASAN						
1	Menjelaskan kebijakan pengembangan SDM serta nilai-nilai Pancasila	Kebijakan Pengembangan SDM dan Penguatan Nilai-Nilai Pancasila.	1. KebijakanPengembangan SDM; 2. Penguatan Nilai- Nilai Pancasila.	Ceramah	Tes Non objektif: Uraian Non Tes: Penilaian	2 JP

					Sikap	
2	Membangun Komitmen Belajar	Building Learning Commitment (BLC)	1. Pengertian dan Proses dinamika kelompok; 2. Kelompok dinamis dan kesepakatan komitmen belajar.	1. Ceramah 2. Curah Pendapat 3. Diskusi Kelompok	Tes Non objektif: Uraian Non Tes: Penilaian Sikap	2 JP
KELOMPOK MATERI INTI						
3	Menjelaskan konsep dan pentingnya keamanan siber dalam pemerintahan	Pengantar Keamanan Siber	1. Pengertian dan prinsip dasar keamanan siber. 2. Urgensi keamanan siber dalam penyelenggaraan pemerintahan secara digital.	1. Ceramah 2. Curah Pendapat	Tes Objektif: Pilihan Ganda Non Tes: Penilaian Sikap	3 JP
4	Mengidentifikasi jenis dan dampak ancaman siber pada instansi pemerintah	Lanskap Ancaman Siber di Sektor Publik	1. Jenis dan pola ancaman siber terhadap instansi pemerintah. 2. Dampak serangan siber terhadap pelayanan publik.	1. Cerama 2. Curah Pendapat 3. Diskusi Kelompok	Tes Objektif: Pilihan Ganda Tes Non objektif: Uraian Non Tes: Penilaian Sikap	3 JP
5	Mempraktikkan pengelolaan identitas digital dan pengamanan akun sesuai kebijakan keamanan yang berlaku	Manajemen Identitas Digital dan Keamanan Akun	1. Pengelolaan Identitas Digital, Autentikasi, dan Kontrol Akses. 2. Praktik terbaik dalam menjaga keamanan akun.	1. Ceramah 2. Diskusi Kelompok 3. Studi Kasus 4. Simulasi	Tes Objektif: Pilihan Ganda Tes Non objektif: Uraian	5 JP

					Non Tes: ● Unjuk Kerja ● Penilaian Sikap	
6	Menjalankan prosedur pengamanan komunikasi dan data digital pemerintah	Pengamanan Komunikasi dan Data Digital Pemerintah	1. Pemahaman Pengamanan Komunikasi dan Data Digital Pemerintah. 2. Penerapan pengamanan komunikasi. dan data digital.	1. Ceramah 2. Diskusi Kelompok 3. Studi Kasus 4. Simulasi	Tes Objektif: Pilihan Ganda Tes Non objektif: Uraian Non Tes: ● Penilaian Sikap ● Unjuk Kerja	9 JP
7	Menyusun langkah-langkah penerapan keamanan siber di instansi sesuai pedoman SPBE	Penyusunan Rencana Penerapan Keamanan Siber Pada Instansi	1. Prinsip dasar kebijakan keamanan informasi instansi. 2. Teknik penyusunan keamanan siber sesuai pedoman SPBE.	1. Ceramah 2. Diskusi Kelompok 3. Studi Kasus 4. Insiden	Tes Objektif: Pilihan Ganda Tes Non objektif: Uraian Non Tes: Produk Penilaian Sikap	8 JP
8	Mensimulasikan penanganan insiden keamanan siber	Simulasi Penanganan Insiden Keamanan Siber	1. Identifikasi dan Analisis Insiden Keamanan Siber 2. Langkah Penanganan dan Pemulihan Pasca Insiden Siber	1. Ceramah 2. Diskusi Kelompok 3. Studi Kasus 4. Simulasi	Tes Objektif: Pilihan Ganda Tes Non objectif: Uraian	8 JP

					Non Tes: ● Unjuk Kerja ● Penilaian Sikap	
	KELOMPOK MATERI PENUNJANG					
9	Menjelaskan konsep dasar, arah kebijakan, dan contoh penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) dalam pelayanan publik.	Konsep, Kebijakan, dan Penerapan SPBE dalam Pelayanan Publik	1. Konsep Dasar dan Arah Kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE) 2. Manfaat transformasi digital dalam mendukung pelayanan public 3. Penerapan SPBE dalam Pelaksanaan Tugas dan Fungsi Instansi Pemerintah	1.Ceramah 2. Curah Pendapat 3.Diskusi Kelompok	Tes Objektif: Pilihan Ganda Tes Non objektif: Uraian Non Tes: Penilaian Sikap	3 JP
10	Menjelaskan etika dan tanggung jawab ASN di lingkungan digital	Etika dan Tanggung Jawab ASN dalam Dunia Digital	1. Prinsip etika dan perilaku ASN di ruang digital. 2. Tanggung jawab ASN dalam menjaga keamanan dan integritas data publik.	1.Ceramah 2. Curah Pendapat	Tes Objektif: Pilihan Ganda Tes Non objektif: Uraian Non Tes: Penilaian Sikap	2 JP
TOTAL JP pelatihan						45 JP

***Ket :** 1. Evaluasi Pembelajaran Tes Objektif dilaksanakan dalam bentuk : a. **pre-test** (di awal pembelajaran); b.**ujian komprehensif** (di akhir pembelajaran 60 menit) 2. Evaluasi Pembelajaran Non Tes Unjuk Kerja dilaksanakan dalam bentuk **Penilaian Praktik** untuk 3 materi berikut : a. Manajemen Identitas Digital dan Keamanan Akun b. Pengamanan Komunikasi dan Data Digital Pemerintah c. Simulasi Penanganan Insiden Keamanan Siber	

1. RANCANG BANGUN PEMBELAJARAN MATA PELATIHAN

1	Nama Pelatihan		:	Pelatihan Teknis Keamanan Siber
2	Mata Pelatihan		:	**Kebijakan Pengembangan SDM dan Penguatan Nilai-Nilai Pancasila**
3	Alokasi Waktu		:	2 JP = 90 menit
4	Deskripsi Singkat		:	Mata pelatihan ini membahas mengenai Kebijakan Pengembangan SDM dan Penguatan Nilai-Nilai Pancasila. Materi disajikan melalui ceramah sehingga diharapkan peserta mampu menjelaskan dasar hukum, isu aktual, arah dan strategi kebijkan pengembangan SDM dan mampu menjelaskan nilai-nilai serta implementasi pengamalan pancasila yang akan dievaluasi melalui Non Tes Penilaian Sikap dan Tes Non Objektif Uraian.
5	Tujuan Pembelajaran			
	a	Hasil belajar	:	Setelah mengikuti pembelajaran ini, peserta mampu menjelaskan kebijakan pengembangan SDM aparatur serta nilai-nilai Pancasila.
	b	Indikator Hasil belajar		Pada akhir pembelajaran diharapkan peserta dapat:

No	Indikator Hasil Belajar	Materi Pokok		Metode Pembelajaran	Alat Bantu Dan Media	Evaluasi	Estimasi Waktu (JP/Menit)				Referensi/ Keterangan
		Materi Pokok	Sub Materi Pokok				T	P	L	Total	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
1.	Menjelaskan dasar hukum, isu aktual, arah dan strategi kebijakan pengembangan SDM	Kebijakan Pengembangan SDM	1. Pengertian dan tujuan Kebijakan pengembangan SDM Aparatur; 2. Jenis-jenis Kebijakan Penyelengga	Ceramah	1. Slide 2. Presentasi (PPT) 3. Tayangan Video	Tes Non objektif: Uraian Non Tes: Penilaian Sikap	1			1	1. Peraturan Menteri Hukum Nomor 1 Tahun 2026 tentang Pelaksanaan Pengemban

			raan pengembangan kompetensi SDM Aparatur di Kementerian Hukum								gan Kompetensi melalui Sistem Pembelajaran Terintegrasi di Bidang Hukum; 2. Kepmen Hukum M.HH.3.PR.01.04 Tahun 2025 BPSDM Sebagai Kampus pancasila
2	Menjelaskan nilai-nilai serta implementasi pengamalan Pancasila	Penguatan Nilai-Nilai Pancasila	1. Nilai-nilai Pancasila 2. Implementasi Nilai-nilai Pancasila	Ceramah	1. Slide Presentasi (PPT) 2. Tayangan Video	Tes Non objektif: Uraian Non Tes: Penilaian Sikap	1			1	
Jumlah							**2**			**2**	

2. RANCANG BANGUN PEMBELAJARAN MATA PELATIHAN

1	Nama Pelatihan		:	Pelatihan Teknis Keamanan Siber
2	Mata Pelatihan		:	***Building Learning Commitment*** **(BLC)**
3	Alokasi Waktu		:	2 JP = 90 menit
4	Deskripsi Singkat		:	Mata Pelatihan ini membahas Pengertian dan Proses Dinamika Kelompok, cara Membangun Kelompok Dinamis dan Kesepakatan Komitmen Belajar. Materi akan disampaikan melalui metode ceramah, curah pendapat, dan diskusi kelompok, sehingga peserta mampu menjelaskan pengertian dan proses dinamika kelompok serta dapat membangun kelompok yang dinamis serta dapat merumuskan komitmen belajar bersama yang efektif yang akan dievaluasi melalui Tes Non Objektif Uraian dan Non Tes Penilaian Sikap.
5	Tujuan Pembelajaran			
	a	Hasil belajar	:	Setelah mengikuti pembelajaran ini, peserta mampu membangun komitmen belajar.
	b	Indikator Hasil belajar		Pada akhir pembelajaran diharapkan peserta dapat:

No	Indikator Hasil Belajar	Materi Pokok		Metode Pembelajaran	Alat Bantu Dan Media	Evaluasi	Estimasi Waktu (JP/Menit)				Referensi/ Keterangan
		Materi Pokok	Sub Materi Pokok				T	P	L	Total	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
1.	Menjelaskan pengertian dan proses dinamika kelompok	Pengertian dan Proses Dinamika Kelompok	1. Pengertian dinamika kelompok 2. Mengenal diri sendiri 3. Mengenal orang lain	1. Ceramah 2. Curah Pendapat 3. Diskusi Kelompok	1. Slide Presentasi (PPT) 2. Tayangan Video 3. Komputer	Tes Non objektif: Uraian Non Tes: Penilaian Sikap	1			1	Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 26 Tahun 2022 tentang Pelaksanaan Pengembang
2	Membangun kelompok	Kelompok Dinamis dan	1. Pengertian kelompok 2. Teori dan	1. Ceramah 2. Curah Pendapat	1. Slide Presentasi (PPT)	Tes Non objektif: Uraian	1			1	

	yang dinamis dan kesepakatan komitmen belajar bersama	Kesepakatan Komitmen Belajar	tahap pembentukan kelompok 3. Pengenalan dan membangun kerjasama 4. Komitmen belajar	3. Diskusi Kelompok	2. Tayangan Video 3. Komputer	Non Tes: Penilaian Sikap					an Kompetensi melalui Sistem Pembelajaran Terintegrasi
Jumlah							**2**			**2**	

3. RANCANG BANGUN PEMBELAJARAN MATA PELATIHAN

1	Nama Pelatihan		:	Pelatihan Teknis Keamanan Siber
2	Mata Pelatihan		:	**Pengantar Keamanan Siber**
3	Alokasi Waktu		:	3 JP @45 Menit = 135 menit
4	Deskripsi Singkat		:	Mata pelatihan ini membahas Pengertian, tujuan, fungsi dan prinsip dasar keamanan siber dan urgensi keamanan siber dalam penyelenggaraan pemerintahan secara digital. Materi akan disampaikan melalui metode ceramah dan curah pendapat, sehingga peserta mampu menjelaskan pengertian, tujuan, fungsi dan prinsip dasar keamanan siber dan menjelaskan urgensi keamanan siber dalam mendukung penyelenggaraan pemerintahan digital yang akan dievaluasi melalui Tes Objektif pilihan ganda, Tes Non objectif Uraian dan Non Tes Penilaian Sikap.
5	Tujuan Pembelajaran			
	a	Hasil belajar	:	Setelah mengikuti pembelajaran ini, peserta mampu menjelaskan konsep dan pentingnya keamanan siber dalam pemerintahan
	b	Indikator Hasil belajar		Pada akhir pembelajaran diharapkan peserta dapat:

No	Indikator Hasil Belajar	Materi Pokok		Metode Pembelajaran	Alat Bantu Dan Media	Evaluasi	Estimasi Waktu (JP/Menit)				Referensi/ Keterangan
		Materi Pokok	Sub Materi Pokok				T	P	L	Total	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
1.	Menjelaskan pengertian, tujuan, fungsi dan prinsip dasar keamanan siber.	Pengertian, tujuan, fungsi dan prinsip dasar keamanan siber.	1. Konsep dasar dan ruang lingkup keamanan siber 2. Tujuan dan fungsi keamanan	1.Ceramah 2.Curah Pendapat 1.	• Slide Presentasi (PPT) • Tayangan Video • Komputer	Tes Objektif: Pilihan Ganda	1			1	• Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-

			siber dalam organisasi 3. Prinsip-prinsip dasar keamanan siber			Tes Non objektif: Uraian Non Tes: Penilaian Sikap					Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
2	Menjelaskan urgensi keamanan siber dalam mendukung penyelenggaraan pemerintahan secara digital.	Urgensi keamanan siber dalam penyelenggaraan pemerintahan secara digital	1. Tantangan dan ancaman siber dalam penyelenggaraan pemerintahan digital 2. Dampak pelanggaran keamanan siber terhadap layanan publik 3. Peran ASN dalam menjaga keamanan siber pemerintahan	1.Ceramah 2.Curah Pendapat	• Slide Presentasi (PPT) • Tayangan Video • Komputer	Tes Objektif: Pilihan Ganda Tes Non objektif: Uraian Non Tes: Penilaian Sikap	2			2	• Perpres No. 95/2018 tentang SPBE. • Peraturan Presiden (Perpres) Nomor 39 Tahun 2019 tentang Satu Data Indonesia • Peraturan Presiden (Perpres) Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional

											• Peraturan Menteri Hukum Nomor 35 Tahun 2025 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik
Jumlah							**3**			**3**	

4. RANCANG BANGUN PEMBELAJARAN MATA PELATIHAN

1	Nama Pelatihan			:	Pelatihan Teknis Keamanan Siber
2	Mata Pelatihan			:	**Lanskap Ancaman Siber di Sektor Publik**
3	Alokasi Waktu			:	3 JP @45 menit = 135 menit
4	Deskripsi Singkat			:	Mata pelatihan ini membahas Jenis dan pola ancaman siber terhadap instansi pemerintah dan Dampak serangan siber terhadap pelayanan publik. Materi disampaikan melalui metode ceramah, curah pendapat dan diskusi kelompok, sehingga peserta diharapkan dapat menjelaskan berbagai jenis dan pola ancaman siber yang dapat menyerang instansi pemerintah dan menjelaskan dampak serangan siber terhadap keberlangsungan dan kepercayaan layanan publik digital yang akan dievaluasi melalui Tes objektif pilihan ganda dan tes non objektif Uraian.
5	Tujuan Pembelajaran				
	a	Hasil belajar		:	Setelah mengikuti pembelajaran ini, peserta mampu mengidentifikasi jenis dan dampak ancaman siber pada instansi pemerintah
	b	Indikator Hasil belajar			Pada akhir pembelajaran diharapkan peserta dapat:

No	Indikator Hasil Belajar	Materi Pokok		Metode Pembelajaran	Alat Bantu Dan Media	Evaluasi	Estimasi Waktu (JP/Menit)				Referensi/ Keterangan
		Materi Pokok	Sub Materi Pokok				T	P	L	Total	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
1.	Menjelaskan berbagai jenis dan pola ancaman siber yang dapat menyerang instansi pemerintah	Jenis dan pola ancaman siber terhadap instansi pemerintah.	1. Klasifikasi ancaman siber (malware, phishing, ransomware, DDoS, insider threat, dll.) 2. Pola dan tren serangan siber yang umum	1. Ceramah 2. Curah Pendapat 3. Diskusi Kelompok	• Slide Presentasi (PPT) • Tayangan Video • Komputer	Tes Objektif: Pilihan Ganda Tes Non objektif: Uraian	2			2	• Perpres No. 95/2018 tentang SPBE. • Peraturan Presiden (Perpres) Nomor 39 Tahun 2019 tentang

			terjadi di sektor public 3. Faktor penyebab kerentanan sistem pemerintahan terhadap serangan siber			Non Tes: Penilaian Sikap				Satu Data Indonesia • Peraturan Presiden (Perpres) Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional • Peraturan Menteri Hukum Nomor 35 Tahun 2025 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik
2.	Menjelaskan dampak serangan siber terhadap keberlangsungan dan kepercayaan layanan publik digital.	Dampak serangan siber terhadap pelayanan publik.	1. Dampak serangan siber terhadap ketersediaan dan keandalan layanan publik digital 2. Konsekuensi kebocoran data dan kehilangan kepercayaan masyarakat 3. Contoh kasus serangan siber pada lembaga pemerintahan dan pelajarannya	1.Ceramah 2.Curah Pendapat 3.Diskusi Kelompok	• Slide Presentasi (PPT) • Tayangan Video • Komputer	Tes Objektif: Pilihan Ganda Tes Non objektif: Uraikn Non Tes: Penilaian Sikap	1			1	
Jumlah							3			3	

5. RANCANG BANGUN PEMBELAJARAN MATA PELATIHAN

1	Nama Pelatihan		:	Pelatihan Teknis Keamanan Siber
2	Mata Pelatihan		:	**Manajemen Identitas Digital dan Keamanan Akun**
3	Alokasi Waktu		:	5 JP = 225 menit
4	Deskripsi Singkat		:	Mata pelatihan ini membahas Pengelolaan Identitas Digital, Autentikasi, dan Kontrol Akses serta Praktik terbaik dalam menjaga keamanan akun. Materi disampaikan melalui metode ceramah, curah pendapat, diskusi kelompok, studi kasus dan simulasi, sehingga Peserta mampu menjelaskan pengelolaan identitas digital dan autentikasi serta mampu mempraktikkan prinsip autentikasi yang aman dalam penggunaan akun yang akan dievaluasi melalui Tes Objektif Pilihan Ganda, Tes Non objektif Uraian, Non Tes Unjuk Kerja dan Penilaian Sikap.
5	Tujuan Pembelajaran			
	a	Hasil belajar	:	Setelah mengikuti pembelajaran ini, peserta mampu mempraktikkan pengelolaan identitas digital dan pengamanan akun sesuai kebijakan keamanan yang berlaku.
	b	Indikator Hasil belajar		Pada akhir pembelajaran diharapkan peserta dapat:

No	Indikator Hasil Belajar	Materi Pokok		Metode Pembelajaran	Alat Bantu Dan Media	Evaluasi	Estimasi Waktu (JP/Menit)				Referensi/ Keterangan
		Materi Pokok	Sub Materi Pokok				T	P	L	Total	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
1.	Menjelaskan pengelolaan identitas digital dan autentikasi	Pengelolaan Identitas Digital, Autentikasi, dan Kontrol Akses.	1. Konsep dan Komponen Identitas Digital ASN; 2. Kebijakan dan Regulasi Pengelolaan Identitas Digital ASN;	1.Ceramah 2.Curah Pendapat 3.Diskusi Kelompok 4.studi kasus	• Slide Presentasi (PPT) • Tayangan Video • Komputer	Tes Objektif: Pilihan Ganda Tes Non objectif: Uraian	2			2	• Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11

			3. Prinsip dan Mekanisme Autentikasi yang Aman; 4. Manajemen Akses dan Kontrol Keamanan Akun berbasis peran (role-based access).			Non Tes: Penilaian Sikap				Tahun 2008 tentang Informasi dan Transaksi Elektronik • Perpres No. 95/2018 tentang SPBE. • Peraturan Presiden (Perpres) Nomor 39 Tahun 2019 tentang Satu Data Indonesia • Peraturan Menteri Hukum Nomor 35 Tahun 2025 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik
2	Mempraktikkan prinsip autentikasi yang aman dalam penggunaan akun	Praktik terbaik dalam menjaga keamanan akun	1. Pengaturan Kata Sandi yang Aman 2. Penerapan Multi-Factor Authentication (MFA) 3. Pengelolaan Perangkat dan Sesi Login 4. Identifikasi dan Penanganan Ancaman terhadap Akun	1.Ceramah 2.Curah Pendapat 3.Diskusi Kelompok 4. Simulasi	• Slide Presentasi (PPT) • Tayangan Video • Komputer	Tes Objektif: Pilihan Ganda Tes Non objektif: Uraian Non Tes: • Unjuk Kerja • Penilaian Sikap	1	2		3	
Jumlah							**3**	**2**		**5**	

6. RANCANG BANGUN PEMBELAJARAN MATA PELATIHAN

1	Nama Pelatihan			:	Pelatihan Teknis Keamanan Siber
2	Mata Pelatihan			:	**Pengamanan Komunikasi dan Data Digital Pemerintah**
3	Alokasi Waktu			:	9 JP @45 menit = 405 menit
4	Deskripsi Singkat			:	Mata pelatihan ini membahas Pemahaman dan Penerapan Pengamanan Komunikasi dan Data Digital Pemerintah. Materi disampaikan melalui metode ceramah, curah pendapat, diskusi kelompok dan simulas sehingga Peserta mampu mampu Menjelaskan Konsep, Prinsip dan ruang lingkup perlindungan komunikasi dan data digital serta mampu menjalankan prosedur pengamanan komunikasi dan data digital pemerintah yang akan dievaluasi melalui Tes Objektif Pilihan Ganda, Tes Non objektif Uraian, Non Tes Unjuk Kerja dan Penilaian Sikap .
5	Tujuan Pembelajaran				
	a	Hasil belajar		:	Setelah mengikuti pembelajaran ini, peserta mampu menjalankan prosedur pengamanan komunikasi dan data digital pemerintah
	b	Indikator Hasil belajar			Pada akhir pembelajaran diharapkan peserta dapat:

No	Indikator Hasil Belajar	Materi Pokok		Metode Pembelajaran	Alat Bantu Dan Media	Evaluasi	Estimasi Waktu (JP/Menit)				Referensi/ Keterangan
		Materi Pokok	Sub Materi Pokok				T	P	L	Total	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
1.	Menjelaskan Konsep, Prinsip dan ruang lingkup perlindungan komunikasi dan data digital	Pemahaman Pengamanan Komunikasi dan Data Digital Pemerintah	1. Konsep dan Ruang Lingkup Pengamanan Komunikasi dan Data Digital Pemerintah; 2. Kebijakan dan Standar	1.Ceramah 2.Curah Pendapat 3.Diskusi Kelompok	• Slide Presentasi (PPT) • Tayangan Video Komputer	Tes Objektif: Pilihan Ganda Tes Non Objektif: Uraian	2			2	• Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11

			Keamanan Pengamanan Komunikasi dan Data Digital; 3. Ancaman dan Risiko terhadap Komunikasi dan Data Digital								Tahun 2008 tentang Informasi dan Transaksi Elektronik • Perpres No. 95/2018 tentang SPBE.
2	Menjalankan prosedur pengamanan komunikasi. dan data digital	Penerapan pengamanan komunikasi. dan data digital.	1. Pengamanan email dinas; 2. Pengamanan komunikasi melalui aplikasi perpesanan dan rapat daring 3. Pengamanan pertukaran informasi dan dokumen digital 4. Pengamanan penyimpanan data pada perangkat kerja dan	1.Ceramah 2.Curah Pendapat 3.Diskusi Kelompok 4.Simulasi	• Slide Presentasi (PPT) • Tayangan Video Komputer	Tes Objektif: Pilihan Ganda Tes Non Objektif: Uraian Non Tes: Unjuk Kerja Penilaian Sikap	2	5		7	• Peraturan Presiden (Perpres) Nomor 39 Tahun 2019 tentang Satu Data Indonesia • Peraturan Menteri Hukum Nomor 35 Tahun 2025 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik

			sistem informasi 5. Pencadangan (backup) dan pemulihan data								
Jumlah							**4**	**5**		**9**	

7. RANCANG BANGUN PEMBELAJARAN MATA PELATIHAN

1	Nama Pelatihan		:	Pelatihan Teknis Keamanan Siber
2	Mata Pelatihan		:	**Penyusunan Rencana Penerapan Keamanan Siber Pada Instansi**
3	Alokasi Waktu		:	8 JP @menit = 360 menit
4	Deskripsi Singkat		:	Mata pelatihan ini membahas Prinsip dasar kebijakan keamanan informasi instansi dan Teknik penyusunan keamanan siber sesuai pedoman SPBE. Materi Disampaikan melalui metode ceramah, curah pendapat, diskusi kelompok dan Insiden, sehingga peserta mampu menjelaskan prinsip dasar kebijakan keamanan informasi instansi dan mampu menerapkan langkah-langkah keamanan sesuai pedoman SPBE yang akan di evaluasi melalui Tes Objektif Pilihan Ganda, Tes Non objektif Uraian dan Non Tes Penilaian Sikap dan Produk.
5	Tujuan Pembelajaran			
	a	Hasil belajar	:	Setelah mengikuti pembelajaran ini, peserta mampu menyusun langkah-langkah penerapan keamanan siber di instansi sesuai pedoman SPBE.
	b	Indikator Hasil belajar		Pada akhir pembelajaran diharapkan peserta dapat:

No	Indikator Hasil Belajar	Materi Pokok		Metode Pembelajaran	Alat Bantu Dan Media	Evaluasi	Estimasi Waktu (JP/Menit)				Referensi/ Keterangan
		Materi Pokok	Sub Materi Pokok				T	P	L	Total	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
1.	Menjelaskan prinsip dasar kebijakan keamanan informasi instansi	Prinsip dasar kebijakan keamanan informasi instansi.	1. Konteks dan Urgensi Kebijakan Keamanan Informasi dalam SPBE 2. Prinsip Fundamental Keamanan Informasi	1.Ceramah 2.Curah Pendapat 3.Diskusi Kelompok	• Slide Presentasi (PPT) • Tayangan Video • Komputer	Tes Objektif: Pilihan Ganda Tes Non Objektif: Uraian	2			2	• Perpres No. 95/2018 tentang SPBE. • Peraturan Presiden (Perpres) Nomor 39 Tahun 2019 tentang Satu

			3. Implementasi Kebijakan Keamanan Informasi di lingkungan Kemenkum			Non Tes: Penilaian Sikap				• Data Indonesia • Peraturan Presiden (Perpres) Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional • Peraturan Menteri Hukum Nomor 35 Tahun 2025 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik
2	Menyusun langkah-langkah keamanan siber sesuai pedoman SPBE	Teknik penyusunan keamanan siber sesuai pedoman SPBE.	1. Perencanaan dan Tata Kelola (Dasar Kebijakan) 2. Klasifikasi Data & Informasi 3. Manajemen Risiko SPBE 4. Penyusunan Kebijakan & SOP 5. Perlindungan Teknis Kontrol Akses (Access Control) 6. Enkripsi Data 7. Tanda Tangan Elektronik (TTE) 8. Operasional & Pemantauan 9. Backup & Recovery Data	1.Ceramah 2.Curah Pendapat 3.Studi kasus	• Slide Presentasi (PPT) • Tayangan Video • Komputer	Tes Objektif: Pilihan Ganda Tes Non Objektif: Uraian Non Tes: • Produk • Penilaian Sikap	1	5		6	

			10. Pemantauan & Penanganan Insiden 11. Audit Keamanan Berkala 12. Penguatan SDM								
Jumlah							**3**	**5**		**8**	

8. RANCANG BANGUN PEMBELAJARAN MATA PELATIHAN

1	Nama Pelatihan		:	Pelatihan Teknis Keamanan Siber
2	Mata Pelatihan		:	**Simulasi Penanganan Insiden Keamanan Siber**
3	Alokasi Waktu		:	8 JP = 360 menit
4	Deskripsi Singkat		:	Mata pelatihan ini membahas Identifikasi dan Analisis Insiden Keamanan Siber dan Langkah Penanganan dan Pemulihan Pasca Insiden Siber. Materi Disampaikan melalui metode ceramah, curah pendapat, diskusi kelompok dan simulasi sehingga Peserta mampu mengidentifikasi jenis dan sumber insiden keamanan siber menggunakan metode dan alat analisis yang sesuai serta mampu melaksanakan prosedur penanganan dan pemulihan insiden siber secara terkoordinasi sesuai standar keamanan informasi yang akan dievaluasi melalui Tes Objektif Pilihan Ganda, Tes Non objektif Uraian, Non Tes Unjuk Kerja dan Penilaian Sikap.
5	Tujuan Pembelajaran			
	a	Hasil belajar	:	Setelah mengikuti pembelajaran ini, peserta mampu mensimulasikan penanganan insiden keamanan siber.
	b	Indikator Hasil belajar		Pada akhir pembelajaran diharapkan peserta dapat:

No	Indikator Hasil Belajar	Materi Pokok		Metode Pembelajaran	Alat Bantu Dan Media	Evaluasi	Estimasi Waktu (JP/Menit)				Referensi/ Keterangan
		Materi Pokok	Sub Materi Pokok				T	P	L	Total	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
1.	Mengidentifikasi jenis dan sumber insiden keamanan siber menggunakan metode dan alat analisis yang sesuai	Identifikasi dan Analisis Insiden Keamanan Siber	1. Pengenalan jenis-jenis insiden keamanan siber 2. Teknik deteksi dini dan analisis	1.Ceramah 2.Diskusi Kelompok 3.Studi Kasus 4.Simulasi	• Slide Presentasi (PPT) • Tayangan Video • Komputer Tools monitoring	Tes Objektif: Pilihan Ganda Tes Non Objektif: Uraian	1	3		4	• Perpres No. 95/2018 tentang SPBE. • Peraturan Presiden (Perpres) Nomor 39 Tahun 2019

			sumber insiden 3. Penggunaan alat bantu (tools) monitoring dan log analisis		dan log analisis	Non Tes: Unjuk Kerja Penilaian Sikap				• tentang Satu Data Indonesia • Peraturan Presiden (Perpres) Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional • Peraturan Menteri Hukum Nomor 35 Tahun 2025 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik
2	Melaksanakan prosedur penanganan dan pemulihan insiden siber secara terkoordinasi sesuai standar keamanan informasi	Langkah Penanganan dan Pemulihan Pasca Insiden Siber	1. Prosedur respons cepat terhadap insiden siber. 2. Koordinasi antar unit dalam proses mitigasi dan pemulihan. 3. Evaluasi insiden dan penyusunan rencana pencegahan berkelanjutan	1.Ceramah 2.Diskusi Kelompok 3.Studi Kasus 4.Simulasi	• Slide Presentasi (PPT) • Tayangan Video Komputer	Tes Objektif: Pilihan Ganda Tes Non Objektif: Uraian Non Tes: • Unjuk Kerja • Penilaian Sikap	1	3		4	
Jumlah							**3**	**5**		**8**	

9. RANCANG BANGUN PEMBELAJARAN MATA PELATIHAN

1	Nama Pelatihan		:	Pelatihan Teknis Keamanan Siber
2	Mata Pelatihan		:	**Konsep, Kebijakan, dan Penerapan SPBE dalam Pelayanan Publik**
3	Alokasi Waktu		:	3 JP @45 menit = 135 menit
4	Deskripsi Singkat		:	Mata pelatihan ini membahas Konsep Dasar dan Arah Kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE) , Manfaat transformasi digital dalam mendukung pelayanan publik, dan Penerapan SPBE dalam Pelaksanaan Tugas dan Fungsi Instansi Pemerintah. Materi akan disampaikan melalui metode ceramah, curah pendapat, dan diskusi kelompok, sehingga peserta mampu menjelaskan konsep dasar dan arah kebijakan SPBE, menguraikan manfaat transformasi digital melalui SPBE bagi pelayanan publik dan memberikan contoh penerapan SPBE di lingkup instansi yang akan dievaluasi melalui Tes Objektif pilihan ganda, Tes Non objektif Uraian dan Non Tes Penilaian Sikap.
5	Tujuan Pembelajaran			
	a	Hasil belajar	:	Setelah mengikuti pembelajaran ini, peserta mampu menjelaskan konsep dasar, arah kebijakan, dan contoh penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) dalam pelayanan publik.
	b	Indikator Hasil belajar		Pada akhir pembelajaran diharapkan peserta dapat:

No	Indikator Hasil Belajar	Materi Pokok		Metode Pembelajaran	Alat Bantu Dan Media	Evaluasi	Estimasi Waktu (JP/Menit)				Referensi/ Keterangan
		Materi Pokok	Sub Materi Pokok				T	P	L	Total	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
1.	Menjelaskan konsep dasar dan arah kebijakan SPBE.	Konsep Dasar dan Arah Kebijakan Sistem Pemerintahan Berbasis	1. Konsep dan arah kebijakan SPBE & Satu Data Indonesia. 2. Penerapan SPBE di Lingkungan	• Ceramah • Curah Pendapat	• Slide Presentasi (PPT) • Tayangan Video Komputer	Tes : Objektif : Pilihan Ganda Non Objektif: Jawaban Singkat	1			1	• Perpres No. 95/2018 tentang SPBE. • Peraturan Presiden (Perpres) Nomor 39 Tahun 2019

		Elektronik (SPBE)	Kementerian Hukum			Non Tes: Penilaian Sikap					tentang Satu Data Indonesia • Peraturan Presiden (Perpres) Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional • Peraturan Menteri Hukum Nomor 35 Tahun 2025 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik
2	Menguraikan manfaat transformasi digital melalui SPBE bagi pelayanan publik.	Manfaat transformasi digital dalam mendukung pelayanan publik	1. Manfaat transformasi digital bagi pemerintah 2. Manfaat transformasi digital bagi masyarakat	• Ceramah • Curah Pendapat	• Slide Presentasi (PPT) • Tayangan Video Komputer	Tes : Objektif : Pilihan Ganda Non Objektif: Jawaban Singkat Non Tes: Penilaian Sikap	1			1	
3	Menjelaskan Penerapan SPBE dalam Pelaksanaan	Penerapan SPBE dalam Pelaksanaa	1. Penerapan SPBE dalam manajemen				1			1	

	Tugas dan Fungsi Instansi	n Tugas dan Fungsi Instansi	dan administrasi perkantoran 2. Penerapan SPBE dalam pelayanan publik di lingkungan Kementeria n Hukum								
Jumlah							**3**			**3**	

10. RANCANG BANGUN PEMBELAJARAN MATA PELATIHAN

1	Nama Pelatihan		:	Pelatihan Teknis Keamanan Siber
2	Mata Pelatihan		:	**Etika dan Tanggung Jawab ASN dalam Dunia Digital**
3	Alokasi Waktu		:	2 JP@45 menit = 90 menit
4	Deskripsi Singkat		:	Mata pelatihan ini membahas Etika dan Tanggung Jawab ASN dalam Dunia Digital dan Tanggung jawab ASN dalam menjaga keamanan dan integritas data publik.. Materi akan disampaikan melalui metode ceramah dan curah pendapat, sehingga peserta mampu Menjelaskan Prinsip etika dan perilaku ASN di ruang digital dan mampu Menguraikan Tanggung jawab ASN dalam menjaga keamanan dan integritas data publik yang akan dievaluasi melalui Tes Objektif pilihan ganda, Tes Non objektif Uraian dan Non Tes Penilaian Sikap.
5	Tujuan Pembelajaran			
	a	Hasil belajar	:	Setelah mengikuti pembelajaran ini, peserta mampu menjelaskan etika dan tanggung jawab ASN di lingkungan digital.
	b	Indikator Hasil belajar		Pada akhir pembelajaran diharapkan peserta dapat:

No	Indikator Hasil Belajar	Materi Pokok		Metode Pembelajaran	Alat Bantu Dan Media	Evaluasi	Estimasi Waktu (JP/Menit)				Referensi/ Keterangan
		Materi Pokok	Sub Materi Pokok				T	P	L	Total	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
1.	Menjelaskan Prinsip etika dan perilaku ASN di ruang digital.	Etika dan Tanggung Jawab ASN dalam Dunia Digital	1. Kode Etik ASN & Etika Bermedia Digital Bagi ASN 2. 4 Pilar Literasi Digital	• Ceramah • Curah Pendapat	• Slide Presentasi (PPT) • Tayangan Video • Komputer	Tes Objektif : Pilihan Ganda Non Objektif: Jawaban Singkat	1			1	• Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11

						Non Tes: Penilaian Sikap				Tahun 2008 tentang Informasi dan Transaksi Elektronik • UU No. 20 Tahun 2023 tentang Aparatur Sipil Negara • UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi • PP No. 94 Tahun 2021 tentang Disiplin Pegawai Negeri Sipil • Perpres No. 95/2018 tentang SPB
2	Menguraikan Tanggung jawab ASN dalam menjaga keamanan dan integritas data publik.	Tanggung jawab ASN dalam menjaga keamanan dan integritas data publik.	1. Hak & Kewajiban ASN Di Era Digital 2. Perlindungan Data Pribadi (PDP) 3. Sanksi Disiplin dan Ancaman Pidana UU ITE	• Ceramah • Curah Pendapat	• Slide Presentasi (PPT) • Tayangan Video • Komputer	Tes Objektif : Pilihan Ganda Non Objektif: Jawaban Singkat Non Tes: Penilaian Sikap	1			1	
Jumlah							**2**			**2**	