IDENTITAS BUKU

PERATURAN DAN STANDAR NASIONAL INDONESIA (SNI) TERKAIT TEKNOLOGI INFORMASI (TI)

Penyusun:

Tim Penyusun Kurikulum dan Hanjar Dikbangspes
Bintara/Gol.II PNS Polri Teknologi Informasi Dasar
Lemdiklat Polri T.A. 2022

Editor:

1. Kombes Pol. Nirboyo, S.I.K.
2. Pembina Rudiyanto, S.Pd.
3. Pembina Nolik Dwi Atmoko, S.E., M.E.
4. Kompol Yon Helmi
5. AKP I Gede Eka Irawan, S.T.
6. Penda Tk I Haryati
7. Penda Paramita Rahmadani, A.Md.
8. Briptu Ginawan Rahmat Permana, S.Kom.

Hanjar Pendidikan Polri
Pendidikan Pengembangan Spesialisasi
Bintara/Gol.II PNS Polri Teknologi Informasi Dasar

Diterbitkan oleh:

Bagian Kurikulum dan Bahan Ajar Pendidikan Pengembangan Spesialisasi
Biro Kurikulum
Lembaga Pendidikan dan Pelatihan Polri
Tahun 2022

DAFTAR ISI

POKOK BAHASAN 2

STANDAR NASIONAL INDONESIA SNI ISO/IEC 27000 TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI)

MODUL	**PERATURAN DAN STANDAR NASIONAL INDONESIA (SNI) TERKAIT TEKNOLOGI INFORMASI (TI)**
	 6 JP (270 menit)

PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat telah membuat batas fisik yang jauh sekalipun bukan suatu kendala, sehingga apa yang terjadi di tempat yang jauh dapat disaksikan real time di tempat yang lain. Perkembangan tersebut tentu sangat membantu manusia dalam mempermudah melaksanakan interaksi sosial dan penyelesaian suatu pekerjaan.

Karena begitu cepat dan luasnya cakupan penyebaran informasi yang memanfaatkan teknologi informasi, maka diperlukan pemahaman yang bijak sesuai dengan peraturan dan standar yang ada sehingga dampak buruk tidak menimpa orang yang memanfaatkan teknologi informasi tersebut.

Untuk itu diperlukan pemahaman tentang peraturan terkait teknologi informasi dan standar teknologi informasi bagi setiap anggota Polri yang di dalamnya dibahas materi tentang Modul 1 meliputi peraturan teknologi informasi dan modul 2 tentang Standar Nasional Indonesia (SNI) tentang Teknologi Informasi (TI).

STANDAR KOMPETENSI

Memahami Peraturan dan Standar Nasional Indonesia (SNI) terkait Teknologi Informasi (TI).

MODUL 01

PERATURAN TERKAIT TEKNOLOGI INFORMASI

4 JP (180 menit)

PENGANTAR

Modul ini membahas materi Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Perpres 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Perpres 39 Tahun 2019 tentang Satu Data Indonesia (SDI).

Tujuannya agar peserta didik memahami peraturan yang berkaitan dengan teknologi informasi.

KOMPETENSI DASAR

1. Memahami Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

   Indikator Hasil Belajar:

   a. Menjelaskan konsep informasi dan transaksi elektronik.
   b. Menjelaskan informasi, dokumen dan tanda tangan elektronik.
   c. Menjelaskan penyelenggaraan sertifikasi elektronik dan sistem elektronik.
   d. Menjelaskan transaksi elektronik.
   e. Menjelaskan domain, hak kekayaan intelektual, dan perlindungan hak pribadi.
   f. Menjelaskan perbuatan yang dilarang.

2. Memahami Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

   Indikator Hasil Belajar:

   a. Menjelaskan konsep penyelenggaraan sistem dan transaksi elektronik.
   b. Menjelaskan penyelenggara sistem elektronik.
   c. Menjelaskan penyelenggara agen elektronik.
   d. Menjelaskan penyelenggaraan transaksi elektronik.

e. Menjelaskan penyelenggaraan sertifikasi elektronik.
f. Menjelaskan pengelolaan nama domain.

3. Memahami Perpres 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE).

Indikator Hasil Belajar:

a. Menjelaskan konsep sistem pemerintahan berbasis elektronik.
b. Menjelaskan tata kelola sistem pemerintahan berbasis elektronik
c. Menjelaskan manajemen sistem pemerintahan berbasis elektronik.
d. Menjelaskan audit teknologi informasi dan komunikasi
e. Menjelaskan penyelenggara sistem pemerintahan berbasis elektronik.
f. Menjelaskan percepatan sistem pemerintahan berbasis elektronik
g. Menjelaskan pemantauan dan evaluasi sistem pemerintahan berbasis elektronik

4. Memahami Perpres 39 Tahun 2019 tentang Satu Data Indonesia (SDI).

Indikator Hasil Belajar:

a. Menjelaskan konsep SDI.
b. Menjelaskan penyelenggara SDI.
c. Menjelaskan penyelenggaraan SDI
d. Menjelaskan partisipasi lembaga negara dan badan hukum publik

MATERI PELAJARAN

1. **Pokok Bahasan 1:**

Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Subpokok Bahasan:

a. Konsep informasi dan transaksi elektronik.
b. Informasi, dokumen dan tanda tangan elektronik.
c. Penyelenggaraan sertifikasi elektronik dan sistem elektronik.
d. Transaksi elektronik.
e. Domain, hak kekayaan intelektual, dan perlindungan hak pribadi.
f. Perbuatan yang dilarang.

2. Pokok Bahasan 2:

Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Subpokok Bahasan:

a. Konsep penyelenggaraan sistem dan transaksi elektronik.
b. Penyelenggara sistem elektronik.
c. Penyelenggara agen elektronik.
d. Penyelenggaraan transaksi elektronik.
e. Penyelenggaraan sertifikasi elektronik.
f. Pengelolaan nama domain.

3. Pokok Bahasan 3:

Perpres 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE).

Subpokok Bahasan:

a. Konsep sistem pemerintahan berbasis elektronik.
b. Tata kelola sistem pemerintahan berbasis elektronik
c. Manajemen sistem pemerintahan berbasis elektronik.
d. Audit teknologi informasi dan komunikasi
e. Penyelenggara sistem pemerintahan berbasis elektronik.
f. Percepatan sistem pemerintahan berbasis elektronik
g. Pemantauan dan evaluasi sistem pemerintahan berbasis elektronik

4. Pokok Bahasan 4:

Perpres 39 Tahun 2019 tentang Satu Data Indonesia (SDI).

Subpokok Bahasan::

a. Konsep SDI.
b. Penyelenggara SDI.
c. Penyelenggaraan SDI
d. Partisipasi lembaga negara dan badan hukum publik.

METODE PEMBELAJARAN

1. Metode Ceramah

Metode ini digunakan untuk menyampaikan materi tentang peraturan teknologi informasi.

2. Metode Tanya Jawab

Metode ini digunakan untuk memperdalam pemahaman materi dan untuk mengetahui tingkat penguasaan materi yang telah disampaikan oleh pendidik tentang materi peraturan teknologi informasi.

ALAT, MEDIA, BAHAN DAN SUMBER BELAJAR

1. Alat, Media dan Bahan:

a. Laptop.
b. LCD.
c. *Flip chart.*
d. *Whiteboard.*
e. Slide
f. Kertas.
g. Alat tulis.

2. Sumber Belajar:

a. Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.
b. Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
c. Perpres 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE).
d. Perpres 39 Tahun 2019 tentang Satu Data Indonesia (SDI).

KEGIATAN PEMBELAJARAN

1. Tahap awal: 10 menit

a. Pendidik melaksanakan apersepsi:
   1) Pendidik melaksanakan perkenalan.
   2) Pendidik menyampaikan tujuan pembelajaran.
   3) Pendidik menciptakan suasana pembelajaran yang kondusif.
b. Peserta didik menyimak, menanggapi dan melaksanakan instruksi pendidik.

2. Tahap inti : 160 menit

a. Pendidik menyampaikan materi tentang peraturan teknologi informasi.
b. Pendidik memberikan kesempatan kepada peserta didik untuk bertanya hal-hal yang belum dipahami.
c. Peserta didik menyimak, mencatat, mananggapi dan menanyakan materi yang belum dipahami.
d. Pendidik menanggapi penyataan atau pertanyaan peserta didik.

	3. Tahap akhir: 10 menit a. Pendidik mengecek penguasaan materi dengan cara bertanya secara lisan dan acak kepada peserta didik. b. Pendidik memberikan kesimpulan dan penguatan materi peraturan teknologi informasi. c. Pendidik melakukan evaluasi pembelajaran dan menutup pembelajaran.

	**TAGIHAN/TUGAS**

	**LEMBAR KEGIATAN**

BAHAN BACAAN

POKOK BAHASAN 1

UNDANG-UNDANG (UU) NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

1. Konsep Informasi dan Transaksi Elektronik

a. Pengertian yang berkaitan dengan Informasi dan Transaksi Elektronik

1) Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic maill, telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

2) Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.

3) Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/ atau menyebarkan informasi.

4) Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

5) Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

6) Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/ atau mengoperasikan Sistem Elektronik, baik secara sendiri-

sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.

7) Jaringan Sistem Elektronik adalah terhubungnya dua Sistem Elektronik atau lebih, yang bersifat tertutup ataupun terbuka.
8) Agen Elektronik adalah perangkat dari suatu Sistem Elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh Orang.
9) Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.
10) Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.
11) Lembaga Sertifikasi Keandalan adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat keandalan dalam Transaksi Elektronik.
12) Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
13) Penanda Tangan adalah subjek hukum yang terasosiasikan atau terkait dengan Tanda Tangan Elektronik.
14) Komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.
15) Akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan.
16) Kode Akses adalah angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya, yang merupakan kunci untuk dapat mengakses Komputer dan/ atau Sistem Elektronik lainnya.
17) Kontrak Elektronik adalah perjanjian para pihak yang dibuat melalui Sistem Elektronik.
18) Pengirim adalah subjek hukum yang mengirimkan Informasi Elektronik dan/ atau Dokumen Elektronik.

19) Penerima adalah subjek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.
20) Nama Domain adalah alamat internet penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
21) Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.
22) Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.
23) Pemerintah adalah Menteri atau pejabat lainnya yang ditunjuk oleh Presiden.

b. Asas dan tujuan

1) Asas
Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi.

2) Tujuan
a) Mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia.
b) Mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat.
c) Meningkatkan efektivitas dan efisiensi pelayanan publik.
d) Membuka kesempatan seluas-luasnya kepada setiap Orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab. dan
e) Memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi.

2. Informasi, Dokumen dan Tanda Tangan Elektronik

Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

a. Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik tidak berlaku untuk:
   1) Surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis. dan
   2) Surat beserta dokumennya yang menurut UndangUndang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

b. Dalam hal terdapat dua atau lebih sistem informasi yang digunakan dalam pengiriman atau penerimaan Informasi Elektronik dan/atau Dokumen Elektronik, maka:
   1) Waktu pengiriman adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi pertama yang berada di luar kendali Pengirim.
   2) Waktu penerimaan adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi terakhir yang berada di bawah kendali Penerima.

c. Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:
   1) Data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan.
   2) Data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan.
   3) Segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui.
   4) Segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui.
   5) Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penandatangannya. dan
   6) Terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.

d. Pengamanan Tanda Tangan Elektronik sekurang-kurangnya meliputi:
   1) Sistem tidak dapat diakses oleh Orang lain yang tidak berhak.
   2) Penanda Tangan harus menerapkan prinsip kehatihatian untuk menghindari penggunaan secara tidak sah terhadap data terkait pembuatan Tanda Tangan Elektronik.

3) Penanda Tangan harus tanpa menunda-nunda, menggunakan cara yang dianjurkan oleh penyelenggara Tanda Tangan Elektronik ataupun cara lain yang layak dan sepatutnya harus segera memberitahukan kepada seseorang yang oleh Penanda Tangan dianggap memercayai Tanda Tangan Elektronik atau kepada pihak pendukung layanan Tanda Tangan Elektronik jika:
   a) Penanda Tangan mengetahui bahwa data pembuatan Tanda Tangan Elektronik telah dibobol.
   b) Keadaan yang diketahui oleh Penanda Tangan dapat menimbulkan risiko yang berarti, kemungkinan akibat bobolnya data pembuatan Tanda Tangan Elektronik.

4) Dalam hal Sertifikat Elektronik digunakan untuk mendukung Tanda Tangan Elektronik, Penanda Tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan Sertifikat Elektronik tersebut.

3. Penyelenggaraan Sertifikasi Elektronik dan Sistem Elektronik

a. Penyelenggara Sertifikasi Elektronik terdiri atas:
   1) Penyelenggara Sertifikasi Elektronik Indonesia.
      Penyelenggara Sertifikasi Elektronik Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia
   2) Penyelenggara Sertifikasi Elektronik asing.
      Penyelenggara Sertifikasi Elektronik asing yang beroperasi di Indonesia harus terdaftar di Indonesia.

b. Penyelenggara Sertifikasi Elektronik harus menyediakan informasi yang akurat, jelas, dan pasti kepada setiap pengguna jasa, yang meliputi:
   1) Metode yang digunakan untuk mengidentifikasi Penanda Tangan.
   2) Hal yang dapat digunakan untuk mengetahui data diri pembuat Tanda Tangan Elektronik.
   3) Hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik.

c. Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:

1) Dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan.
2) Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut.
3) Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut.
4) Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut.
5) Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

4. Transaksi Elektronik

Penyelenggaraan Transaksi Elektronik dapat dilakukan dalam lingkup publik ataupun privat. Para pihak yang melakukan Transaksi Elektronik wajib beriktikad baik dalam melakukan interaksi dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektronik selama transaksi berlangsung.

Pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan Transaksi Elektronik diatur sebagai berikut:

a. Jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab para pihak yang bertransaksi.
b. Jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab pemberi kuasa. atau
c. Jika dilakukan melalui Agen Elektronik, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab penyelenggara Agen Elektronik.

5. Nama Domain, Hak Kekayaan Intelektual, dan Perlindungan Hak Pribadi

Setiap penyelenggara negara, orang, badan usaha, dan/atau masyarakat berhak memiliki nama domain berdasarkan prinsip pendaftar pertama. Pemilikan dan penggunaan nama domain harus didasarkan pada iktikad baik, tidak melanggar prinsip persaingan usaha secara sehat, dan tidak melanggar hak orang lain.

Setiap penyelenggara negara, orang, badan usaha, atau masyarakat yang dirugikan karena penggunaan nama domain secara tanpa hak oleh orang lain, berhak mengajukan gugatan pembatalan nama domain dimaksud.

Informasi elektronik dan/atau dokumen elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai hak kekayaan intelektual.

6. Perbuatan yang Dilarang

a. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
b. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
c. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
d. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.
e. Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
f. Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).
g. Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.
h. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

	i. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. j. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. k. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan Dokumen Elektronik dalam suatu Komputer dan Sistem Elektronik tertentu milik Orang lain. l. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan. m. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik. n. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak. o. Terhadap perbuatan yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya. p. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya. q. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: 1) Perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan.

2) Sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan.

r. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

POKOK BAHASAN 2

PERATURAN PEMERINTAH (PP) NOMOR 71 TAHUN 2019 TENTANG PENYELENGGARAAN SISTEM DAN TRANSAKSI ELEKTRONIK

1. Konsep Penyelenggaraan Sistem dan Transaksi Elektronik

a. Pengertian yang berkaitan dengan Penyelenggaraan Sistem dan Transaksi Elektronik.

1) Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi. mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
2) Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/ atau media elektronik lainnya.
3) Agen Elektronik adalah perangkat dari suatu Sistem Elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh Orang.
4) Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluair dirinya dan/ atau keperluan pihak lain.
5) Penyelenggara Sistem Elektronik Lingkup Publik adalah penyelenggaraan Sistem Elektronik oleh Instansi Penyelenggara Negara atau institusi yang ditunjuk oleh Instansi PenyelenggaraNegara.
6) Penyelenggara Sistem Elektronik Lingkup Privat adalah penyelenggaraan Sistem Elektronik oleh Orang, Badan Usaha, dan masyarakat.
7) Informasi Elektronik adalah satu atau sekumpulan Data Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, eledrontc data interchange (EDI), surat elektronik (electronic maill, telegram, teleks, telecopg atau sejenisnya, huruf, tanda, angka, kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

	8) Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/ atau didengar melalui komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. 9) Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi. 10) Pengguna Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang memanfaatkan barang, jasa, fasilitas, atau informasi yang disediakan oleh Penyelenggara Sistem Elektronik. 11) Perangkat Keras adalah satu atau serangkaian alat yang terhubung dalam Sistem Elektronik. 12) Perangkat Lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian Sistem Elektronik. 13) Uji Kelaikan Sistem Elektronik adalah suatu rangkaian proses penilaian secara objektif terhadap setiap komponen Sistem Elektronik, baik dilakukan secara mandiri dan/atau dilakukan oleh institusi yang berwenang dan berkompeten. 14) Akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan. 15) Penyelengaraan Transaksi Elektronik adalah rangkaian kegiatan Transaksi Elektronik yang dilakukan oleh Pengirim dan Penerima dengan menggunakan Sistem Elektronik. 16) Kontrak Elektronik adalah perjanjian para pihak yang dibuat melalui Sistem Elektronik. 17) Pengirim adalah subjek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik. 19. Penerima adalah subjek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim. 18) Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.

	19) Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik. 20) Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. 21) Penanda Tangan adalah subjek hukum yang terasosiasikan atau terkait dengan Tanda Tangan Elektronik. 22) Perangkat Pembuat Tanda Tangan Elektronik adalah Perangkat Lunak atau Perangkat Keras yang dikonfigurasi dan digunakan untuk membuat Tanda Tangan Elektronik. 23) Data Pembuatan Tanda Tangan Elektronik adalah kode pribadi, kode biometrik, kode kriptografi, dan/ atau kode yang dihasilkan dari pengubahan tanda tangan manual menjadi Tanda Tangan Elektronik, termasuk kode lain yang dihasilkan dari perkembangan Teknologi Informasi. 24) Sertilikat Keandalan adalah dokumen yang menyatakan Pelaku Usaha yang menyelenggarakan Transaksi Elektronik telah lulus audit atau uji kesesuaian dari Lembaga Sertifikasi Keandalan. 25) Pelaku Usaha adalah setiap orang perseorangan atau Badan Usaha, baik berbentuk badan hukum maupun bukan badan hukum, yang didirikan dan berkedudukan atau melakukan kegiatan dalam wilayah hukum Negara Republik Indonesia, secara sendiri-sendiri maupun bersama-sama, melalui perjanjian penyelenggaraan kegiatan usaha dalam berbagai bidang ekonomi. 26) Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan /atau nonelektronik. 27) Data Elektronik adalah data berbentuk elektronik yang tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic dcita interchange (EDI), surat elektronik (electronic mait1, telegram, teleks, teleapg atau sejenisnya, huruf, tanda, angka, kode Akses, simbol, atau perforasi. 28) Nama Domain adalah alamat internet penyeldnggara negara, Orang, Badan Usaha, dan/ atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang

bersifat unik untuk menunjukkan lokasi tertentu dalam internet.

29) Registri Nama Domain adalah penyelenggara yang bertanggung jawab dalam melakukan pengelolaan, pengoperasian, dan pemeliharaan penyelenggaraan Sistem Elektronik Nama Domain.

30) Registrar Nama Domain adalah Orang, Badan Usaha, atau masyarakat yang menyediakan jasa pendaftaran Nama Domain.

31) Pengguna Nama Domain adalah Orang, Instansi Penyelenggara Negara, Badan Usaha, atau masyarakat yang mengajukan pendaftaran untuk penggunaan Nama Domain kepada Registrar Nama Domain.

2. Penyelenggara Sistem Elektronik

a. Penyelenggara Sistem Elektronik meliputi:

1) Penyelenggara Sistem Elektronik Lingkup Publik.
Penyelenggara Sistem Elektronik Lingkup Publik meliputi:
a) Instansi.
b) Institusi yang ditunjuk oleh Instansi.

2) Penyelenggara Sistem Elektronik Lingkup Privat.

Penyelenggara Sistem Elektronik Lingkup Privat meliputi:

a) Penyelenggara Sistem Elektronik yang diatur atau diawasi oleh Kementerian atau kmbaga berdasarkan ketentuan peraturan pemndang-undangan.
b) Penyelenggara Sistem Elektronik yang memiliki portal, situs, atau aplikasi dalam jaringan melalui internet yang dipergunakan untuk:
(1) Menyediakan, mengelola, dan/atau mengoperasikan penawaran dan/atau perdagangan barang dan/ atau jasa.
(2) Menyediakan, mengelola, dan/atau mengoperasikan layanan transaksi keuangan.
(3) Pengiriman materi atau muatan digital berbayar melalui jaringan data baik dengan cara unduh melalui portal atau situs, pengiriman lewat surat elektronik, atau melalui aplikasi lain ke perangkat pengguna.
(4) Menyediakan, mengelola, dan/atau mengoperasikan layanan komunikasi meliputi namun tidak terbatas pada pesan singkat,

panggilan suara, panggilan video, surat elektronik, dan percakapan dalam jaringan dalam bentuk platform digital, layanan jejaring dan media sosial.

(5) Layanan mesin pencari, layanan penyediaan Informasi Elektronik yang berbentuk tulisan, suara, gambar, animasi, musik, video, frlm, dan permainan atau kombinasi dari sebagian dan/ atau seluruhnya.

(6) Pemrosesan Data Pribadi untuk kegiatan operasional melayani masyarakat yang terkait dengan aktivitas Transaksi Elektronik.

b. Sepanjang tidak ditentukan lain undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:

1) Dapat menampilkan kembali Informasi Elektronik dan/ atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan.
2) Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam penyelenggaraan Sistem Elektronik tersebut.
3) Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan Sistem Elektronik tersebut.
4) Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan Sistem Elektronik tersebut.
5) Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungiawaban prosedur atau petunjuk.

c. Pendaftaran Sistem Elektronik

Kewajiban melakukan pendaftaran bagi Penyelenggara Sistem Elektronik dilakukan sebelum Sistem Elektronik mulai digunakan oleh Pengguna Sistem Elektronik. Pendaftaran Penyelenggara Sistem Elektronik diajukan kepada Menteri melalui pelayanan perizinan berusaha terintegrasi secara elektronik sesuai dengan ketentuan peraturan perundang-undangan.

d. Perangkat Keras

Perangkat Keras yang digunakan oleh Penyelenggara Sistem Elektronik harus:

1) Memenuhi aspek keamanan, interkonektivitas dan kompatibilitas dengan sistem yang digunakan.

2) Mempunyai layanan dukungan teknis, pemeliharaan, dan/ atau purnajual dari penjual atau penyedia.
3) Memiliki jaminan keberlanjutan layanan.

e. Perangkat Lunak

Perangkat Lunak yang digunakan oleh Penyelenggara Sistem Elektronik harus:
1) Terjamin keamanan dan keandalan operasi sebagaimana mestinya.
2) Memastikan keberlanjutan layanan.

f. Tenaga Ahli

Tenaga ahli yang digunakan oleh Penyelenggara Sistem Elektronik harus memiliki kompetensi di bidang Sistem Elektronik atau Teknologi Informasi.

g. Tata Kelola Sistem Elektronik

Penyelenggara Sistem Elektronik harus menjamin:
1) Tersedianya perjanjian tingkat layahan.
2) Tersedianya perjanjian keamanan informasi terhadap jasa layanan teknologi informasi yang digunakan.
3) Keamanan informasi dan sarana komunikasi internal yang diselenggarakan

Penyelenggara Sistem Elektronik wajib melaksanakan prinsip pelindungan Data Pribadi dalam melakukan pemrosesan Data Pribadi meliputi:

1) Pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetqluan dari pemilik Data Pribadi.
2) Pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya.
3) Pemrosesan Data Pribadi dilakukan dengan menjamin hak pemilik Data Pribadi.
4) Pemrosesan Data Pribadi dilakukan secara alurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dan memperhatikan tu-iuan pemrosesan Data Pribadi.
5) Pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari kehilangan, penyalahgunaan, Akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan Data Pribadi.
6) Pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan pengumpulan, aktivitas pemrosesan, dan kegagalan pelindungan Data Pribadi.

7) Pemrosesan Data Pribadi dimusnahkan dan/ atau dihapus kecuali masih dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan.

Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang dilakukan penghapusan (*right to erasurel*) terdiri atas Data Pribadi yang:

1) Diperoleh dan diproses tanpa persetujuan pemilik Data Pribadi.
2) Telah ditarik persetqjuannya oleh pemilik Data Pribadi.
3) Diperoleh dan diproses dengan cara melawan hukum.
4) Sudah tidak sesuai lagi dengan tujuan perolehan berdasarkan perjanjian dan/atau ketentuan peraturan perundang-undangan.
5) Penggunaannya telah melampaui waktu sesuai dengan perjanjian dan/atau ketentuan peraturan perundang-undangan.
6) Ditampilkan oleh Penyelenggara Sistem Elektronik yang mengakibatkan kerugian bagi pemilik Data Pribadi.

h. Pengamanan Penyelenggaraan Sistem Elektronik

Penyelenggara Sistem Elektronik wajib menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan Sistem Elektronik. Rekam jejak audit digunakan untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lainnya.

Penyelenggara Sistem Elektronik wajib memiliki dan menjalankan prosedur dan sarana untuk pengamanan Sistem Elektronik dalam menghindari gangguan, kegagalan, dan kerugian. Penyelenggara Sistem Elektronik wajib menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian. Dalam hal terjadi kegagalan atau gangguan sistem yang berdampak serius sebagai akibat perbuatan dari pihak lain terhadap Sistem Elektronik, Penyelenggara Sistem Elektronik wajib mengamankan Informasi Elektronik dan/atau Dokumen Elektronik dan segera melaporkan dalam kesempatan pertama kepada aparat penegak hukum dan Kementerian atau Lembaga terkait. Ketentuan lebih lanjut mengenai sistem pengamanan yang melaksanakan urLlsan pemerintahan di bidang keamanan siber.

Penyelenggara Sistem Elektronik wajib menjaga kerahasiaan, keutuhan, keautentikan, keteraksesan, ketersediaan, dan dapat ditelusurinya suatu Informasi Elektronik dan/atau Dokumen Elektronik sesuai dengan

ketentuan peraturan perundang-undangan. Dalam penyelenggaraan Sistem Elektronik yang ditujukan untuk Informasi Elektronik dan/atau Dokumen Elektronik yang dapat dipindahtangankan, Informasi Elektronik dan/ atau Dokumen Elektronik harus unik serta menjelaskan penguasaan dan kepemilikannya.

Penyelenggara Sistem Elektronik wajib menyampaikan informasi kepada Pengguna Sistem Elektronik paling sedikit mengenai:

1) Identitas Penyelenggara Sistem Elektronik.
2) Objek yang ditransaksikan.
3) Kelaikan atau keamanan Sistem Elektronik.
4) Tata cara penggunaan perangkat.
5) Syarat kontrak.
6) Prosedur mencapai kesepakatan.
7) Jaminan privasi dan/atau pelindungan Data Pribadi.
8) Nomor telepon pusat pengaduan.

i. Uji Kelaikan Sistem Elektronik

Penyelenggara Sistem Elektronik wajib melakukan Uji Kelaikan Sistem Elektronik. Kewajiban dapat dilaksanakan terhadap seluruh komponen atau sebagian komponen dalam Sistem Elektronik sesuai dengan karakteristik kebutuhan pelindungan dan sifat strategis penyelenggaraan Sistem Elektronik.

3. Penyelenggara Agen Elektronik

a. Agen Elektronik

Penyelenggara Siste dapat menyelenggarakan sendiri Sistem Elektroniknya atau melalui Agen Elektronik. Agen Elektronik dapat berbentuk:

1) Visual.
2) Audio.
3) Data Elektronik.
4) Bentuk Lainnya.

Penyelenggara Agen Elektronik wajib memuat atau menyampaikan informasi untuk melindungi hak pengguna pada Agen Elektronik yang diselenggarakannya, meliputi paling sedikit informasi mengenai:

1) Identitas penyelenggara Agen Elektronik.
2) Objek yang ditransaksikan.
3) Kelayakan atau keamanan Agen Elektronik.
4) Tata cara penggunaan perangkat.
5) Syarat kontrak.
6) Prosedur mencapai kesepakatan.

7) Jaminan privasi dan/atau pelindungan Data Pribadi.
8) Nomor telepon pusat pengaduan.

b. Kewajiban

Dalam penyelenggaraan Agen Elektronik, penyelenggara Agen Elektronik harus memperhatikan prinsip:

1) Kehati-hatian.
2) Pengamanan dan terintegrasinya sistem teknologi informasi.
3) Pengendalian pengamanan atas aktivitas transaksi elektronik.
4) Efektivitas dan efisiensi biaya.
5) Pelindungan konsumen sesuai dengan ketentuan peraturan perundang-undangan.

Prinsip pengendalian pengamanan data pengguna dan Transaksi Elektronik meliputi:

1) Kerahasiaan.
2) Integritas.
3) Ketersediaan.
4) Keautentikan.
5) Otorisasi. dan
6) Kenirsangkalan.

Penyelenggara Agen Elektronik wajib:

1) Melakukan pengujian keautentikan identitas dan memeriksa otorisasi Pengguna Sistem Elektronik yang melakukan Transaksi Elektronik.
2) Memiliki dan melaksanakan kebijakan dan prosedur untuk mengambil tindakan jika terdapat indikasi teq'adi pencurian data.
3) Memastikan pengendalian terhadap otorisasi dan hak Akses terhadap sistem, database, dan aplikasi Transaksi Elektronik.
4) Menyusun dan melaksanakan metode dan prosedur untuk melindungi dan/atau merahasiakan integritas data, catatan, dan informasi terkait Transaksi Elektronik.
5) Memiliki dan melaksanakan standar dan pengendalian atas penggunaan dan pelindungan data jika pihak penyedia jasa memiliki Akses terhadap data tersebut.
6) Memiliki rencana keberlangsungan bisnis termasuk rencana kontingensi yang efektif untuk memastikan tersedianya sistem dan jasa Transaksi Elektronik secara berkesinambungan.
7) Memiliki prosedur penanganan kejadian tak terduga yang cepat dan tepat untuk mengurangi dampak suatu insiden, penipuan, dan kegagalan Sistem Elektronik.

4. Penyelenggaraan Transaksi Elektronik.

a. Lingkup Penyelenggaraan Transaksi Elektronik

Penyelenggaraan Transaksi Elektronik dalam lingkup publik meliputi Penyelenggaraan Transaksi Elektronik oleh:

1) Instansi.
2) Institusi yang ditunjuk oleh instansi.
3) Antar-instansi.
4) Antar-institusi yang ditunjuk.
5) Antara instansi dengan institusi yang ditunjuk. dan
6) Antara instansi atau institusi dengan pelaku usaha sesuai dengan ketentuan peraturan perundangundangan.

Penyelenggaraan Transaksi Elektronik dalhm lingkup privat meliputi Transaksi Elektronik:

1) Antar-pelaku usaha.
2) Antara pelaku usaha dengan konsumen.
3) Antarpribadi.

b. Persyaratan Penyelenggaraan Transaksi Elektronik

Penyelenggaraan Transaksi Elektronik wajib menggunakan Sertifikat Elektronik yang diterbitkan oleh Penyelenggara Sertifikasi Elektronik Indonesia. Penyelenggaraan Transaksi Elektronik dapat menggunakan Sertifikat Keandalan. Dalam hal menggunakan Sertifikat Keandalan Penyelenggaraan Transaksi Elektronik wajib menggunakan Sertifikat Keandalan yang diterbitkan oleh Lembaga Sertifikasi Keandalan yang terdaftar.

Penyelenggaraan Transaksi Elektronik yang dilaksanakan oleh Penyelenggara Sistem Elektronik Lingkup Publik harus memperhatikan aspek keamanan, keandalan, dan efisiensi.

c. Persyaratan Transaksi Elektronik

Penyelenggaraan Transaksi Elektronik yang dilakukan para pihak harus memperhatikan:

1) Iktikad baik.
2) Prinsip kehati-hatian.
3) Transparansi.
4) Akuntabilitas.
5) Kewajaran.

Transaksi Elektronik dapat dilakukan berdasarkan Kontrak Elektronik atau bentuk kontraktual lainnya sebagai bentuk kesepakatan yang dilakukan oleh para pihak.

Kontrak Elektronik dianggap sah apabila:

1) Terdapat kesepakatan para pihak.
2) Dilakukan oleh subjek hukum yang cakap atau yang berwenang mewakili sesuai dengan ketentuan peraturan perundang-undangan.
3) Terdapat hal tertentu. dan
4) Objek transaksi tidak boleh bertentangan dengan peraturan perundang-undangan,. kesusilaan, dan ketertiban umum.

5. Penyelenggaraan Sertifikasi Elektronik

a. Sertifikat Elektronik

Penyelenggara Sistem Elektronik wajib memiliki Sertifikat Elektronik. Pengguna Sistem Elektronik dapat Sertifikat Elektronik dalam Transaksi Elektronik. Untuk memiliki Sertilikat Elektronik, Penyelenggara Sistem Elektronik dan Pengguna Sistem Elektronik harus mengajukan permohonan kepada Penyelenggara Sertifikasi Elektronik Indonesia. Dalam hal diperlukan, Kementerian atau lembaga dapat mewajibkan Pengguna Sistem Elektronik menggunakan Sertifikat Elektronik dalam Transaksi Elektronik.

b. Penyelenggara Sertifikasi Elektronik

Penyelenggara Sirtifikasi Elektronik berwenang melakukan:

1) pemeriksaan calon pemilik dan/ atau pemegang Sertifikat Elektronik, penerbitan Sertifikat Elektronik, perpanjangan masa berlaku Sertifikat Elektronik, pemblokiran dan pencabutan Sertifikat Elektronik, validasi Sertilikat Elektronik. dan pembuatan daftar Sertifikat Elektronik yang aktif dan yang dicabut. dan
2) pembuatan, verifikasi, dan validasi terhadap Tanda Tangan Elektronik dan/atau layanan lain yang menggunakan Sertifikat Elektronik.

c. Layanan Penyelenggara Sertifikasi Elektronik

Penyelenggara Sertilikasi Elektronik Indonesia menyediakan layanan yang tersertifikasi. Penyelenggara Sertifikasi Elektronik Indonesia menanggung kerugian yang diakibatkan oleh keseng4iaan atau kelalaian kepada Orang, Badan Usaha atau Instansi karena kegagalannya dalam mematuhi kewajibannya. Penyelenggara Sertifikasi Elektronik Indonesia dianggap sengaja atau lalai kecuali Penyelenggara Sertifikasi Elektronik Indonesia tersebut dapat membuktikan bahwa kerugian terjadi bukan karena kesengajaan atau kelalaiannya. Tanggung jawab pembuktian terhadap

kesengajaan atau kelalaian yang dilakukan oleh pihak yang bukan Penyelenggara Sertifikasi Elektronik Indonesia menjadi tanggung jawab dari Orang, Badan Usaha atau Instansi yang mengalami kerugian.

6. **Pengelolaan Nama Domain**.

Pengelolaan Nama Domain diselenggarakan oleh pengelola Nama Domain.

Nama Domain terdiri atas:

a. Nama Domain tingkat tinggi generik.
b. Nama Domain tingkat tinggi Indonesia.
c. Nama Domain Indonesia tingkat kedua.
d. Nama Domain Indonesia tingkat turunan.

Registri Nama Domain berfungsi:

a. Memberikan masukan terhadap rencana pengaturan Nama Domain kepada Menteri.
b. Melakukan pengawasan terhadap Registrar Nama Domain.
c. Menyelesaikan perselisihan Nama Domain.

Nama Domain yang didaftarkan harus memenuhi persyaratan:

a. Sesuai dengan ketentuan peraturan perundangundangan.
b. Kepatutan yang berlaku dalam masyarakat.
c. Iktikad baik.

POKOK BAHASAN 3

PERPRES 95 TAHUN 2018 TENTANG SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE)

1. Konsep Sistem Pemerintahan Berbasis Elektronik

a. Pengertian yang berkaitan dengan Sistem Pemerintahan Berbasis Elektronik

1) Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
2) Tata Kelola SPBE adalah kerangka kerja yang memastikan terlaksananya pengaturan, pengarahan, dan pengendalian dalam penerapan SPBE secara terpadu.
3) Manajemen SPBE adalah serangkaian proses untuk mencapai penerapan SPBE yang efektif, efisien, dan berkesinambungan, serta layanan SPBE yang berkualitas.
4) Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
5) Rencana Induk SPBE Nasional adalah dokumen perencanaan pembangunan SPBE secara nasional untuk jangka waktu 20 (dua puluh) tahun.
6) Arsitektur SPBE adalah kerangka dasar yang mendeskripsikan integrasi proses bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, dan keamanan SPBE untuk menghasilkan layanan SPBE yang terintegrasi.
7) Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
8) Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
9) Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.

10) Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
11) Audit Teknologi Informasi dan Komunikasi adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.
12) Pengguna SPBE adalah instansi pusat, pemerintah daerah, pegawai Aparatur Sipil Negara, perorangan, masyarakat, pelaku usaha, dan pihak lain yang memanfaatkan Layanan SPBE.

b. Prinsip SPBE

1) Efektivitas.
Merupakan optimalisasi pemanfaatan sumber daya yang mendukung SPBE yang berhasil guna sesuai dengan kebutuhan.

2) Keterpaduan.
Merupakan pengintegrasian sumber daya yang mendukung SPBE

3) Kesinambungan.
Merupakan keberlanjutan SPBE secara terencana, bertahap, dan terus menerus sesuai dengan perkembangannya.

4) Efisiensi.
Merupakan optimalisasi pemanfaatan sumber daya yang mendukung SPBE yang tepat guna

5) Akuntabilitas.
Merupakan kejelasan fungsi dan pertanggungjawaban dari SPBE

6) Interoperabilitas.
Merupakan koordinasi dan kolaborasi antar Proses Bisnis dan antar sistem elektronik, dalam rangka pertukaran data, informasi, atau Layanan SPBE.

7) Keamanan.
Merupakan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya yang mendukung SPBE

2. Tata Kelola Sistem Pemerintahan Berbasis Elektronik

a. Rencana Induk Sistem Pemerintahan Berbasis Elektronik Nasional.

Rencana Induk SPBE Nasional bertujuan untuk memberikan arah SPBE yang terpadu dan berkesinambungan secara nasional. Rencana Induk SPBE Nasional disusun berdasarkan Rencana Pembangunan Jangka Panjang Nasional dan Grand Design Reformasi Birokrasi.

b. Arsitektur Sistem Pemerintahan Berbasis Elektronik

Arsitektur SPBE terdiri atas:

1) Arsitektur SPBE Nasional.
Arsitektur SPBE Nasional bertujuan untuk memberikan panduan dalam pelaksanaan integrasi Proses Bisnis, data dan informasi, Infrastruktur SPBE, Aplikasi SPBE, dan Keamanan SPBE untuk menghasilkan Layanan SPBE yang terpadu secara nasional.

2) Arsitektur SPBE Instansi Pusat.
Arsitektur SPBE Instansi Pusat disusun dengan berpedoman pada Arsitektur SPBE Nasional dan rencana strategis Instansi Pusat.

3) Arsitektur SPBE Pemerintah Daerah.
Arsitektur SPBE Pemerintah Daerah disusun dengan berpedoman pada Arsitektur SPBE Nasional dan Rencana Pembangunan Jangka Menengah Daerah.

c. Peta Rencana Sistem Pemerintahan Berbasis Elektronik

1) Peta Rencana SPBE Nasional
Peta Rencana SPBE Nasional memuat:
a) Tata Kelola SPBE.
b) Manajemen SPBE.
c) Layanan SPBE.
d) Infrastruktur SPBE.
e) Aplikasi SPBE.
f) Keamanan SPBE.
g) Audit Teknologi Informasi dan Komunikasi.

2) Peta Rencana SPBE Instansi Pusat.
Peta Rencana SPBE Instansi Pusat disusun dengan berpedoman pada Peta Rencana SPBE Nasional, Arsitektur SPBE Instansi Pusat, dan rencana strategis Instansi Pusat. Peta Rencana SPBE Instansi Pusat disusun untuk jangka waktu 5 (lima) tahun.

3) Peta Rencana SPBE Pemerintah Daerah
Peta Rencana SPBE Pemerintah Daerah disusun dengan berpedoman pada Peta Rencana SPBE Nasional, Arsitektur SPBE Pemerintah Daerah,

Rencana Pembangunan Jangka Menengah Daerah, dan rencana strategis Pemerintah Daerah.

d. Rencana dan Anggaran Sistem Pemerintahan Berbasis Elektronik

Rencana dan anggaran SPBE disusun sesuai dengan proses perencanaan dan penganggaran tahunan pemerintah.

Setiap Instansi Pusat men)rusun rencana dan anggaran SPBE sebagaimana dimaksud dalam Pasal 20 dengan berpedoman pada Arsitektur SPBE Instansi Pusat dan Peta Rencana SPBE Instansi Pusat masing-masing.

Untuk keterpaduan rencana SPBE, penyusunan rencana SPBE Instansi Pusat dikoordinasikan dengan menteri yang menyelenggarakan urusan pemerintahan di bidang perencanaan pembangunan nasional.

Untuk keterpaduan anggaran SPBE, penyusunan anggaran SPBE Instansi Fusat dikoordinasikan dengan menteri yang menyelenggarakan urusan pemerintahan di bidang keuangan.

e. Data dan Informasi

Data dan informasi mencakup semua jenis data dan informasi yang dimiliki oleh Instansi Pusat dan Pemerintah Daerah, dan/atau yang diperoleh dari masyarakat, pelaku usaha, dan/atau pihak lain.

f. Infrastruktur Sistem Pemerintahan Berbasis Elektronik

Infrastruktur SPBE terdiri atas:

1) Infrastruktur SPBE Nasional.
   a) Pusat Data nasional.
   b) Jaringan Intra pemerintah. dan
   c) Sistem Penghubung Layanan pemerintah.
2) Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah.
   a) Jaringan Intra Instansi Pusat dan Pemerintah Daerah. dan
   b) Sistem Penghubung Layanan Instansi Pusat dan Pemerintah Daerah.

g. Infrastruktur Sistem Pemerintahan Berbasis Elektronik Instansi Pusat dan Pemerintah Daerah

Penggunaan Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah bertujuan untuk meningkatkan efisiensi, keamanan, dan kemudahan integrasi dalam rangka memenuhi kebutuhan Infrastruktur SPBE bagi internal Instansi Pusat dan Pemerintah Daerah.

Penggunaan Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah dilakukan secara bagi pakai di dalam Instansi Pusat dan Pemerintah Daerah. Pembangunan dan pengembangan Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah harus didasarkan pada Arsitektur SPBE

Instansi Pusat dan Pemerintah Daerah. Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah diselenggarakan oleh masing-masing pimpinan Instansi Pusat dan masing-masing kepala daerah

h. Pusat Data Nasional

Penggunaan Pusat Data nasional bertujuan untuk meningkatkan efisiensi dalam memanfaatkan sumber daya Pusat Data nasional oleh Instansi Pusat dan Pemerintah Daerah.

Pusat Data nasional harus:

1) Memenuhi Standar Nasional Indonesia terkait desain Pusat Data dan manajemen Pusat Data.
2) Menyediakan fasilitas bagi pakai dengan Instansi Pusat dan Pemerintah Daerah lain.
3) Mendapatkan pertimbangan kelaikan operasi dari menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.
4) Mendapatkan pertimbangan kelaikan keamanan dari kepala lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

i. Aplikasi Sistem Pemerintahan Berbasis Elektronik

Aplikasi SPBE digunakan oleh Instansi Fusat dan Pemerintah Daerah untuk memberikan Layanan SPBE. Aplikasi SPBE terdiri atas:

1) Aplikasi Umum.

Aplikasi Umum ditetapkan oleh menteri yang menyelenggarakan urusan pemerintahan di bidang aparatur negara. Pembangunan dan pengembangan Aplikasi Umum didasarkan pada Arsitektur SPBE Nasional. Pembangunan dan pengembangan Aplikasi Umum dapat dilakukan oleh Instansi Pusat atau Pemerintah Daerah setelah mendapat pertimbangan menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

2) Aplikasi Khusus.

Instansi Pusat dan Pemerintah Daerah dapat melakukan pembangunan dan pengembangan Aplikasi Khusus. Pembangunan dan pengembangan Aplikasi Khusus didasarkan pada Arsitektur SPBE Instansi Pusat dan Arsitektur SPBE Pemerintah Daerah masing-masing. Sebelum melakukan pembangunan dan pengembangan Aplikasi Khusus, Instansi Pusat dan Pemerintah Daerah harus mendapatkan pertimbangan dari menteri yang menyelenggarakan urusan pemerintahan di bidang aparatur negara. Pembangunan dan pengembangan Aplikasi Khusus harus memenuhi

standar teknis dan prosedur pembangunan dan pengembangan Aplikasi Khusus.

j. Keamanan Sistem Pemerintahan Berbasis Elektronik

Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.

k. Layanan Sistem Pemerintahan Berbasis Elektronik

Layanan SPBE terdiri atas:

1) layanan administrasi pemerintahan berbasis elektronik.
Layanan administrasi pemerintahan berbasis elektronik merupakan Layanan SPBE yang mendukung tata laksana internal birokrasi dalam rangka meningkatkan kinerja dan akuntabillitas pemerintah di Instansi Pusat dan Pemerintah Daerah.

2) layanan publik berbasis elektronik
Layanan publik berbasis elektronik merupakan Layanan SPBE yang mendukung pelaksanaan pelayanan publik di Instansi Pusat dan Pemerintah Daerah.

3. **Manajemen Sistem Pemerintahan Berbasis Elektronik**.

Manajemen SPBE meliputi:

a. Manajemen risiko

Manajemen risiko bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko dalam SPBE. Manajemen risiko dilakukan melalui serangkaian proses identifikasi, analisis, pengendalian, pemantauan, dan evaluasi terhadap risiko dalam SPBE.

b. Manajemen keamanan informasi

Manajemen keamanan informasi bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan informasi. Manajemen keamanan informasi dilakukan melalui serangkaian proses yang meliputi penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap keamanan informasi dalam SPBE.

c. Manajemen data

Manajemen data bertujuan untuk menjamin terwujudnya data yang akurat, mutakhir, terintegrasi, dan dapat diakses sebagai dasar perencanaan, pelaksanaan, evaluasi, dan pengendalian pembangunan nasional. Manajemen data

dilakukan melalui serangkaian proses pengelolaan arsitektur data, data induk, data referensi, basis data, dan kualitas data.

d. Manajemen aset teknologi informasi dan komunikasi

Manajemen aset teknologi informasi dan komunikasi bertujuan untuk menjamin ketersediaan dan optimalisasi pemanfaatan aset teknologi informasi dan komunikasi dalam SPBE. Manajemen aset teknologi informasi dan komunikasi dilakukan melalui serangkaian proses perencanaan, pengadaan, pengelolaan, dan penghapusan perangkat keras dan perangkat lunak yang digunakan dalam SPBE.

e. Manajemen sumber daya manusia

Manajemen sumber daya manusia bertujuan untuk menjamin keberlangsungan dan peningkatan mutu layanan dalam SPBE. Manajemen sumber daya manusia dilakukan melalui serangkaian proses perencanaan, pengembangan, pembinaan, dan pendayagunaan sumber daya manusia dalam SPBE.

f. Manajemen pengetahuan

Manajemen pengetahuan bertujuan untuk meningkatkan kualitas Layanan SPBE dan mendukung proses pengambilan keputusan dalam SPBE. Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam SPBE.

g. Manajemen perubahan

Manajemen perubahan bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan SPBE melalui pengendalian perubahan yang terjadi dalam SPBE. Manajemen perubahan dilakukan melalui serangkaian proses perencanaan, analisis, pengembangan, implementasi, pemantauan dan evaluasi terhadap perubahan SPBE.

h. Manajemen Layanan SPBE

Manajemen Layanan SPBE bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan SPBE kepada Pengguna SPBE. Manajemen Layanan SPBE dilakukan melalui serangkaian proses pelayanan Pengguna SPBE, pengoperasian Layanan SPBE, dan pengelolaan Aplikasi SPBE.

4. Audit Teknologi Informasi dan Komunikasi

Audit Teknologi Informasi dan Komunikasi terdiri atas:

a. Audit Infrastruktur SPBE

Audit Infrastruktur SPBE terdiri atas:
1) Audit Infrastruktur SPBE Nasional.
2) Audit Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah

b. Audit Aplikasi SPBE.

Audit Aplikasi SPBE terdiri atas:
1) Audit Aplikasi Umum.
2) Audit Aplikasi Khusus

c. Audit Keamanan SPBE.

Audit keamanan SPBE terdiri atas:
1) Audit keamanan Infrastruktur SPBE Nasional.
2) Audit keamanan Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah.
3) Audit keamanan Aplikasi Umum.
4) Audit keamanan Aplikasi Khusus.

5. Penyelenggara Sistem Pemerintahan Berbasis Elektronik.

Untuk meningkatkan keterpaduan pelaksanaan Tata Kelola SPBE, Manajemen SPBE, dan Audit Teknologi Informasi dan Komunikasi, serta pemantauan dan evaluasi SPBE nasional dibentuk Tim Koordinasi SPBE Nasional.

Dalam melaksanakan tugas Tim Koordinasi SPBE Nasional dapat melibatkan menteri/kepala lembaga terkait. Tugas dan tata kerja Tim Koordinasi SPBE Nasional ditetapkan oleh Ketua Tim Koordinasi SPBE Nasional.

6. Percepatan Sistem Pemerintahan Berbasis Elektronik

Untuk meningkatkan kualitas penyelenggaraan pemerintahan dan pelayanan publik, dilakukan percepatan SPBE di Instansi Pusat dan Pemerintah Daerah. Percepatan SPBE dilakukan dengan membangun Aplikasi Umum dan Infrastruktur SPBE Nasional untuk memberikan Layanan SPBE.

Pengaduan Pelayanan Publik

Untuk kecepatan, transparansi, dan akuntabilitas pelayanan publik, dilakukan penerapan pengaduan pelayanan publik berbasis elektronik bagi Instansi Pusat dan Pemerintah Daerah. Penyusunan keterpaduan Proses Bisnis pengaduan pelayanan publik dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan. Keterpaduan Proses Bisnis pengaduan

pelayanan publik diterapkan melalui integrasi layanan pengaduan berbasis elektronik bagi Instansi Pusat dan Pemerintah Daerah. Integrasi layanan pengaduan pelayanan publik dilakukan melalui:

a. Bagi pakai data dan informasi pengaduan pelayanan publik dalam Instansi Pusat, dalam Pemerintah Daerah, dan/atau antar Instansi Pusat dan Pemerintah Daerah.
b. Penyelenggaraan basis data terintegrasi untuk bagi pakai data dan informasi pengaduan pelayanan publik. dan
c. Penyelenggaraan sistem aplikasi pengaduan pelayanan publik yang terintegrasi.

7. Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik

Pemantauan dan evaluasi SPBE bertujuan untuk mengukur kemajuan dan meningkatkan kualitas SPBE di Instansi Fusat dan Pemerintah Daerah. Tim Koordinasi SPBE Nasional melakukan pemantauan dan evaluasi terhadap SPBE secara nasional dan berkala. Koordinator SPBE Instansi Pusat dan Pemerintah Daerah melakukan pemantauan dan evaluasi terhadap SPBE pada Instansi Pusat dan Pemerintah Daerah masing-masing secara berkala. Pelaksanaan pemantauan dan evaluasi SPBE dikoordinasikan oleh menteri yang menyelenggarakan urusan pemerintahan di bidang aparatur negara.

POKOK BAHASAN 4
PERPRES 39 TAHUN 2019 TENTANG
SATU DATA INDONESIA (SDI)

1. Konsep SDI

a. Pengertian

Satu Data Indonesia adalah kebijakan tata kelola Data pemerintah untuk menghasilkan Data yang akurat, mutakhir, terpadu, dan dapat dipertanggungjawabkan, serta mudah diakses dan dibagipakaikan antar Instansi Pusat dan Instansi Daerah melalui pemenuhan Standar Data, Metadata, Interoperabilitas Data, dan menggunakan Kode Rcferensi dan Data Induk.

Portal Satu Data Indonesia adalah media bagi-pakai Data di tingkat nasional yang dapat diakses melalui pemanfaatan teknologi informasi dan komunikasi.

b. Tujuan SDI

1) Memberikan acuan pelaksanaan dan pedoman bagi Instansi Pusat dan hrstansi Daerah dalam rangka penyelenggaraan tata kelola Data untuk mendukung perencanaan, pelaksanaan, evaluasi, dan pengendalian pembangunan.
2) Mewujudkan ketersediaan Data yang akurat, mutakhir, terpadu, dapat dipertanggungjawabkan, serta mudah diakses dan dibagipakaikan antar Instansi Pusat dan Instansi Daerah sebagai dasar perencanaan, pelaksanaan, evaluasi, dan pengendalian pembangunan.
3) Mendorong keterbukaan dan transparansi Data sehingga tercipta perencanaan dan perLrmusan kebijakan pembangunan yang berbasis pada Data.
4) Mendukung sistem statistik nasional peraturan perundang-undangan.

c. Prinsip SDI

1) Data yang dihasilkan oleh Produsen Data harus memenuhi Standar Data.
2) Data yang dihasilkan oleh Produsen Data harus memiliki Metadata.
3) Data yang dihasilkan oleh Produsen Data harus memenuhi kaidah Interoperabilitas Data. dan
4) Data yang dihasilkan oleh Produsen Data harus menggunakan Kode Referensi dan/atau Data Induk

d. Standar Data

Standar Data terdiri atas:

1) Konsep.
   Konsep merupakan ide yang mendasari Data dan tujuan Data tersebut diproduksi.
2) Definisi.
   Definisi merupakan penjelasan tentang Data yang memberi batas atau membedakan secara jelas arti dan cakupan Data tertentu dengan Data yang lain.
3) Klasifikasi.
   Klasifikasi merupakan penggolongan Data secara sistematis ke dalam kelompok atau kategori berdasarkan kriteria yang ditetapkan oleh Pembina Data atau dibakukan secara luas
4) Ukuran.
   Ukuran merupakan unit yang digunakan dalam pengukuran jumlah, kadar, atau cakupan.
5) Satuan.
   Satuan merupakan besaran tertentu dalam Data yang digunakan sebagai standar untuk mengukur atau menakar sebagai sebuah keseluruhan.

e. Metadata

Data yang dihasilkan oleh Produsen Data harus dilengkapi dengan Metadata. Informasi dalam Metadata harus mengikuti struktur yang baku dan format yang baku.

f. Interoperabilitas Data

Untuk memenuhi kaidah Interoperabilitas Data, Data harus:

1) konsisten dalam sintak/bentuk, struktur/skema/komposisi penyajian, dan semantik/ artikulasi keterbacaan. dan
2) disimpan dalam format terbuka yang dapat dibaca sistem elektronik

g. Kode Referensi dan Data Induk

Data yang dihasilkan oleh Produsen Data harus menggunakan Kode Referensi dan/atau Data Induk.

2. Penyelenggara SDI

a. Penyelenggara Satu Data Indonesia Tingkat Pusat

Penyelenggara Satu Data Indonesia tingkat pusat dilaksanakan oleh:

1) Dewan Pengarah.
2) Pembina Data tingkat pusat.

3) Walidata tingkat pusat.
4) Produsen Data tingkat pusat

b. Penyelenggara Satu Data Indonesia Tingkat Daerah

Penyelenggara Satu Data Indonesia dilaksanakan oleh:
1) Pembina Data tingkat daerah.
2) Walidata tingkat daerah.
3) Walidata pendukung. dan
4) Produsen Data tingkat daerah.

3. Penyelenggaraan SDI

Penyelenggaraan Satu Data Indonesia terdiri atas

a. Perencanaan Data.

Instansi Fusat melaksanakan perencanaan Data yang terdiri atas:
1) Penentuan daftar Data yang akan dikumpulkan di tahun selanjutnya.
2) Penentuan daftar Data yang dijadikan Data Prioritas.
3) Penentuan rencana aksi Satu Data Indonesia.

Penentuan daftar Data yang akan dikurnpulkan di tahun selanjutnya dilakukan berdasarkan:

1) Arsitektur sistem pemerintahan berbasis etektronik sesuai dengarr ketentuan peraturan perundang-undangan tentang sistem pemerintahan berbasis elektronik.
2) Kesepakatan forum satu data indonesia.
3) Rekornendasi pembina data.

Daftar Data yang akan dikumpulkan memuat:

1) Produsen Data untuk masing-masing Data.
2) Jadwal rilis dan/atau pemutakhiran Data.

Data yang dapat diusulkan untuk rnenjadi Data Prioritas harus memenuhi kriteria:

1) Mendukung prioritas pembangunan dan prioritas Presiden dalam Rencana Pembangunan Jangka Menengah Nasional dan/atau Rencana Kerja Pemerintah.
2) Mendukung pencapaian tujuan pembangunan berkelanjutan.
3) Memenuhi kebutuhan mendesak.

Rencana aksi Satu Data Indonesia dapat mencakup:

1) Pengembangan sumber daya manusia yang kompeten.
2) Penyusunan petunjuk teknis pelaksanaan Satu Data Indonesia.

3) Kegiatan terkait pengumpulan Data.
4) Kegiatan terkait pemeriksaan Data.
5) Kegiatan terkait penyebarluasan Data.
6) Kegiatan lain yang mendukung tercapainya Data yang sesuai dengan prinsip Satu Data Indonesia.

b. Pengumpulan Data.
Produsen Data melakukan pengumpuian Data sesuai dengan:
1) Standar Data.
2) daftar data yang telah ditentukan dalam Forum Satu Data Indoncsia.
3) jadwal pemutakhiran Data atau rilis Data.
Penyampaian Data disertai:
1) Data yang telah dikumpulkan.
2) Standar Data yang berlaku untuk Data tersebut.
3) Metadata yang melekat pada Data tersebut.

c. Pemeriksaan Data.
Data yang dihasilkan oleh Produsen Data diperiksa kesesuaiannya dengan prinsip Satu Data Indonesia oleh Walidata. Dalam hal Data yang disampaikan oleh Produsen Data belum sesuai dengan prinsip Satu Data Indonesia, Walidata mengembalikan Data tersebut kepada Produsen Data.
Data Prioritas yang dihasilkan oleh Produsen Data diperiksa kesesuaiannya dengan prinsip Satu Data Indonesia oleh Walidata. Hasil pemeriksaan Data Prioritas, diperiksa kembali oleh Pembina Data. Dalam hal Data Prioritas yang disampaikan oleh Produsen Data belum sesuai dengan prinsip Satu Data Indonesia, Pembina Data mengembalikan Data tersebut kepada Walidata. Walidata menyampaikan hasil pemeriksaan Pembina Data kepada Produsen Data. Produsen Data memperbaiki Data sesuai hasil pemeriksaan.

d. Penyebarluasan Data.
Penyebarluasan Data nrerupakan kegiatan pemberian akses, pendistribusian, dan pertukaran Data. Penyebarluasan Data dilakukan oleh Walidata. Penyebarluasan Data dilakukan melalui Portal Satu Data Indonesia dan media lainnya sesuai dengan ketentuan peraturan perundang-undangan dan perkembangan ilmu pengetahuan dan teknologi.

Portal Satu Data Indonesia menyediakan akses:
1) Kode Referensi.
2) Data Induk.
3) Data.
4) Metadata.
5) Data Prioritas.
6) Jadwal rilis dan/atau pemutakhiran Data

	4.	**Partisipasi Lembaga Negara dan Badan Hukum Publik** Lembaga negara dan badan hukum publik, yang meliputi Bank Indonesia, Otoritas Jasa Keuangan, Badan Penyelenggara Jaminan Sosial, dan lembaga negara dan badan hukum publik lainnya dapat berpartisipasi dalam penyelenggaraan Satu Data Indonesia. Partisipasi lembaga negara dan badan hukum publik tidak mengurangi wewenang dan independensi tugas dan fungsinya sesuai dengan ketentuan peraturan perundang-undangan.

RANGKUMAN

1. Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik berisi tentang (1) konsep informasi dan transaksi elektronik. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic maill, telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. (2) informasi, dokumen dan tanda tangan elektronik. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. (3) penyelenggaraan sertifikasi elektronik dan sistem elektronik terdiri atas: Penyelenggara Sertifikasi Elektronik Indonesia dan asing. (4) transaksi elektronik. Penyelenggaraan Transaksi Elektronik dapat dilakukan dalam lingkup publik ataupun privat. Para pihak yang melakukan Transaksi Elektronik wajib beriktikad baik dalam melakukan interaksi dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektronik selama transaksi berlangsung. (5) domain, hak kekayaan intelektual, dan perlindungan hak pribadi. Setiap penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat berhak memiliki Nama Domain berdasarkan prinsip pendaftar pertama. Pemilikan dan penggunaan Nama Domain harus didasarkan pada iktikad baik, tidak melanggar prinsip persaingan usaha secara sehat, dan tidak melanggar hak Orang lain. (6) perbuatan yang dilarang salah satunya antara lain: Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan
2. Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik berisi tentang (1) konsep penyelenggaraan sistem dan transaksi elektronik. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi. mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik. (2) penyelenggara sistem elektronik meliputi Penyelenggara Sistem Elektronik Lingkup Publik dan privat. (3) penyelenggara agen elektronik dapat berbentuk: visual, audio, data elektronik dan bentuk lainnya. (4) penyelenggaraan

transaksi elektronik dalam lingkup publik meliputi Penyelenggaraan Transaksi Elektronik oleh instansi, institusi yang ditunjuk oleh instansi, antar instansi, antar institusi yang ditunjuk, Antara instansi dengan institusi yang ditunjuk dan Antara instansi atau institusi dengan pelaku usaha sesuai dengan ketentuan peraturan perundangundangan. (5) penyelenggaraan sertifikasi elektronik. Penyelenggara Sistem Elektronik wajib memiliki Sertifikat Elektronik. (6) pengelolaan nama domain. Pengelolaan Nama Domain diselenggarakan oleh pengelola Nama Domain

3. Perpres 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) berisi tentang: (1) konsep sistem pemerintahan berbasis elektronik. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE (2) tata kelola sistem pemerintahan berbasis elektronik terdiri dari: rencana induk sistem pemerintahan berbasis elektronik nasional, arsitektur sistem pemerintahan berbasis elektronik, peta rencana sistem pemerintahan berbasis elektronik, rencana dan anggaran sistem pemerintahan berbasis elektronik, data dan informasi, infrastruktur sistem pemerintahan berbasis elektronik, infrastruktur sistem pemerintahan berbasis elektronik instansi pusat dan pemerintah daerah, pusat data nasional, aplikasi sistem pemerintahan berbasis elektronik, keamanan sistem pemerintahan berbasis elektronik, layanan sistem pemerintahan berbasis elektronik. (3) manajemen sistem pemerintahan berbasis elektronik terdiri dari manajemen: risiko, keamanan informasi, data, aset teknologi informasi dan komunikasi, sumber daya manusia, pengetahuan, perubahan, dan Layanan SPBE. (4) audit teknologi informasi dan komunikasi terdiri dari: Audit Infrastruktur SPBE, Audit Aplikasi SPBE, Audit Keamanan SPBE. (5) penyelenggara sistem pemerintahan berbasis elektronik bertujuan untuk meningkatkan keterpaduan pelaksanaan Tata Kelola SPBE, Manajemen SPBE, dan Audit Teknologi Informasi dan Komunikasi, serta pemantauan dan evaluasi SPBE nasional dibentuk Tim Koordinasi SPBE Nasional. (6) percepatan sistem pemerintahan berbasis elektronik dilakukan dengan membangun Aplikasi Umum dan Infrastruktur SPBE Nasional untuk memberikan Layanan SPBE. (7) pemantauan dan evaluasi sistem pemerintahan berbasis elektronik bertujuan untuk mengukur kemajuan dan meningkatkan kualitas SPBE di Instansi Fusat dan Pemerintah Daerah.
4. Perpres 39 Tahun 2019 tentang Satu Data Indonesia (SDI) berisi tentang: (1) konsep SDI. Satu Data Indonesia adalah kebijakan tata kelola Data pemerintah untuk menghasilkan Data yang akurat, mutakhir, terpadu, dan dapat dipertanggungjawabkan,

serta mudah diakses dan dibagipakaikan antar Instansi Pusat dan Instansi Daerah melalui pemenuhan Standar Data, Metadata, Interoperabilitas Data, dan menggunakan Kode Rcferensi dan Data Induk. (2) penyelenggara SDI terdiri dari Penyelenggara Satu Data Indonesia tingkat pusat dan daerah. (3) penyelenggaraan SDI terdiri dari: perencanaan data, pengumpulan data, pemeriksaan data dan penyebarluasan data. (4) partisipasi lembaga negara dan badan hukum publik antara lain Lembaga negara dan badan hukum publik, yang meliputi Bank Indonesia, Otoritas Jasa Keuangan, Badan Penyelenggara Jaminan Sosial, dan lembaga negara dan badan hukum publik lainnya

SOAL LATIHAN

1. Jelaskan konsep informasi dan transaksi elektronik!
2. Jelaskan informasi, dokumen dan tanda tangan elektronik!
3. Jelaskan penyelenggaraan sertifikasi elektronik dan sistem elektronik!
4. Jelaskan transaksi elektronik!
5. Jelaskan domain, hak kekayaan intelektual, dan perlindungan hak pribadi!
6. Jelaskan perbuatan yang dilarang!
7. Jelaskan konsep penyelenggaraan sistem dan transaksi elektronik!
8. Jelaskan penyelenggara sistem elektronik!
9. Jelaskan penyelenggara agen elektronik!
10. Jelaskan penyelenggaraan transaksi elektronik!
11. Jelaskan penyelenggaraan sertifikasi elektronik!
12. Jelaskan pengelolaan nama domain!
13. Jelaskan konsep sistem pemerintahan berbasis elektronik!
14. Jelaskan tata kelola sistem pemerintahan berbasis elektronik!
15. Jelaskan manajemen sistem pemerintahan berbasis elektronik!
16. Jelaskan audit teknologi informasi dan komunikasi!
17. Jelaskan penyelenggara sistem pemerintahan berbasis elektronik!
18. Jelaskan percepatan sistem pemerintahan berbasis elektronik!
19. Jelaskan pemantauan dan evaluasi sistem pemerintahan berbasis elektronik!
20. Jelaskan konsep SDI!
21. Jelaskan penyelenggara SDI!
22. Jelaskan penyelenggaraan SDI!
23. Jelaskan partisipasi lembaga negara dan badan hukum publik!

MODUL 02	**STANDAR NASIONAL INDONESIA (SNI) TENTANG TEKNOLOGI INFORMASI (TI)**
	2 JP (90 menit)

PENGANTAR

Modul ini membahas materi: perencanaan dan pelaksanaan manajemen layanan TI, proses penyampai dan penyampaian layanan TI, proses resolusi layanan TI, proses kontrol layanan TI, Proses rilis layanan TI, perencanaan SMKI, dukungan SMKI, operasi SMKI, evaluasi SMKI dan perbaikan SMKI

Tujuannya agar peserta didik memahami standar nasional Indonesia tentang teknologi informasi

KOMPETENSI DASAR

1. Memahami Standar Nasional Indonesia SNI ISO/IEC 20000 tentang Manajemen Layanan Teknologi Informasi (TI).

   Indikator Hasil Belajar:

   a. Menjelaskan perencanaan dan pelaksanaan manajemen layanan TI.
   b. Menjelaskan proses penyampai dan penyampaian layanan TI.
   c. Menjelaskan proses resolusi layanan TI.
   d. Menjelaskan proses kontrol layanan TI.
   e. Menjelaskan proses rilis layanan TI.

2. Memahami Standar Nasional Indonesia SNI ISO/IEC 27000 tentang Sistem Manajemen Keamanan Informasi (SMKI);

   Indikator Hasil Belajar:

   a. Menjelaskan perencanaan SMKI.
   b. Menjelaskan dukungan SMKI.
   c. Menjelaskan operasi SMKI.
   d. Menjelaskan evaluasi kinerja SMKI.
   e. Menjelaskan perbaikan SMKI.

MATERI PELAJARAN

1. **Pokok Bahasan 1:**

   Standar Nasional Indonesia SNI ISO/IEC 20000 tentang Manajemen Layanan Teknologi Informasi (TI).

   Subpokok Bahasan:

   a. Perencanaan dan pelaksanaan manajemen layanan TI
   b. Proses penyampai dan penyampaian layanan TI.
   c. Proses resolusi layanan TI.
   d. Proses kontrol layanan TI.
   e. Proses rilis layanan TI.

2. **Pokok Bahasan 2:**

   Standar Nasional Indonesia SNI ISO/IEC 27000 tentang Sistem Manajemen Keamanan Informasi (SMKI).

   Subpokok Bahasan:

   a. Perencanaan SMKI.
   b. Dukungan SMKI.
   c. Operasi SMKI.
   d. Evaluasi SMKI.
   e. Perbaikan SMKI.

METODE PEMBELAJARAN

1. **Metode Ceramah**

   Metode ini digunakan untuk menyampaikan materi standar nasional Indonesia tentang teknologi informasi.

2. **Metode Tanya Jawab**

   Metode ini digunakan untuk memperdalam pemahaman materi dan untuk mengetahui tingkat penguasaan materi yang telah disampaikan oleh pendidik tentang materi standar nasional Indonesia tentang teknologi informasi.

ALAT, MEDIA, BAHAN DAN SUMBER BELAJAR

1. Alat, Media dan Bahan:

a. Laptop.
b. LCD.
c. *Flip chart.*
d. *Whiteboard.*
e. Slide.
f. Kertas.
g. Alat tulis.

2. Sumber Belajar:

a. Standar Nasional Indonesia SNI ISO/IEC 20000 tentang Manajemen Layanan Teknologi Informasi.
b. Standar Nasional Indonesia SNI ISO/IEC 27000 tentang Sistem Manajemen Keamanan Informasi.

KEGIATAN PEMBELAJARAN

1. Tahap awal: 10 menit

a. Pendidik melaksanakan apersepsi:
   1) pendidik melaksanakan perkenalan.
   2) pendidik menyampaikan tujuan pembelajaran.
   3) pendidik menciptakan suasana pembelajaran yang kondusif.
b. Peserta didik menyimak, menanggapi dan melaksanakan instruksi pendidik.

2. Tahap inti : 70 menit

a. Pendidik menyampaikan materi tentang standar nasional Indonesia tentang teknologi informasi
b. Pendidik memberikan kesempatan kepada peserta didik untuk bertanya hal-hal yang belum dipahami.
c. Peserta didik menyimak, mencatat, mananggapi dan menanyakan materi yang belum dipahami.
d. Pendidik menanggapi penyataan atau pertanyaan peserta didik.

3. Tahap akhir: 10 menit

a. Pendidik mengecek penguasaan materi dengan cara bertanya secara lisan dan acak kepada peserta didik.

	b. Pendidik memberikan kesimpulan dan penguatan materi standar nasional Indonesia tentang teknologi informasi. c. Pendidik melakukan evaluasi pembelajaran dan menutup pembelajaran.

TAGIHAN/TUGAS

LEMBAR KEGIATAN

BAHAN BACAAN

POKOK BAHASAN 1

STANDAR NASIONAL INDONESIA SNI ISO/IEC 20000 TENTANG MANAJEMEN LAYANAN TEKNOLOGI INFORMASI

1. Rencana dan Pelaksanaan Manajemen Layanan TI

a. Perencanaan manajemen layanan

Tujuan: Untuk merencanakan pelaksanaan dan penyampaian manajemen layanan.

Rencana tersebut minimal menetapkan:

1) Ruang lingkup manajemen layanan layanan penyedia layanan.
2) Tujuan dan persyaratan yang akan dicapai oleh manajemen layanan.
3) Proses yang akan dilaksanakan dalam manajemen layanan.
4) Kerangka kerja posisi dan tanggung jawab manajemen.
5) Pengkoordinasian proses manajemen layanan.
6) Pendekatan dalam mengenali, menilai dan mengelola persoalan serta risiko dalam pencapaian tujuan.
7) Pendekatan dalam setiap antarmuka untuk menciptakan dan memodifikasi layanan.
8) Sumber daya, fasilitas dan anggaran yang diperlukan untuk mencapai tujuan yang ditetapkan.
9) Alat yang tepat untuk menunjang proses layanan.
10) Bagaimana kualitas layanan akan dikelola, diaudit dan ditingkatkan.

b. Melaksanakan manajemen layanan dan menyediakan layanan.

Tujuan untuk melaksanakan tujuan dan rencana manajemen layanan. Penyedia layanan harus melaksanakan rencana manajemen layanan untuk mengelola dan menyampaikan layanan, termasuk:

1) Alokasi dana dan anggaran.
2) Alokasi posisi dan tanggung jawab.
3) Pendokumentasian dan pemeliharaan kebijakan, rencana, prosedur dan ketentuan untuk tiap proses atau sekumpulan proses.
4) Identifikasi dan manajemen resiko untuk layanan.
5) Mengelola kelompok, seperti merekrut dan

mengembangkan pegawai yang tepat dan mengelola pegawai secara menerus.

6) Mengelola fasilitas dan anggaran.
7) Mengelola kelompok termasuk bagian layanan dan pelaksanaan.
8) Melaporkan kemajuan terhadap rencana.
9) Koordinasi proses manajemen layanan.

c. Memonitor, mengukur dan mengkaji

Tujuan untuk mengawasi, mengukur dan mengkaji bahwa tujuan dan rencana manajemen layanan telah tercapai.

Manajemen harus mengadakan pengkajian pada selang waktu yang direncakanan untuk menentukan apakah persyaratan manajemen layanan:

1) Sesuai dengan rencana manajemen layanan dan persyaratan standar ini.
2) Dilaksanakan dan dipelihara secara efektif.

Sebuah program audit harus direncanakan, dengan memperhitungkan status dan tingkat kepentingan proses dan bagian yang diaudit serta hasil dari audit sebelumnya. Kriteria, ruang lingkup, frekuensi dan cara audit harus ditetapkan dalam sebuah prosedur. Pemilihan auditor dan tatalaksana audit harus memastikan keobyektifan dan ketidakberpihakan proses audit. Auditor tidak boleh mengaudit pekerjaan mereka sendiri. Tujuan peninjauan, pengakajian dan audit manajemen layanan harus direkam bersamaan dengan temuan audit dan peninjauan, serta tindakan perbaikan yang diidentifikasi. Tiap bagian penting yang tidak memenuhi atau mengkhawatirkan harus dikomunikasikan pada pihak yang berwenang.

d. Penyempurnaan berkelanjutan:

Tujuan : Untuk meningkatkan keefektifan dan efisiensi manajemen dan penyampaian layanan.

1) Manajemen penyempurnaan

Semua saran untuk penyempurnaan layanan harus dinilai, direkam, diberi urutan prioritas, dan disetujui. Sebuah rencana harus digunakan untuk mengendalikan kegiatan. Penyedia layanan harus mempunyai sebuah proses yang disediakan untuk mengendalikan, mengukur, melaporkan dan mengelola kegiatan penyempurnaan berkelanjutan. Hal ini harus meliputi:

a) Penyempurnaan pada proses individual yang dapat dilaksanakan oleh pemilik proses dengan

sumber daya pegawai biasanya, seperti melakukan tindakan pencegahan dan perbaikan individual;

b) Penyempurnaan lintas organisasi atau lintas lebih dari satu proses.

2) Kegiatan

Penyedia layanan harus melakukan kegiatan untuk:

a) Mengumpulkan dan menganalisa data untuk dijadikan dasar dan tolok ukur kemampuan penyedia layanan untuk mengelola dan menyampaikan layanan dan proses manajemen layanan.
b) Mengenali, merencakanan dan melaksanakan perbaikan.
c) Melakukan konsultasi dengan semua pihak yang terlibat
d) Menentukan target untuk perbaikan penyempurnaan kualitas, biaya dan penggunaan sumber daya.
e) Memperhitungkan masukan yang relevan mengenai perbaikan dari seluruh proses manajemen layanan.
f) Mengukur, melaporkan dan mengomunikasikan perbaikan layanan.
g) Memperbaiki kebijakan, proses, prosedur dan rencana manajemen layanan jika diperlukan
h) Memastikan bahwa seluruh tindakan yang disetujui telah dilaksanakan dan bahwa tindakan tersebut mencapai tujuan yang dimaksud.

e. Merencanakan dan melaksanakan layanan baru atau perubahan layanan

Tujuan: Untuk memastikan bahwa layanan baru dan perubahan pada layanan dapat dilaksanakan dan dapat dikelola dengan biaya dan dilaksanakan dan dapat dikelola dengan biaya dan kualitas layanan yang disetujui.

Rencana harus mencakup:

1) Posisi dan tanggung jawab untuk melaksanakan, mengoperasikan dan memelihara layanan baru atau perubahan layanan, termasuk kegiatan yang dilakukan oleh pelanggan dan pemasok
2) Perubahan pada kerangka kerja manajemen layanan dan layanan yang ada pada saat ini.
3) Komunikasi dengan pihak yang relevan
4) Kontrak dan perjanjian baru atau perubahannya untuk menyesuaikan dengan perubahan dalam kebutuhan

bisnis
5) Perekrutan dan tenaga kerja yang diperlukan
6) Persyaratan keahlian dan pelatihan, contoh pengguna, penunjang teknis.
7) Proses, ukuran, cara dan alat yang digunakan dalam layanan baru atau perubahan layanan seperti manajemen kapasitas, manajemen keuangan
8) Anggaran dan skala waktu
9) Kriteria layanan yang dapat diterima
10) Hasil yang diinginkan dari pengopersian layanan baru yang terukur.

Layanan baru atau perubahan layanan harus disetujui oleh penyedia layanan sebelum diimplementasikan dalam lingkungan yang sebenarnya. Penyedia layanan harus melaporkan hasil yang telah dicapai oleh layanan baru atau perubahan layanan terhadap yang direncanakan setelah pelaksanaannya. Peninjauan pasca pelaksanaan yang membandingkan hasil aktual terhadap yang direncanakan harus dilakukan melalui proses manajemen perubahan.

2. Proses Penyampaian Layanan TI

a. Manajemen tingkat layanan

Tujuan: untuk menetapkan, menyetujui, merekam dan mengelola tingkat layanan. Rangkaian keseluruhan layanan yang harus disediakan bersamaan dengan target dan karakteristik beban kerja tingkat layanan yang harus disetujui oleh pihak terkait dan direkam. Tiap layanan yang disediakan harus ditetapkan, disetujui dan didokumentasikan dalam satu atau lebih perjanjian tingkat layanan (PTL)

b. Pelaporan layanan

Tujuan: untuk menghasilkan laporanan yang akurat, andal, tepat waktu, disetujui untuk pembuatan keputusan yang cerdas dan komunikasi yang efektif. Harus ada gambaran yang jelas untuk tiap laporan layanan termasuk identitas, tujuan pembaca dan detil sumber data.

Laporan layanan harus dibuat untuk memenuhi kebutuhan yang diidentifikasi dan persyaratan pelanggan. Laporan layanan yang harus memasukkan:

1) Kinerja terhadap target tingkat layanan.
2) Ketidaksesuaian dan masalah seperti terhadap PTL, pelanggaran sistem keamanan.
3) Karakteristik beban kerja seperti volume, penggunaan sumber daya
4) Hasil laporan mengenai kejadian besar seperti insiden

dan perubahan besar.
5) Tren informasi
6) Analisa pemenuhan

c. Manajemen kelanjutan layanan dan ketersediaan

Tujuan : untuk memastikan bahwa kelanjutan layanan dan komitmen ketersediaan pada pelanggan yang disetujui dapat dipenuhi dalam segala keadaan.

Persyaratan ketersediaan dan kelanjutan layanan harus diidentifikasi berdasarkan rencana bisnis, PTL dan penilaian risiko.

Persyaratan harus termasuk hak akses dan waktu tanggapan serta serta ketersediaan komponen sistem yang tanpa henti.

d. Penganggaran dan Akuntansi untuk layanan TI

Tujuan : Untuk menganggarkan dan melakukan perhitungan biaya untuk penyediaan layanan.

Penyedia layanan direkomendasikan bahwa ketika penagihan digunakan, mekanisme kerjanya ditetapkan secara menyeluruh dan dimengerti oleh semua pihak.Semua praktik akuntansi yang digunakan harus sesuai dengan praktik akuntansi yang digunakan secara luas oleh organisasi penyedia layanan.

Penyedia layanan harus mengawasi dan melaporkan biaya terhadap anggaran, meninjau ramalan keuangan dan mengelola biaya secara sesuai.Perubahan layanan harus dikenakan biaya dan disetujui melalui proses manajemen perubahan.

e. Manajemen kapasitas

Tujuan: Untuk memastikan bahwa penyedia layanan mempunyai kapasitas yang cukup untuk memenuhi permintaan kebutuhan bisnis pelanggan yang telah disetujui baik pada saat ini maupun saat mendatang.

f. Manajemen keamanan informasi

Tujuan : Untuk mengelola keamanan informasi secara efektif didalam seluruh kegiatan layanan.

Manajemen dengan wewenang yang tepat harus menyetujui sebuah kebijakan keamanan informasi yang harus dikomunikasikan pada seluruh orang yang bersangkutan dan pelanggan yang tepat

Kendali keamanan yang tepat harus bekerja untuk:

1) Melaksanakan persyaratan kebijakan keamanan informasi;

2) Mengelola risiko yang berhubungan dengan akses pada layanan atau sistem.

3. Proses Resolusi Layanan TI

a. Manajemen insiden

Tujuan: untuk mengembalikan layanan yang dijanjikan untuk bisnis secepat mungkin atau untuk menanggapi permintaan layanan.

Seluruh insiden harus direkam. Prosedur harus dipakai untuk mengelola dampak insiden. Prosedur harus menetapkan perekaman, urutan prioritas, dampak bisnis, klasifikasi, pemutakhiran data, perluasan, pemecahan dan penutupan seluruh insiden secara formal. Pelanggan harus tetap diberikan informasi kemajuan dari insiden yang dilaporkan atau permintaan layanan oleh mereka dan diberikan peringatan awal jika tingkat layanan mereka tidak sesuai dan tidak sesuai dan sebuah tindakan disetujui.

b. Manajemen masalah

Tujuan : Untuk meminimalkan gangguan pada bisnis dengan mengenali dan menganalisis secara proaktif akibat insiden dan dengan mengatasi masalah hingga selesai. Seluruh masalah yang diidentifikasi harus direkam.

Prosedur harus dipakai untuk mengenali, meminimalkan atau menghindari dampak insiden dan masalah. Prosedur harus menetapkan rekaman, klasifikasi, pemutakhiran data, perluasan, pemecahan dan penutupan seluruh perluasan, pemecahan dan penutupan seluruh masalah.

Manajemen masalah harus bertanggung jawab untuk memastikan informasi temutakhir mengenai kesalahan yang diketahui dan masalah yang sudah diperbaiki tersedia bagi manajemen insiden. Tindakan untuk perbaikan dan penyempurnaan yang diidentifikasi selama proses ini harus direkam dan menjadi masukan dalam sebuah direkam dan menjadi masukan dalam sebuah rencana untuk peningkatan layanan.

4. Proses Kontrol Layanan TI

a. Manajemen konfigurasi

Tujuan : Untuk menetapkan dan mengendalikan komponen layanan dan infrastruktur dan menjaga keakuratan informasi menjaga keakuratan informasi konfigurasi.

Informasi yang direkam untuk tiap jenis barang harus

	ditentukan dan harus mencakup hubungan dan dokumentasi yang diperlukan untuk manajemen layanan yang efektif. Manajemen konfigurasi harus menyediakan mekanisme untuk mengidentifikasi, mengendalikan, dan mengikuti versi dari komponen yang dapat diidentifikasi dari konfigurasi layanan dan infrastruktur. Hal ini harus dipastikan bahwa tingkat pengendalian cukup untuk memenuhi keperluan bisnis, risiko memenuhi keperluan bisnis, risiko kegagalan dan kegagalan dan layanan yang layanan yang kritis. Manajemen konfigurasi harus menyediakan informasi untuk proses manajemen perubahan mengenai dampak sebuah perubahan yang diminta pada konfigurasi layanan dan infrastruktur. Perubahan pada jenis barang konfigurasi harus dapat diikuti dan diaudit selama sesuai, seperti pada perubahan dan pemindahan perangkat lunak dan perangkat keras. Prosedur kontrol konfigurasi harus memastikan bahwa integritas sistem, layanan dan komponen layanan dipelihara. Sebuah ukuran dasar bagi jenis barang konfigurasi yang tepat harus ditetapkan sebelum penggunaan pada lingkungan yang sebenarnya. Duplikat induk dari jenis barang kofigurasi digital harus dikendalikan dalam perpustakaan elektronik atau fisik yang aman dan dirujuk pada rekaman konfigurasi, seperti perangkat lunak, produk uji, dokumen penunjang. Seluruh jenis barang konfigurasi harus diidentifikasi secara unik dan direkam dalam BDMK dimana pemutakhiran akses harus dikendalikan secara ketat. BDMK harus secara aktif dikelola dan diverifikasi untuk memastikan keandalan dan keakuratannya. Status jenis barang konfigurasi, versi, lokasi, perubahan dan masalah serta dokumentasi terkait harus dapat dilihat dokumentasi terkait harus dapat dilihat untuk merek untuk mereka yang memerlukannya b. Manajemen perubahan Tujuan : Untuk memastikan semua perubahan telah dikaji, disetujui, dilaksanakan, dan ditinjau dalam sebuah cara yang ditinjau dalam sebuah cara yang terkendali. Perubahan layanan dan infrastruktur harus mempunyai ruang lingkup yang terdokumentasi dan ditetapkan secara jelas. Semua permintaan untuk perubahan harus direkam dan diklasifikasikan, seperti penting, darurat, besar, kecil. Permintaan untuk perubahan harus dinilai berdasarkan risiko, dampak dan keuntungan bisnisnya. Proses manajemen perubahan harus mencakup aturan dimana perubahan harus dapat dikembalikan seperti semula atau diperbaiki jika tidak berhasil.

5. Proses Rilis Layanan TI

Tujuan: Untuk menyampaikan, mendistribusikan dan mengikuti satu atau lebih perubahan pada rilis dalam lingkungan yang sebenarnya.

Kebijakan rilis yang menyatakan frekuensi dan tipe rilis harus didokumentasikan dan disetujui. Penyedia layanan harus merencanakan dengan pihak bisnis mengenai rilis layanan, sistem, perangkat lunak dan perangkat keras. Rencana tentang bagaimana mengeluarkan rilis harus disetujui dan disahkan oleh seluruh pihak terkait, seperti pelanggan, pengguna, pegawai pelaksana dan penunjang. Rencana harus merekam waktu rilis dan penyampaian dan merujuk pada permintaan perubahan, kesalahan yang diketahui, dan masalah terkait. Proses manajemen rilis harus memberikan informasi yang sesuai kepada proses manajemen insiden.

Permintaan perubahan harus dikaji berdasarkan dampaknya pada rencana rilis. Prosedur manajemen rilis harus mencakup pemutakhiran dan perubahan informasi konfigurasi dan rekaman perubahan. Rilis darurat harus dikelola sesuai dengan sebuah proses yang ditetapkan yang berantarmuka dengan proses manajemen perubahan darurat.

Rilis dan distribusi harus didesain dan dilaksanakan sehingga integritas perangkat keras dan perangkat lunak terpelihara selama instalasi, penanganan, pengemasan dan penyampaian. Keberhasilan dan kegagalan rilis harus diukur. Pengukuran harus termasuk insiden yang terkait dengan sebuah rilis dalam periode yang mengikuti sebuah rilis.

POKOK BAHASAN 2

STANDAR NASIONAL INDONESIA SNI ISO/IEC 27000 TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI)

1. Perencanaan SMKI

a. Tindakan untuk menangani resiko dan peluang

Ketika merencanakan SMKI organisasi harus mempertimbangkan permasalahan serta menentukan resiko dan peluang yang ditangani untuk:

1) Memastikan SMKI dapat mencapai manfaat yang diharapkan
2) Mencegah, atau mengurangi efek yang tidak diinginkan
3) Mencapai perbaikan yang berkelanjutan

b. Penilaian resiko keamanan informasi

Organisasi harus menetapkan dan menerapkan proses penilaian risiko keamanan informasi, yakni:

1) Menetapkan dan memelihara kriteria risiko keamanan informasiyang meliputi
   a) Kriteria keberterimaan resiko
   b) Kriteria untuk melakukan penilaian resiko keamanan informasi
2) Memastikan bahwa penilaian risiko keamanan informasi yang diulang akan memberikan hasilyang konsisten, valid dan sebanding
3) Mengidentifikasi resiko keamanan informasi
   a) Menerapkan proses penilaian risiko keamanan informasi untuk mengidentifikasi risiko yang terkait dengan hilangnya kerahasiaan, integritas dan ketersediaan informasidalam ruang lingkup SMKI
   b) Mengidentifikasi pemilik risiko
4) Menganalisis risiko keamanan informasi
5) Mengevaluasi risiko keamanan informasi

c. Penanganan risiko keamanan informasi

Organisasi harus menetapkan dan menerapkan proses penanganan risiko keamanan informasi untuk

1) Memilih opsi penanganan risiko keamanan informasi yang tepat, dengan mempertimbangkan hasil penilaian risiko.
2) Menentukan semua kendali yang diperlukan untuk

menerapkan opsi penanganan risiko keamanan informasi yang dipilih

3) Membandingkan kendali yang ditentukan di atas dengan yang ada dalam Lampiran dan memverifikasi bahwa tidak terlewatnya kendali yang diperlukan;
4) Menghasilkan *Statement of Applicabitity* yang berisi kendali yang diperlukan dan alasan pencantuman, apakah kendali itu diterapkan atau tidak, dan alasan pengecualian kendali dari Lampiran A;
5) Merumuskan rencana penanganan risiko keamanan informasi
6) Mendapatkan persetujuan pemilik risiko terhadap rencana penanganan risiko keamanan informasi dan keberterimaan risiko keamanan informasiyang tersisa.

d. Sasaran keamanan informasi dan perencanaan untuk mencapainya

Organisasi harus menetapkan sasaran keamanan informasi pada fungsi dan tingkatan yang relevan. Sasaran keamanan informasi harus:

1) Konsisten dengan fenilJkan keamanan informasi;
2) Dapat diukur (jika dapat diterapkan);
3) Mempertimbangkan persyaratan keamanan informasi yang berlaku, dan hasil dari penilaian risiko dan penanganan risiko;
4) Dikomunikasikan;
5) Diperbarui jika diperlukan

2. Dukungan SMKI

a. Sumber daya

Organisasi harus menentukan dan menyediakan sumber daya yang dibutuhkan untuk penetapan, penerapan, pemeliharaan dan perbaikan berkelanjutan terhadap SMKI.

b. Kompetensi

Organisasi harus:

1) Menentukan kompetensi yang diperlukan untuk personel yang melakukan pekerjaan di bawah kendaliorganisasiyang mempengaruhi kinerja keamanan informasiorganisasi;
2) Memastikan bahwa personel ini kompeten berdasarkan pendidikan, pelatihan, atau pengalaman yang sesuai;
3) Apabila memungkinkan, mengambil tindakan untuk memperoleh kompetensi yang diperlukan, dan mengevaluasi efektivitas tindakan yang diambil;

4) Menyimpan informasi terdokumentasi yang sesuai sebagai alat bukti kompetensi

c. Kepedulian

Personel yang bekerja di bawah kendali organisasi harus peduli terhadap:

1) Kebijakan keamanan informasi;
2) Kontribusinya terhadap efektivitas SMKI, termasuk manfaat peningkatan kinerja keamanan informasi;
3) Implikasi dari ketidaksesuaian dengan persyaratan SMKI.

d. Komunikasi

Organisasi harus menentukan kebutuhan berkomunikasi internal dan eksternal yang relevan dengan SMKI yang mencakup:

1) Apa yang dikomunikasikan;
2) Kapan dikomunikasikan;
3) Dengan siapa dikomunikasikan;
4) Siapa yang harus mengomunikasikan; dan
5) Proses yang dipengaruhi oleh komunikasi tersebut

e. Informasi terdokumentasi

Organisasi SMKI harus mencakup:

1) Informasi terdokumentasi yang disyaratkan.
2) Informasi terdokumentasi yang ditentukan oleh organisasi, sesuai yang diperlukan untuk efektivitas SMKI.

3. Operasi SMKI

a. Perencanaan dan pengendalian operasional

Organisasi harus merencanakan, menerapkan dan mengendalikan proses yang diperlukan untuk memenuhi persyaratan keamanan informasi, dan untuk menerapkan tindakan yang ditentukan. Organisasi juga harus menerapkan rencana untuk mencapai sasaran keamanan informasi yang ditentukan.

Organisasi harus menyimpan informasi terdokumentasi selama yang diperlukan untuk memiliki keyakinan bahwa proses telah dilakukan seperti yang direncanakan. Organisasi harus mengendalikan perubahan yang direncanakan dan mereviu konsekuensi dari perubahan yang tidak diinginkan, mengambil tindakan seperlunya untuk mengurangi efek buruk. Organisasi harus memastikan bahwa proses yang dialih dayakan telah ditetapkan dan dikendalikan.

b. Penilaian resiko keamanan informasi

Organisasi harus melakukan penilaian risiko keamanan informasi pada selang waktu terencana atau ketika perubahan signifikan diusulkan atau terjadi, dengan mempertimbangkan kriteria yang ditetapkan. Organisasi harus menyimpan informasi terdokumentasi dari hasil penilaian risiko keamanan informasi.

c. Penanganan risiko keamanan informasi

Organisasi harus menerapkan rencana penanganan risiko keamanan informasi. Organisasi harus menyimpan informasi terdokumentasi hasil penanganan risiko keamanan informasi.

4. Evaluasi SMKI

a. Pemantauan, pengukuran, analisis dan evaluasi

Organisasi harus mengevaluasi kinerja keamanan informasi dan efektivitas SMKI.

Organisasi harus menentukan:

1) Apa yang perlu dipantau dan diukur, termasuk proses dan pengendalian keamanan informasi;
2) Metode untuk pemantauan, pengukuran, analisis dan evaluasi, jika dapat diterapkan, untuk memastikan hasil yang valid.
3) Kapan pemantauan dan pengukuran harus dilakukan;
4) Siapa yang harus memantau dan mengukur;
5) Kapan hasil dari pemantauan dan pengukuran harus dianalisis dan dievaluasi; dan
6) Siapa yang harus menganalisis dan mengevaluasi hasil tersebut

b. Audit internal

Organisasi harus melakukan audit internal pada selang waktu terencana untuk memberikan informasi apakah SMKI:

1) Sesuai dengan persyaratan yang ditetapkan organisasi untuk SMKInya dan persyaratan standar ini
2) Diimplementasikan dan dipelihara secara efektif
3) Organisasi harus merencanakan, menetapkan dan memelihara program audit termasuk frekuensi, metode, tanggung jawab, persyaratan perencanaan dan pelaporan. Program audit harus mempertimbangkan pentingnya proses yang bersangkutan dan hasil audit sebelumnya.
4) Menentukan kriteria audit dan ruang lingkup untuk setiap audit

5) Memilih auditor dan melakukan audit yang menjamin objektivitas dan ketidakberpihakan proses audit
6) Memastikan bahwa hasil audit tersebut dilaporkan kepada manajemen yang relevan; dan
7) Menyimpan informasi terdokumentasi sebagai alat bukti dari program audit dan hasil audit

c. Reviu manajemen

Reviu manajemen harus mencakup pertimbangan:

1) Status tindakan dari reviu manajemen sebelumnya;
2) Perubahan isu eksternaldan internalyang relevan dengan SMKI;
3) Umpan balik dari kinerja keamanan informasi, termasuk kecenderungan dalam hal:
   a) Ketidaksesuaian dan tindakan korektif;
   b) Hasll pemantauan dan pengukuran;
   c) Hasil audit;
   d) Pemenuhan terhadap sasaran keamanan informasi
4) Umpan balik dari pihak yang berkepentingan;
5) Hasil penilaian risiko dan status rencana penanganan risiko;
6) Peluang untuk perbaikan berkelanjutan

5. Perbaikan SMKI

a. Ketidaksesuaian dan tindakan korektif

Jika terjadi ketidaksesuaian, organisasi harus:

1) Bereaksi terhadap ketidaksesuaian, dan jika dapat diterapkan
2) Mengevaluasi kebutuhan tindakan untuk menghilangkan penyebab ketidaksesuaian, agaihal itu tidak terulang atau terjadi di tempat lain, dengan cara:
   a) Mereviu ketidaksesuaian;
   b) Menentukan penyebab ketidaksesuaian; dan
   c) Menentukan apakah ada ketidaksesuaian serupa, atau berpotensiterjadi kembali;
3) Melaksanakan tindakan apapun yang diperlukan;
4) Mereviu efektivitas tindakan korektif apapun yang diambil;
5) Membuat perubahan pada SMKI, jika diperlukan.
6) Sifat ketidaksesuaian dan tindakan berikutnya yang diambil.
7) Hasil dari setiap tindakan korektif.

	b. Perbaikan berkelanjutan Organisasi harus terus memperbaiki kesesuaian, kecukupan dan efektivitas SMKI

RANGKUMAN

1. Standar Nasional Indonesia SNI ISO/IEC 20000 tentang Manajemen Layanan Teknologi Informasi (TI) berisi tentang: (1) perencanaan dan pelaksanaan manajemen layanan TI. Tujuan: Untuk merencanakan pelaksanaan dan penyampaian manajemen layanan. (2) proses penyampai dan penyampaian layanan TI terdiri dari: Manajemen tingkat layanan, Pelaporan layanan, Manajemen kelanjutan layanan dan ketersediaan, Penganggaran dan Akuntansi untuk layanan TI, Manajemen kapasitas, dan Manajemen keamanan informasi. (3) proses resolusi layanan TI terdiri dari: Manajemen insiden dan Manajemen masalah. (4) proses kontrol layanan TI terdiri dari: Manajemen konfigurasi dan Manajemen perubahan. (5) proses rilis layanan TI bertujuan untuk menyampaikan, mendistribusikan dan mengikuti satu atau lebih perubahan pada rilis dalam lingkungan yang sebenarnya
2. Standar Nasional Indonesia SNI ISO/IEC 27000 tentang Sistem Manajemen Keamanan Informasi (SMKI) berisi tentang (1) perencanaan SMKI. Ketika merencanakan SMKI organisasi harus mempertimbangkan permasalahan serta menentukan resiko dan peluang yang ditangani. (2) dukungan SMKI terdiri dari sumber daya, kompetensi, kepedulian, komunikasi, dan informasi terdokumentasi. (3) operasi SMKI terdiri dari: Perencanaan dan pengendalian operasional, Penilaian resiko keamanan informasi, dan Penanganan risiko keamanan informasi. (4) evaluasi kinerja SMKI terdiri dari Pemantauan, pengukuran, analisis dan evaluasi, audit internal dan reviu manajemen. (5) perbaikan SMKI. Jika terjadi ketidaksesuaian, organisasi salah satunya harus: mengevaluasi kebutuhan tindakan untuk menghilangkan penyebab ketidaksesuaian

SOAL LATIHAN

1. Jelaskan perencanaan dan pelaksanaan manajemen layanan TI!
2. Jelaskan proses penyampai dan penyampaian layanan TI!
3. Jelaskan proses resolusi layanan TI!
4. Jelaskan proses kontrol layanan TI!
5. Jelaskan proses rilis layanan TI!
6. Jelaskan perencanaan SMKI!
7. Jelaskan dukungan SMKI!
8. Jelaskan operasi SMKI!
9. Jelaskan evaluasi kinerja SMKI!
10. Jelaskan perbaikan SMKI!