



SALINAN

BUPATI JOMBANG  
PROVINSI JAWA TIMUR

PERATURAN BUPATI JOMBANG  
NOMOR 81 TAHUN 2023

TENTANG

PEDOMAN MANAJEMEN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN  
AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI DI LINGKUP PEMERINTAH  
KABUPATEN JOMBANG

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI JOMBANG.

Menimbang : a. bahwa untuk mengukur tingkat kematangan domain Manajemen Sistem Pemerintahan Berbasis Elektronik sesuai petunjuk Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik, perlu ditetapkan dengan Peraturan Bupati;

b. bahwa untuk melaksanakan sebagaimana dimaksud pada huruf a, perlu menetapkan Pedoman Manajemen Sistem Pemerintahan Berbasis Elektronik dan Audit Teknologi Informasi dan Komunikasi di Lingkup Pemerintah Kabupaten Jombang dalam Peraturan Bupati;

Mengingat : 1. Undang-Undang Nomor 12 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Jawa Timur (Berita Negara Republik Indonesia Tahun 1950 Nomor 41) sebagaimana telah diubah dengan Undang-Undang Nomor 2 Tahun 1965 (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 19, Tambahan Lembaran Negara Republik Indonesia Nomor 2730);

2. Undang-Undang Nomor 17 Tahun 2003 tentang Keuangan Negara (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 47, Tambahan Lembaran Negara Republik Indonesia Nomor 4286);

3. Undang-Undang Nomor 1 Tahun 2004 tentang Perbendaharaan Negara (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 5, Tambahan Lembaran Negara Republik Indonesia Nomor 4355);

4. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);

5. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 125, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 9 Tahun 2015 (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
6. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
7. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 994);
10. Pedoman Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 6 Tahun 2023 tentang Tata Cara Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
11. Peraturan Daerah Kabupaten Jombang Nomor 1 Tahun 2019 tentang Rencana Pembangunan Jangka Menengah Daerah Kabupaten Jombang Tahun 2018-2023 (Lembaran Daerah Kabupaten Jombang Tahun 2019 Nomor 1/E) sebagaimana telah diubah dengan Peraturan Daerah Kabupaten Jombang Nomor 8 Tahun 2021 (Lembaran Daerah Kabupaten Jombang Tahun 2021 Nomor 8/E);
12. Peraturan Bupati Jombang Nomor 15 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Jombang (Berita Daerah Kabupaten Jombang Tahun 2021 Nomor 15/E);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG PEDOMAN MANAJEMEN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI DI LINGKUP PEMERINTAH KABUPATEN JOMBANG.

## Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Jombang.
2. Pemerintah Daerah adalah Pemerintah Kabupaten Jombang.
3. Bupati adalah Bupati Jombang.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Jombang.
5. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
6. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
7. Manajemen SPBE adalah serangkaian proses untuk mencapai penerapan SPBE yang efektif, efisien dan berkesinambungan, serta layanan SPBE yang berkualitas.
8. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
9. Arsitektur SPBE Pemerintah Daerah adalah kerangka dasar yang mendeskripsikan integrasi proses bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, dan keamanan SPBE untuk menghasilkan layanan SPBE yang terintegrasi.

## Pasal 2

Manajemen SPBE di lingkungan Pemerintah Daerah Kabupaten Jombang meliputi:

- a. Pedoman Manajemen Risiko SPBE;
- b. Pedoman Manajemen Keamanan Informasi SPBE;
- c. Pedoman Manajemen Data SPBE;
- d. Pedoman Manajemen Aset Teknologi dan Komunikasi SPBE;
- e. Pedoman Manajemen Sumber Daya Manusia SPBE;
- f. Pedoman Manajemen Pengetahuan SPBE;
- g. Pedoman Manajemen Perubahan SPBE;
- h. Pedoman Manajemen Layanan SPBE;
- i. Pedoman Audit Infrastruktur SPBE;
- j. Pedoman Audit Aplikasi SPBE; dan
- k. Pedoman Audit Keamanan SPBE

## Pasal 3

Pedoman mengenai penerapan Manajemen SPBE dan Audit Teknologi Informasi dan Komunikasi sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal 4

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.  
Agar setiap orang mengetahuinya, memerintahkan pengundangan  
Peraturan Bupati ini dengan penempatannya dalam Berita Daerah  
Kabupaten Jombang.

Ditetapkan di Jombang  
Pada tanggal 10 Juli 2023  
BUPATI JOMBANG,

ttd

MUNDJIDAH WAHAB

Diundangkan di Jombang  
pada tanggal 10 Juli 2023  
SEKRETARIS DAERAH  
KABUPATEN JOMBANG,

ttd

AGUS PURNOMO  
BERITA DAERAH KABUPATEN JOMBANG TAHUN 2023 NOMOR 81/E



**BAB I**  
**PEDOMAN MANAJEMEN RISIKO**  
**SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK**

**I. PENDAHULUAN**

Revolusi Teknologi Informasi dan Komunikasi (TIK) memberikan peluang bagi pemerintah untuk melakukan inovasi pembangunan aparatur negara melalui penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) atau E-Government, yaitu penyelenggaraan pemerintahan yang memanfaatkan TIK untuk memberikan layanan kepada instansi pemerintah, Aparatur Sipil Negara (ASN), pelaku bisnis, masyarakat, dan pihak-pihak lainnya. Penerapan SPBE akan mendorong dan mewujudkan penyelenggaraan pemerintahan yang terbuka, partisipatif, inovatif, dan akuntabel, meningkatkan kolaborasi antar instansi pemerintah dalam melaksanakan urusan dan tugas pemerintahan untuk mencapai tujuan bersama, meningkatkan kualitas dan jangkauan pelayanan publik kepada masyarakat luas, dan menekan tingkat penyalahgunaan kewenangan dalam bentuk kolusi, korupsi, dan nepotisme melalui penerapan sistem pengawasan dan pengaduan masyarakat berbasis elektronik. Momentum pengembangan SPBE telah dimulai sejak diterbitkannya Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government dimana menteri, kepala lembaga, dan kepala daerah diinstruksikan untuk melaksanakan pengembangan SPBE sesuai tugas, fungsi, kewenangan, dan kapasitas sumber daya yang dimilikinya.

Berbagai penerapan SPBE telah dihasilkan oleh Pemerintah Daerah dan telah memberi kontribusi dan efektivitas penyelenggaraan pemerintahan. Namun demikian, hasil pengembangan SPBE menunjukkan tingkat maturitas yang relatif rendah dan kesenjangan yang tinggi antara Pemerintah Daerah. Berdasarkan hasil evaluasi SPBE tahun 2018 pada 616 Pemerintah Daerah, indeks SPBE Nasional mencapai nilai 1,98 dengan predikat Cukup dari target indeks SPBE sebesar 2,6 dari 5 (lima) level dengan predikat Baik. Ditinjau dari capaian Pemerintah Daerah, rata-rata indeks SPBE Instansi Pusat sebesar 2,6 dengan predikat Baik, sementara rata-rata indeks SPBE Pemerintah Daerah sebesar 1,87 dengan predikat Cukup. Ditinjau dari sebaran capaian target, 13,3% Pemerintah Daerah telah mencapai atau melebihi target indeks SPBE 2,6, sedangkan 86,7% belum mencapai target indeks SPBE 2,6. Hal ini menunjukkan adanya permasalahan dalam pengembangan SPBE secara nasional.

Permasalahan pertama adalah belum adanya tata kelola SPBE yang terpadu di tingkat nasional maupun di tingkat Pemerintah Daerah. Berdasarkan kajian Dewan Teknologi Informasi dan Komunikasi Nasional tahun 2016, ditemukan bahwa 65% dari belanja perangkat lunak (aplikasi). Digunakan untuk membangun aplikasi yang sejenis antar instansi pemerintah. Disamping itu, berdasarkan survei infrastruktur Pusat Data termasuk ruang server yang dilakukan oleh Kementerian Komunikasi dan Informatika tahun 2018 terdapat 2700 pusat data dan ruang server di 630 Pemerintah Daerah, yang berarti rata-rata terdapat 4 (empat) pusat data dan ruang server di setiap Pemerintah Daerah. Rata rata utilisasi pusat data dan ruang server secara nasional hanya mencapai 30% dari kapasitas tersedia. Fakta ini menunjukkan adanya ego sektoral dan sulitnya koordinasi di dalam dan antar Pemerintah Daerah sehingga menyebabkan terjadi duplikasi anggaran belanja dan kapasitas yang melebihi kebutuhan.

Permasalahan kedua adalah belum optimalnya penerapan layanan SPBE yang terpadu. Sebagaimana diketahui bahwa proses perencanaan, penganggaran, pengadaan, pelaporan keuangan, pemantauan dan evaluasi,

dan akuntabilitas kinerja adalah saling terkait antara satu proses dengan proses lainnya. Saat ini, penerapan layanan perencanaan, penganggaran, pengadaan, pelaporan keuangan, pemantauan dan evaluasi, dan akuntabilitas kinerja diwujudkan dalam bentuk sistem aplikasi yang berdiri sendiri di sebagian besar Instansi Pemerintah. Kondisi sistem aplikasi yang berdiri sendiri berlaku pula pada layanan kepegawaian, kearsipan, dan pelayanan publik lainnya. Permasalahan layanan SPBE yang belum terpadu dapat mengakibatkan kualitas pelaksanaan kegiatan pemerintah menjadi kurang efektif dan kurang efisien.

Permasalahan ketiga adalah terbatasnya jumlah pegawai ASN yang memiliki kompetensi TIK untuk mendukung SPBE. Saat ini terjadi kesenjangan antara standar kompetensi jabatan fungsional ASN terkait dengan TIK seperti Jabatan Fungsional Pranata Komputer dan Jabatan Fungsional Sandiman dengan standar kompetensi okupasi TIK yang diakui oleh industri TIK. Peningkatan kapasitas pegawai ASN melalui pelatihan di bidang TIK belum dapat dipenuhi dikarenakan terbatasnya anggaran. Di sisi lain, permintaan Sumber Daya Manusia (SDM) TIK di pasar tenaga kerja termasuk di Instansi Pemerintah tidak diimbangi dengan ketersediaan SDM TIK itu sendiri. Hal ini dapat mengakibatkan terganggunya pengoperasian aplikasi, infrastruktur TIK, dan keamanan untuk memberikan layanan SPBE yang terbaik.

Di sisi lain, perkembangan tren TIK 4.0 merupakan faktor kunci eksternal yang mampu mendorong terwujudnya penerapan SPBE yang terpadu dan peningkatan kualitas layanan SPBE yang memudahkan pengguna dalam mengakses layanan pemerintah. Beberapa tren TIK 4.0 yang berkembang antara lain : pertama, teknologi mobile internet dapat dimanfaatkan untuk kemudahan akses layanan pemerintah melalui gawai personal pengguna yang bebas bergerak tanpa batasan waktu dan lokasi; kedua, teknologi cloud computing memberikan efektivitas dan efisiensi yang tinggi untuk melakukan integrasi TIK; ketiga, teknologi internet of things (IoT) mampu memberikan layanan yang bersifat adaptif dan responsif terhadap kebutuhan kustomisasi layanan yang diinginkan pengguna serta memperluas persediaan kanal-kanal layanan pemerintah; keempat, teknologi big data analytics mampu memberikan dukungan pengambilan keputusan dan penyusunan kebijakan bagi pemerintah; dan kelima, teknologi artificial intelligence dapat membantu pemerintah dalam mengurangi beban administrasi seperti penerjemahan dokumen dalam bentuk tulisan suara serta membantu publik dalam memecahkan permasalahan yang kompleks seperti kesehatan dan keuangan.

Adanya permasalahan penerapan SPBE dan tren revolusi TIK 4.0 melahirkan sejumlah risiko yang dapat berpengaruh terhadap pencapaian tujuan SPBE. Permasalahan penerapan SPBE dapat berkontribusi pada risiko negatif yang dapat menghambat pencapaian tujuan SPBE. Sementara tren revolusi TIK 4.0 dapat berkontribusi pada risiko positif yang dapat meningkatkan peluang keberhasilan pencapaian tujuan SPBE. Oleh karena itu, berbagai risiko yang timbul dalam penerapan SPBE harus dikelola dengan baik oleh Pemerintah Daerah sebagai penyelenggara SPBE. Untuk menjamin keberlangsungan penerapan SPBE, diperlukan manajemen risiko SPBE yang dilaksanakan oleh Pemerintah Daerah untuk mencapai tujuan SPBE sebagaimana diamanatkan dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

Pedoman Manajemen Risiko SPBE dimaksudkan untuk memberikan panduan bagi Pemerintah Daerah dalam melaksanakan Manajemen Risiko SPBE di lingkungannya. Sedangkan tujuan dari Manajemen Risiko SPBE adalah :

1. Meningkatkan kemungkinan pencapaian tujuan penerapan SPBE di Pemerintah Daerah;

2. Memberikan dasar yang kuat untuk perencanaan dan pengambilan keputusan melalui penyajian informasi Risiko SPBE yang memadai di Pemerintah Daerah dalam penerapan SPBE;
3. Meningkatkan optimalisasi pemanfaatan sumberdaya SPBE di Pemerintah Daerah dalam penerapan SPBE;
4. Meningkatkan kepatuhan kepada peraturan dalam penerapan SPBE; dan
5. Menciptakan budaya sadar Risiko SPBE bagi pegawai ASN di lingkungan Pemerintah Daerah dalam penerapan SPBE.

Manfaat dari penerapan Manajemen Risiko SPBE dalam penerapan SPBE adalah :

1. Mewujudkan tata kelola pemerintahan yang efektif, efisien, transparan, dan akuntabel melalui penerapan SPBE di Pemerintah Daerah;
2. Mewujudkan penerapan SPBE yang terpadu di Pemerintah Daerah;
3. Meningkatkan kinerja pemerintahan di Pemerintah Daerah;
4. Meningkatkan reputasi dan kepercayaan pemangku kepentingan kepada Pemerintah Daerah; dan
5. Mewujudkan budaya kerja yang profesional dan berintegritas di Pemerintah Daerah.

Ruang lingkup Pedoman Manajemen Risiko SPBE yang menjadi fokus pembahasan mencakup:

1. Kerangka kerja Manajemen Risiko SPBE;
2. Proses Manajemen Risiko SPBE;
3. Struktur Manajemen Risiko SPBE; dan
4. Budaya sadar Risiko SPBE

## **II. DEFINISI**

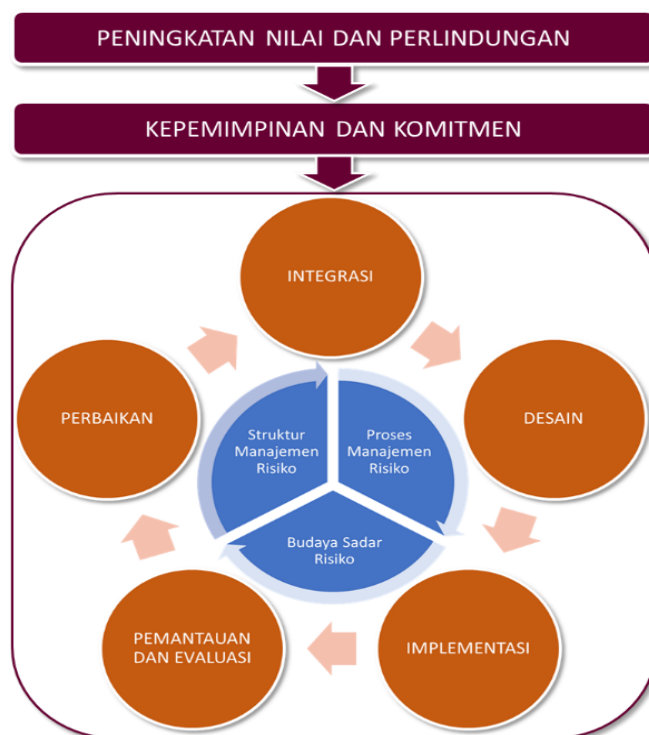
1. Manajemen Risiko SPBE adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur, dan budaya untuk menentukan tindakan terbaik terkait Risiko SPBE.
2. Risiko SPBE adalah peluang terjadinya suatu peristiwa yang akan mempengaruhi keberhasilan terhadap pencapaian tujuan penerapan SPBE.
3. Risiko SPBE Positif adalah peluang terjadinya suatu peristiwa yang akan meningkatkan keberhasilan terhadap pencapaian tujuan penerapan SPBE.
4. Risiko SPBE Negatif adalah peluang terjadinya suatu peristiwa yang akan menurunkan keberhasilan terhadap pencapaian tujuan penerapan SPBE.
5. Kategori Risiko SPBE adalah pengelompokan Risiko SPBE berdasarkan karakteristik penyebab Risiko SPBE yang menggambarkan seluruh jenis Risiko SPBE yang terdapat pada Pemerintah Daerah.
6. Area Dampak Risiko SPBE adalah pengelompokan area yang terkena dampak dari Risiko SPBE.
7. Kriteria Risiko SPBE adalah parameter atau ukuran secara kuantitatif atau kualitatif yang digunakan untuk menentukan Kriteria Kemungkinan Risiko SPBE dan Kriteria Dampak Risiko SPBE.
8. Kriteria Kemungkinan Risiko SPBE adalah besarnya peluang terjadinya suatu Risiko SPBE dalam periode tertentu
9. Kriteria Dampak Risiko SPBE adalah besarnya akibat terjadinya suatu Risiko SPBE yang mempengaruhi sasaran SPBE.
10. Besaran Risiko SPBE adalah nilai Risiko SPBE yang dihasilkan dari proses analisis Risiko SPBE.
11. Level Risiko SPBE adalah pengelompokan Besaran Risiko SPBE yang mendeskripsikan tingkat Risiko SPBE.
12. Selera Risiko SPBE adalah penentuan Besaran Risiko SPBE di Pemerintah Daerah yang dapat diterima atau ditangani.

## **III. KEBIJAKAN PENYELENGGARAAN**

Kerangka kerja Manajemen Risiko SPBE mendeskripsikan komponen

dasar yang digunakan sebagai landasan penerapan Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah. Tujuan dari kerangka kerja Manajemen Risiko SPBE adalah untuk membantu Instansi Pusat dan Pemerintah Daerah dalam mengintegrasikan Manajemen Risiko SPBE ke dalam kegiatan pelaksanaan tugas dan fungsi Instansi Pusat dan Pemerintah Daerah. Agar Manajemen Risiko SPBE dapat dilaksanakan dengan baik, Instansi Pusat dan Pemerintah Daerah dapat mengadopsi secara langsung atau memodifikasi kerangka kerja Manajemen Risiko SPBE ini sesuai dengan konteks internal dan eksternal di lingkungannya masing-masing.

Komponen dasar dari kerangka kerja ini terdiri atas prinsip mengenai peningkatan nilai dan perlindungan, kepemimpinan dan komitmen, serta proses dan tata kelola Manajemen Risiko SPBE sebagaimana terlihat pada Gambar 1.



Gambar 1. Kerangka Kerja Manajemen Risiko SPBE

#### A. Peningkatan Nilai dan Perlindungan

Prinsip utama dari penerapan Manajemen Risiko SPBE adalah menciptakan peningkatan nilai tambah dan perlindungan bagi Instansi Pusat dan Pemerintah Daerah dalam penerapan SPBE. Prinsip utama tersebut memiliki karakteristik sebagai berikut:

1. Terintegrasi, yaitu Manajemen Risiko SPBE merupakan serangkaian proses yang terintegrasi dengan proses pelaksanaan tugas dan fungsi Instansi Pusat dan Pemerintah Daerah;
2. Terstruktur dan komprehensif, yaitu Manajemen Risiko SPBE dibangun secara terstruktur, sistematis, dan menyeluruh untuk memberikan kontribusi terhadap efisiensi dan konsistensi hasil yang dapat diukur dalam peningkatan kualitas penerapan SPBE;
3. Dapat disesuaikan, yaitu kerangka kerja dan proses Manajemen Risiko SPBE dapat disesuaikan dengan konteks internal dan eksternal Instansi Pusat dan Pemerintah Daerah dalam penerapan SPBE;
4. Inklusif, yaitu Manajemen Risiko SPBE melibatkan semua pemangku kepentingan sesuai dengan pengetahuan, pandangan, dan persepsinya untuk membangun budaya sadar Risiko SPBE di Instansi Pusat dan Pemerintah Daerah;
5. Dinamis, yaitu Manajemen Risiko SPBE dapat dipergunakan untuk



mengantisipasi dan merespon perubahan konteks Instansi Pusat dan Pemerintah Daerah dengan tepat dan sesuai waktu;

6. Informasi tersedia dan terbaik, yaitu informasi yang digunakan sebagai masukan dalam proses Manajemen Risiko SPBE didasarkan pada data historis, pengalaman, observasi, perkiraan, penilaian ahli, dan data dukung lain yang tersedia di Instansi Pusat dan Pemerintah Daerah;
7. Faktor manusia dan budaya, yaitu keberhasilan penerapan Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah dipengaruhi oleh kapasitas, persepsi, kesungguhan, dan budaya kerja dari pegawai ASN yang terlibat dalam penerapan SPBE; dan
8. Perbaikan berkelanjutan, yaitu Manajemen Risiko SPBE senantiasa dikembangkan melalui strategi perbaikan manajemen secara berkelanjutan dan peningkatan kematangan penerapan Manajemen Risiko SPBE.

## B. Kepemimpinan dan Komitmen

Pimpinan Instansi Pusat dan Pemerintah Daerah hendaknya menunjukkan kepemimpinan dan komitmen dalam penerapan kerangka kerja Manajemen Risiko SPBE melalui proses:

### 1. Integrasi

Kerangka kerja Manajemen Risiko SPBE hendaknya diintegrasikan dengan proses pelaksanaan tugas dan fungsi Instansi Pusat dan Pemerintah Daerah. Integrasi dapat dilakukan dengan memahami struktur dan konteks organisasi yang didasarkan pada tujuan, sasaran, dan kompleksitas organisasi.

Berdasarkan struktur dan konteks organisasi tersebut, tata kelola Manajemen Risiko SPBE perlu dibangun dengan menyusun struktur Manajemen Risiko SPBE beserta tugas-tugasnya untuk menjalankan, mengendalikan, dan melakukan pengawasan terhadap penerapan proses Manajemen Risiko SPBE dalam rangka mencapai sasaran dan target kinerja organisasi dalam penerapan SPBE.

### 2. Desain

Perancangan kerangka kerja Manajemen Risiko SPBE dilakukan dengan cara:

- a) Memahami struktur dan konteks organisasi termasuk tujuan, sasaran, dan kompleksitas organisasi;
- b) Mengekspresikan komitmen pimpinan terhadap penerapan kerangka kerja Manajemen Risiko SPBE dalam bentuk kebijakan, pernyataan, atau bentuk dukungan lainnya;
- c) Menetapkan kewenangan, tanggung jawab, dan akuntabilitas dari setiap peran di dalam kerangka kerja Manajemen Risiko SPBE;
- d) Menyediakan sumber daya yang diperlukan seperti SDM dan kompetensi, anggaran, proses dan prosedur, informasi dan pengetahuan, dan pelatihan; dan
- e) Membangun komunikasi dan konsultasi untuk efektivitas implementasi kerangka kerja Manajemen Risiko SPBE.

### 3. Implementasi

Kerangka kerja Manajemen Risiko SPBE diterapkan dengan melibatkan semua pemangku kepentingan di Instansi Pusat dan Pemerintah Daerah melalui penyusunan rencana, penyediaan sumber daya, pembuatan keputusan, dan pelaksanaan Manajemen Risiko SPBE.

### 4. Pemantauan dan Evaluasi

Untuk mengukur efektivitas implementasi kerangka kerja Manajemen Risiko SPBE, pimpinan Instansi Pusat dan Pemerintah Daerah perlu melakukan pemantauan dan evaluasi secara berkala untuk pengukuran kinerja dan kesesuaian kerangka kerja

Manajemen Risiko SPBE terhadap tujuan dan sasaran SPBE.

5. Perbaikan

Hasil pemantauan dan evaluasi kerangka kerja Manajemen Risiko SPBE digunakan untuk melakukan perubahan dan perbaikan kerangka kerja Manajemen Risiko SPBE secara berkelanjutan sehingga kesesuaian, kecukupan, dan efektivitas dari kerangka kerja tersebut dapat ditingkatkan.

C. Proses dan Tata Kelola Manajemen Risiko SPBE

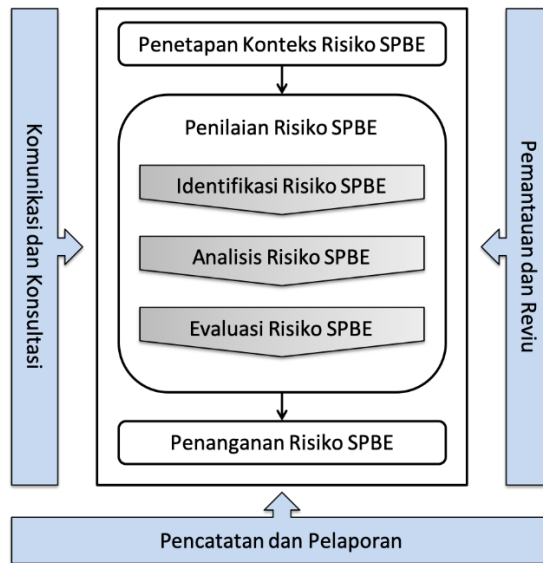
Proses Manajemen Risiko SPBE merupakan rangkaian proses yang sistematis dan menjadi bagian dari proses pelaksanaan tugas dan fungsi Instansi Pusat dan Pemerintah Daerah untuk pengambilan keputusan di tingkat strategis, operasional, dan pelaksanaan proyek. Proses Manajemen Risiko SPBE yang dilaksanakan oleh Instansi Pusat dan Pemerintah Daerah terdiri atas proses:

1. komunikasi dan konsultasi;
2. penetapan konteks Risiko SPBE;
3. penilaian Risiko SPBE, yang terdiri atas identifikasi Risiko SPBE, analisis Risiko SPBE, dan evaluasi Risiko SPBE;
4. penanganan Risiko SPBE;
5. pemantauan dan reuiu;
6. pencatatan dan pelaporan.

Sedangkan, tata kelola Manajemen Risiko SPBE merupakan mekanisme untuk mengatur kewenangan dan memastikan akuntabilitas pelaksanaan Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah. Dalam hal ini, tata kelola Manajemen Risiko SPBE dibangun dengan menyusun struktur Manajemen Risiko SPBE dan membangun budaya sadar Risiko SPBE. Struktur Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah sedikitnya terdiri atas fungsi yang terkait dengan strategi dan kebijakan, pelaksanaan, dan pengawasan Manajemen Risiko SPBE. Selain itu, budaya sadar Risiko SPBE perlu dibangun dan dikembangkan oleh Instansi Pusat dan Pemerintah Daerah melalui perencanaan, pelaksanaan, dan pemantauan dan evaluasi kegiatan budaya sadar Risiko SPBE.

**IV. STANDAR PENYELENGGARAAN**

Proses Manajemen Risiko SPBE merupakan penerapan secara sistematis dari kebijakan, prosedur, dan praktik terhadap aktivitas komunikasi dan konsultasi, penetapan konteks, penilaian risiko (identifikasi risiko, analisis risiko, evaluasi risiko), penanganan risiko, pemantauan dan reuiu, serta pencatatan dan pelaporan. Proses Manajemen Risiko SPBE diilustrasikan pada Gambar 2.



Gambar 2. Proses Manajemen Risiko

A. Komunikasi dan Konsultasi

Komunikasi dan konsultasi merupakan proses yang berkelanjutan dan berulang untuk menyediakan, membagikan, ataupun mendapatkan informasi dan menciptakan dialog dengan para pemangku kepentingan mengenai Risiko SPBE. Komunikasi dilakukan untuk meningkatkan kesadaran dan pemahaman mengenai Risiko SPBE. Sementara konsultasi dilakukan untuk mendapatkan umpan balik dan informasi dalam rangka mendukung pengambilan keputusan.

Bentuk kegiatan komunikasi dan konsultasi antara lain:

1. Rapat berkala, merupakan rapat yang diadakan secara rutin;
2. Rapat insidental, merupakan rapat yang diadakan sewaktu-waktu; dan
3. Focus Group Discussion (FGD), merupakan kelompok diskusi yang terarah untuk membahas topik tertentu.

B. Penetapan Konteks Risiko SPBE

Penetapan konteks Risiko SPBE bertujuan untuk mengidentifikasi parameter dasar dan ruang lingkup penerapan Risiko SPBE yang harus dikelola dalam proses Manajemen Risiko SPBE. Tahapan penetapan konteks meliputi:

1. Inventarisasi Informasi Umum

Inventarisasi informasi umum bertujuan untuk mendapatkan gambaran umum mengenai unit kerja yang menerapkan Manajemen Risiko SPBE. Informasi yang dicantumkan meliputi nama Unit Pemilik Risiko (UPR) SPBE, tugas UPR SPBE, fungsi UPR SPBE, dan periode waktu pelaksanaan Manajemen Risiko SPBE dalam kurun waktu satu tahun. Informasi umum dituangkan ke dalam Formulir 2.1 seperti terlihat pada Tabel 1 di bawah ini.

Tabel 1  
Contoh Pengisian Formulir 2.1 Informasi Umum

Informasi Umum	
Nama UPR SPBE	Deputi Bidang Kelembagaan dan Tata Laksana
Tugas UPR SPBE	Menyelenggarakan perumusan kebijakan serta koordinasi dan sinkronisasi pelaksanaan kebijakan di bidang kelembagaan dan ketatalaksanaan Pemerintah
Fungsi UPR SPBE	1. perumusan kebijakan di bidang kelembagaan pemerintahan 2. perumusan kebijakan di bidang ketatalaksanaan pemerintahan, penyelenggaraan administrasi pemerintahan, dan pengembangan penerapan

	sistem pemerintahan berbasis elektronik
Periode Waktu	1 Januari - 31 Desember 2019

## 2. Identifikasi Sasaran SPBE

Identifikasi sasaran SPBE bertujuan untuk menentukan sasaran SPBE beserta indikator dan targetnya yang mendukung sasaran unit kerja sebagai UPR SPBE. Informasi yang dicantumkan meliputi:

- Sasaran UPR SPBE, diisi dengan sasaran unit kerja sebagai UPR SPBE yang tertuang dalam dokumen rencana strategis, rencana kerja, penetapan kinerja, atau dokumen perencanaan lainnya;
- Sasaran SPBE, diisi dengan sasaran SPBE yang mendukung sasaran UPR SPBE;
- Indikator Kinerja SPBE, diisi dengan indikator kinerja SPBE yang mendeskripsikan pencapaian sasaran SPBE; dan

- Target Kinerja SPBE, diisi dengan target kinerja SPBE yang mendeskripsikan ukuran indikator kinerja untuk pencapaian sasaran SPBE.

Informasi sasaran SPBE dituangkan ke dalam Formulir 2.2 seperti terlihat pada Tabel 2 di bawah ini.

Tabel 2  
Contoh Pengisian Formulir 2.2 Sasaran SPBE

No	Sasaran UPR SPBE	Sasaran SPBE	Indikator Kinerja SPBE	Target Kinerja SPBE
1	Terwujudnya tata kelola pemerintahan yang berbasis elektronik	Meningkatnya Kualitas Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik	Indeks SPBE Nasional Jumlah Instansi Pemerintah yang mencapai predikat SPBE "Baik"	2,1  121 IP

## 3. Penentuan Struktur Pelaksana Manajemen Risiko SPBE

Penentuan struktur pelaksana Manajemen Risiko SPBE bertujuan untuk menentukan unit kerja yang bertanggung jawab atas pelaksanaan Manajemen Risiko SPBE. Penentuan struktur pelaksana Manajemen Risiko SPBE meliputi:

- Unit Pemilik Risiko SPBE;
- Pemilik Risiko SPBE;
- Koordinator Risiko SPBE; dan
- Pengelola Risiko SPBE.

Informasi struktur pelaksana Manajemen Risiko SPBE dituangkan ke dalam Formulir 2.3 seperti terlihat pada Tabel 3 di bawah ini

Tabel 3  
Contoh Pengisian Formulir 2.3 Struktur Pelaksana Manajemen Risiko SPBE

Struktur Pelaksana Manajemen Risiko SPBE	
Pemilik Risiko SPBE	Rini Widyantini Deputi Bidang Kelembagaan dan Tata Laksana
Koordinator Risiko SPBE	T. Eddy Syahputra Sekretaris Deputi Bidang Kelembagaan dan Tata Laksana
Pengelola Risiko SPBE	Imam Machdi Asisten Deputi SPBE

## 4. Identifikasi Pemangku Kepentingan

Identifikasi pemangku kepentingan bertujuan untuk mendapatkan informasi dan memahami pihak-pihak yang melakukan interaksi dengan UPR SPBE dalam rangka pencapaian sasaran SPBE. Pihak-pihak tersebut meliputi unit kerja internal, unit kerja eksternal, instansi pemerintah, atau non instansi pemerintah. Hubungan kerja antara UPR SPBE dan setiap pihak pemangku kepentingan yang terkait dengan penerapan SPBE perlu dideskripsikan dengan jelas. Daftar pemangku kepentingan dituangkan ke dalam Formulir 2.4 seperti terlihat pada Tabel 4 di bawah ini.

Tabel 4  
Contoh Pengisian Formulir 2.4 Daftar Pemangku Kepentingan

No	Nama Unit/Instansi	Hubungan
1	Perguruan Tinggi (UI, UGM, PENS, Tel-U, UG)	Pelaksana evaluasi SPBE sebagai evaluator eksternal
2	Badan Siber dan Sandi Negara	Penyedia layanan repositori data evaluasi SPBE

#### 5. Identifikasi Peraturan Perundang-Undangan

Identifikasi peraturan perundang-undangan bertujuan untuk memahami kewenangan, tanggung jawab, tugas dan fungsi, serta kewajiban hukum yang harus dilaksanakan oleh UPR SPBE. Informasi yang perlu dijelaskan dalam melakukan identifikasi peraturan perundang-undangan meliputi nama peraturan dan amanat dalam peraturan tersebut. Daftar peraturan dituangkan ke dalam Formulir 2.5 seperti terlihat pada Tabel 5 di bawah ini.

Tabel 5  
Contoh Pengisian Formulir 2.5 Daftar Peraturan Perundang-Undangan

No	Nama Peraturan	Amanat
1	Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik	<p>Pasal 70</p> <p>(1) Pemantauan dan evaluasi SPBE bertujuan untuk mengukur kemajuan dan meningkatkan kualitas SPBE di Instansi Pusat dan Pemerintah Daerah.</p> <p>(2) Tim Koordinasi SPBE Nasional melakukan pemantauan dan evaluasi terhadap SPBE secara nasional dan berkala.</p> <p>(3) Koordinator SPBE Instansi Pusat dan Pemerintah Daerah melakukan pemantauan dan evaluasi terhadap SPBE pada Instansi Pusat dan Pemerintah Daerah masing-masing secara berkala.</p> <p>(4) Pelaksanaan pemantauan dan evaluasi SPBE sebagaimana dimaksud pada ayat (3) dikoordinasikan oleh menteri yang menyelenggarakan urusan pemerintahan di bidang aparatur negara.</p>
2	Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2018 tentang Pedoman Evaluasi SPBE	<p>Pasal 6</p> <p>Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi melakukan:</p> <p>a. pembinaan, koordinasi, pemantauan, dan/atau supervisi terhadap evaluasi mandiri Sistem Pemerintahan Berbasis Elektronik; dan</p> <p>b. penyusunan profil nasional pelaksanaan Sistem Pemerintahan Berbasis Elektronik berdasarkan hasil evaluasi eksternal.</p>

#### 6. Penetapan Kategori Risiko SPBE

Penetapan Kategori Risiko SPBE bertujuan untuk menjamin agar proses identifikasi, analisis, dan evaluasi Risiko SPBE dapat dilakukan secara komprehensif. Kategori Risiko SPBE meliputi:

- a) Rencana Induk SPBE Nasional, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan pelaksanaan perencanaan pembangunan SPBE Nasional;

- b) Arsitektur SPBE, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan pemanfaatan arsitektur SPBE yang mendeskripsikan integrasi proses bisnis, data dan informasi, infrastruktur SPBE, dan keamanan SPBE;
- c) Peta Rencana SPBE, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan pelaksanaan Peta Rencana SPBE;
- d) Proses Bisnis, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan penerapan proses bisnis SPBE;
- e) Rencana dan Anggaran, merupakan Risiko SPBE yang berkaitan dengan proses perencanaan dan penganggaran SPBE;
- f) Inovasi, merupakan Risiko SPBE yang berkaitan dengan ide baru atau pemikiran kreatif yang memberikan nilai manfaat dalam penerapan SPBE;
- g) Kepatuhan terhadap Peraturan, merupakan Risiko SPBE yang berkaitan dengan kepatuhan unit kerja di lingkungan Instansi Pusat dan Pemerintah Daerah terhadap peraturan perundang-undangan, kesepakatan internasional, maupun ketentuan lain yang berlaku;
- h) Pengadaan Barang dan Jasa, merupakan Risiko SPBE yang berkaitan dengan proses pengadaan dan penyediaan barang dan jasa;
- i) Proyek Pembangunan/Pengembangan Sistem, merupakan Risiko SPBE yang berkaitan dengan proyek pembangunan ataupun pengembangan sistem pada penerapan SPBE;
- j) Data dan Informasi, merupakan Risiko SPBE yang berkaitan dengan semua data dan informasi yang dimiliki oleh Instansi Pusat dan Pemerintah Daerah;
- k) Infrastruktur SPBE, merupakan Risiko SPBE yang berkaitan dengan pusat data, jaringan intra pemerintah, dan sistem penghubung layanan pemerintah termasuk perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama;
- l) Aplikasi SPBE, merupakan Risiko SPBE yang berkaitan dengan program komputer yang diterapkan untuk melakukan tugas atau fungsi layanan SPBE;
- m) Keamanan SPBE, merupakan Risiko SPBE yang berkaitan dengan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya yang mendukung SPBE;
- n) Layanan SPBE, merupakan Risiko SPBE yang berkaitan dengan pemberian layanan SPBE kepada Pengguna SPBE;
- o) Sumber Daya Manusia SPBE, merupakan Risiko SPBE yang berkaitan dengan SDM yang bekerja sebagai penggerak penerapan SPBE di Instansi Pusat dan Pemerintah Daerah; dan
- p) Bencana Alam, merupakan Risiko SPBE yang berkaitan dengan peristiwa yang disebabkan oleh alam.

Kategori Risiko SPBE dapat disesuaikan dengan konteks internal dan eksternal di masing-masing Instansi Pusat dan Pemerintah Daerah. Kategori Risiko SPBE dituangkan ke dalam Formulir 2.6 seperti terlihat pada Tabel 6 di bawah ini.

Tabel 6  
Formulir 2.6 Kategori Risiko SPBE

No	Kategori Risiko SPBE
1	Rencana Induk SPBE Nasional
2	Arsitektur SPBE
3	Peta Rencana SPBE
4	Proses Bisnis
5	Rencana dan Anggaran

6	Inovasi
7	Kepatuhan terhadap Peraturan
8	Pengadaan Barang dan Jasa
9	Proyek Pembangunan/Pengembangan Sistem
10	Data dan Informasi
11	Infrastruktur SPBE
12	Aplikasi SPBE
13	Keamanan SPBE
14	Layanan SPBE
15	SDM SPBE
16	Bencana Alam

#### 7. Penetapan Area Dampak Risiko SPBE

Penetapan Area Dampak Risiko SPBE bertujuan untuk mengetahui area mana saja yang terkena efek dari Risiko SPBE di Instansi Pusat dan Pemerintah Daerah. Penetapan Area Dampak Risiko SPBE diawali dengan melakukan identifikasi dampak Risiko SPBE. Area Dampak Risiko SPBE yang menjadi fokus penerapan Manajemen Risiko SPBE meliputi:

- a) Finansial, dampak Risiko SPBE berupa aspek yang berkaitan dengan keuangan;
- b) Reputasi, dampak Risiko SPBE berupa aspek yang berkaitan dengan tingkat kepercayaan pemangku kepentingan;
- c) Kinerja, dampak Risiko SPBE berupa aspek yang berkaitan dengan pencapaian sasaran SPBE;
- d) Layanan Organisasi, dampak Risiko SPBE berupa aspek yang berkaitan dengan pemenuhan kebutuhan atau jasa kepada pemangku kepentingan;
- e) Operasional dan Aset TIK, dampak Risiko SPBE berupa aspek yang berkaitan dengan kegiatan operasional TIK dan pengelolaan aset TIK;
- f) Hukum dan Regulasi, dampak Risiko SPBE berupa aspek yang berkaitan dengan peraturan perundang-undangan dan kebijakan; dan
- g) Sumber Daya Manusia, dampak Risiko SPBE berupa aspek yang berkaitan dengan fisik dan mental pegawai.

Area Dampak Risiko SPBE terdiri atas area dampak positif dan/atau negatif. Area Dampak Risiko SPBE dapat disesuaikan dengan konteks internal dan eksternal di masing-masing Instansi Pusat dan Pemerintah Daerah. Area Dampak Risiko SPBE dituangkan ke dalam Formulir 2.7 seperti terlihat pada Tabel 7 di bawah ini

Tabel 7  
Formulir 2.7 Area Dampak Risiko SPBE

No	Area Dampak Risiko SPBE
1	Finansial
2	Reputasi
3	Kinerja
4	Layanan Organisasi
5	Operasional dan Aset TIK
6	Hukum dan Regulasi
7	Sumber Daya Manusia

#### 8. Penetapan Kriteria Risiko SPBE

Penetapan Kriteria Risiko SPBE bertujuan untuk mengukur dan menetapkan seberapa besar kemungkinan kejadian dan dampak Risiko SPBE yang dapat terjadi. Kriteria Risiko SPBE ini ditinjau secara berkala dan perlu melakukan penyesuaian dengan perubahan yang terjadi. Penetapan Kriteria Risiko SPBE ini terdiri atas:

## a) Kriteria Kemungkinan SPBE

Penetapan Kriteria Kemungkinan Risiko SPBE dilakukan berdasarkan penetapan level kemungkinan dan penetapan kriteria dari setiap level kemungkinan terhadap Risiko SPBE. Instansi Pusat dan Pemerintah Daerah dapat menggunakan level kemungkinan dengan 3 level, 4 level, 5 level, atau level lainnya yang disesuaikan dengan kompleksitas Risiko SPBE. Untuk 5 level kemungkinan, dapat diuraikan sebagai berikut:

- 1) Hampir Tidak Terjadi;
- 2) Jarang Terjadi;
- 3) Kadang-Kadang Terjadi;
- 4) Sering Terjadi;
- 5) Hampir Pasti Terjadi.

Sedangkan, penetapan kriteria kemungkinan dilakukan melalui pendekatan persentase probabilitas statistik, jumlah frekuensi terjadinya suatu Risiko SPBE dalam satuan waktu, ataupun berdasarkan expert judgement. Selanjutnya, kriteria kemungkinan dituliskan pada setiap level kemungkinan yang dituangkan ke dalam Formulir 2.8.A seperti terlihat pada Tabel 8 di bawah ini.

Tabel 8  
Contoh Pengisian Formulir 2.8.A Kriteria Kemungkinan Risiko SPBE

Level Kemungkinan		Persentase Kemungkinan Terjadinya dalam Satu Tahun	Jumlah Frekuensi Kemungkinan Terjadinya dalam Satu Tahun
1	Hampir Tidak Terjadi	$X \leq 5\%$	$X < 2$ kali
2	Jarang Terjadi	$5\% < X \leq 10\%$	$2 \leq X \leq 5$ kali
3	Kadang-Kadang Terjadi	$10\% < X \leq 20\%$	$6 \leq X \leq 9$ kali
4	Sering Terjadi	$20\% < X \leq 50\%$	$10 \leq X \leq 12$ kali
5	Hampir Pasti Terjadi	$X > 50\%$	$> 12$ kali

## b) Kriteria Dampak SPBE

Penetapan Kriteria Dampak Risiko SPBE dilakukan dengan kombinasi antara Area Dampak Risiko SPBE (sepaimana dijelaskan pada angka 7 di atas tentang Penetapan Area Dampak Risiko SPBE) dan level dampak. Instansi Pusat dan Pemerintah Daerah dapat menggunakan 3 level, 4 level, 5 level, atau level dampak lainnya yang disesuaikan dengan kompleksitas Risiko SPBE. Untuk 5 level dampak, dapat diuraikan sebagai berikut:

- 1) Tidak Signifikan;
- 2) Kurang Signifikan;
- 3) Cukup Signifikan;
- 4) Signifikan;
- 5) Sangat Signifikan.

Kriteria Dampak Risiko SPBE dijabarkan untuk setiap Area Dampak Risiko SPBE Positif dan Area Dampak Risiko SPBE Negatif terhadap setiap level dampak ke dalam Formulir 2.8.B seperti terlihat pada Tabel 9 di bawah ini.

Tabel 9  
Contoh Pengisian Formulir 2.8.B Kriteria Dampak Risiko SPBE

Area Dampak	Level Dampak				
	1	2	3	4	5
	Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan



Kinerja	Positif	Peningkatan kinerja < 20%	Peningkatan kinerja 20% s.d < 40%	Peningkatan kinerja 40% s.d < 60%	Peningkatan kinerja 60% s.d < 80%	Peningkatan kinerja > 80%
	Negatif	Penurunan kinerja < 20%	Penurunan kinerja 20% s.d < 40%	Penurunan kinerja 40% s.d < 60%	Penurunan kinerja 60% s.d < 80%	Penurunan kinerja >= 80%

#### 9. Matriks Analisis Risiko SPBE dan Level Risiko SPBE

Matriks analisis Risiko SPBE berisi kombinasi antara level kemungkinan dan level dampak untuk dapat menetapkan Besaran Risiko SPBE yang direpresentasikan dalam bentuk angka. Besaran Risiko SPBE kemudian dimasukkan ke dalam Formulir 2.9.A seperti terlihat pada Tabel 10 di bawah ini.

Tabel 10  
Contoh Pengisian Formulir 2.9.A Matriks Analisis Risiko SPBE

Matriks Analisis Risiko 5 x 5			Level Dampak				
			1	2	3	4	5
			Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Level Kemungkinan	5	Hampir Pasti Terjadi	9	15	18	23	25
	4	Sering Terjadi	6	12	16	19	24
	3	Kadang-Kadang Terjadi	4	10	14	17	22
	2	Jarang Terjadi	2	7	11	13	21
	1	Hampir Tidak Terjadi	1	3	5	8	20

Besaran Risiko SPBE ini selanjutnya dikelompokkan ke dalam Level Risiko SPBE dimana setiap Level Risiko SPBE memiliki rentang nilai Besaran Risiko SPBE. Pemilihan Level Risiko SPBE dapat menggunakan 3 level, 4 level, 5 level, atau Level Risiko SPBE lainnya yang disesuaikan dengan kompleksitas Risiko SPBE. Setiap level tersebut direpresentasikan dengan warna sesuai dengan preferensi masing-masing Instansi Pusat dan Pemerintah Daerah. Untuk 5 Level Risiko SPBE, dapat diuraikan sebagai berikut:

- Sangat Rendah, direpresentasikan dengan warna biru;
- Rendah, direpresentasikan dengan warna hijau;
- Sedang, direpresentasikan dengan warna kuning;
- Tinggi, direpresentasikan dengan warna jingga;
- Sangat Tinggi, direpresentasikan dengan warna merah.

Nilai rentang Besaran Risiko dituangkan ke dalam Formulir 2.9.B seperti terlihat pada Tabel 11 di bawah ini.

Tabel 11  
Contoh Pengisian Formulir 2.9.B Level Risiko SPBE

Level Risiko	Rentang Besaran Risiko	Keterangan Warna	
1	Sangat Rendah	1-5	Biru
2	Rendah	6-10	Hijau
3	Sedang	11-15	Kuning
4	Tinggi	16-20	Jingga

5	Sangat Tinggi	21-25	Merah
---	---------------	-------	-------

#### 10. Selera Risiko SPBE

Selera Risiko SPBE bertujuan untuk memberikan acuan dalam penentuan ambang batas minimum terhadap Besaran Risiko SPBE yang harus ditangani untuk setiap Kategori Risiko SPBE baik Risiko SPBE Positif maupun Risiko SPBE Negatif. Penentuan Selera Risiko SPBE ini dapat disesuaikan dengan kompleksitas Risiko SPBE serta konteks internal dan eksternal masing-masing Instansi Pusat dan Pemerintah Daerah. Besaran Risiko yang ditangani pada setiap Kategori Risiko SPBE dituangkan ke dalam Formulir 2.10 seperti terlihat pada Tabel 12 di bawah ini.

Tabel 12  
Contoh Pengisian Formulir 2.10 Selera Risiko SPBE

No	Kategori Risiko SPBE	Besaran Risiko Minimum yang Ditangani	
		Risiko SPBE Positif	Risiko SPBE Negatif
1	Rencana dan Anggaran	16	6
2	Pengadaan Barang dan Jasa	18	11
3	SDM SPBE	20	14

#### C. Penilaian Risiko SPBE

Penilaian Risiko SPBE pada penerapan SPBE dilakukan melalui proses identifikasi, analisis, dan evaluasi Risiko SPBE. Penilaian Risiko SPBE bertujuan untuk memahami penyebab, kemungkinan, dan dampak Risiko SPBE yang dapat terjadi di Instansi Pusat dan Pemerintah Daerah. Penilaian Risiko SPBE dilakukan pada setiap Sasaran SPBE. Tahapan penilaian Risiko SPBE meliputi:

##### 1. Identifikasi Risiko SPBE

Identifikasi Risiko SPBE merupakan proses menggali informasi mengenai kejadian, penyebab, dan dampak Risiko SPBE. Informasi yang dicantumkan meliputi:

##### a) Jenis Risiko SPBE

Jenis Risiko SPBE terbagi menjadi Risiko SPBE positif dan Risiko SPBE negatif. Dalam melakukan identifikasi Risiko SPBE, Risiko SPBE dituliskan ke dalam masing-masing jenis Risiko SPBE.

##### b) Kejadian

Kejadian dapat diidentifikasi dari terjadinya suatu peristiwa yang menimbulkan Risiko SPBE yang diperoleh dari riwayat peristiwa dan/atau prediksi terjadinya peristiwa di masa yang akan datang. Kejadian selanjutnya disebut sebagai Risiko SPBE.

##### c) Penyebab

Penyebab dapat diidentifikasi dari akar masalah yang menjadi pemicu munculnya Risiko SPBE. Penyebab dapat berasal dari lingkungan internal maupun eksternal Instansi Pusat dan Pemerintah Daerah. Identifikasi penyebab akan membantu menemukan tindakan yang tepat untuk menangani Risiko SPBE.

##### d) Kategori

Penentuan Kategori Risiko SPBE didasarkan pada penyebab dari munculnya Risiko SPBE. Kategori Risiko SPBE telah dijelaskan pada bagian huruf B angka 6 tentang Penetapan Kategori Risiko SPBE.

##### e) Dampak

Dampak dapat diidentifikasi dari pengaruh atau akibat yang timbul dari Risiko SPBE.

## f) Area Dampak

Penentuan Area Dampak Risiko SPBE didasarkan pada dampak yang telah teridentifikasi. Area Dampak Risiko telah dijelaskan pada bagian huruf B angka 7 tentang Penetapan Area Dampak. Proses Identifikasi Risiko SPBE dituangkan ke dalam Formulir 3.0 pada bagian Identifikasi Risiko SPBE seperti terlihat pada Tabel 13.

Tabel 13  
Contoh Pengisian Formulir 3.0 Penilaian Risiko SPBE Bagian Identifikasi Risiko SPBE

Identifikasi Risiko SPBE					
Jenis Risiko SPBE	Kejadian	Penyebab	Kategori	Dampak	Area Dampak
Positif	Respon dari K/L/D sangat antusias	Adanya mandat dari Peraturan Presiden No 95 Tahun 2018	Kepatuhan terhadap Peraturan	Peningkatan kualitas layanan SPBE	Kinerja
Negatif	Terdapat K/L/D yang tidak dievaluasi	Kurangnya jumlah evaluator eksternal	SDM SPBE	Penurunan kinerja	Kinerja

## 2. Analisis Risiko SPBE

Analisis Risiko SPBE merupakan proses untuk melakukan penilaian atas Risiko SPBE yang telah diidentifikasi sebelumnya. Analisis Risiko SPBE dilakukan dengan cara menentukan sistem pengendalian, level kemungkinan, dan level dampak terjadinya Risiko SPBE. Informasi yang dicantumkan pada analisis Risiko SPBE meliputi:

## a) Sistem Pengendalian

- 1) Sistem pengendalian internal mencakup perangkat manajemen yang dapat menurunkan/meningkatkan level Risiko SPBE dalam rangka pencapaian sasaran SPBE.
- 2) Sistem pengendalian internal dapat berupa Standard Operating Procedure (SOP), pengawasan melekat, reviu berjenjang, regulasi, dan pemantauan rutin yang dilaksanakan terkait Risiko SPBE tersebut.

## b) Level Kemungkinan

Penentuan level kemungkinan dilakukan dengan mengukur persentase probabilitas atau frekuensi peluang terjadinya Risiko SPBE dalam satu periode yang dicocokkan dengan Kriteria Kemungkinan Risiko SPBE sebagaimana telah dijelaskan pada bagian huruf B angka 8 huruf a. Penentuan level kemungkinan harus didukung dengan penjelasan singkat untuk mengetahui alasan pemilihan level kemungkinan tersebut.

## c) Level Dampak

Penentuan level dampak dilakukan dengan mengukur besar dampak dari terjadinya Risiko SPBE yang dicocokkan dengan Kriteria Dampak Risiko SPBE sebagaimana telah dijelaskan pada bagian huruf B angka 8 huruf b. Level dampak harus didukung dengan penjelasan singkat untuk mengetahui alasan pemilihan level dampak tersebut.

## d) Besaran Risiko SPBE dan Level Risiko SPBE

Penentuan Besaran Risiko SPBE dan Level Risiko SPBE didapat dari kombinasi Level Kemungkinan dan Level Dampak dengan menggunakan rumusan dalam Matriks Analisis Risiko SPBE sebagaimana telah dijelaskan pada bagian huruf B angka 9.

Proses Analisis Risiko SPBE dituangkan ke dalam Formulir 3.0 pada bagian Analisis Risiko SPBE seperti terlihat pada Tabel 14 di bawah ini.

Tabel 14  
Contoh Pengisian Formulir 3.0 Penilaian Risiko SPBE Bagian Analisis Risiko SPBE

Analisis Risiko SPBE						
Sistem Pengendalian	Kemungkinan		Dampak		Besaran Risiko SPBE	Level Risiko SPBE
	Level	Penjelasan	Level	Penjelasan		
Konfirmasi Keikutsertaan dalam evaluasi SPBE	Hampir Pasti Terjadi	Keikutsertaan lebih dari 80%	Sangat Signifikan	Peningkatan kinerja hingga 80%	25	Sangat Tinggi
Analisis beban kerja evaluator eksternal	Kadang-Kadang Terjadi	Terjadi sekitar 15% dalam satu periode	Cukup Signifikan	Penurunan kinerja hingga 50%	14	Sedang

### 3. Evaluasi Risiko SPBE

Evaluasi Risiko SPBE dilakukan untuk mengambil keputusan mengenai perlu tidaknya dilakukan upaya penanganan Risiko SPBE lebih lanjut serta penentuan prioritas penanganannya. Pengambilan keputusan mengacu pada Selera Risiko SPBE yang telah ditentukan sebagaimana telah dijelaskan pada bagian huruf B angka 10. Prioritas penanganan Risiko SPBE diurutkan berdasarkan Besaran Risiko SPBE. Apabila terdapat lebih dari satu Risiko SPBE yang memiliki besaran yang sama maka cara penentuan prioritas berdasarkan expert judgement. Proses Evaluasi Risiko SPBE dituangkan ke dalam Formulir 3.0 pada bagian Penilaian Risiko SPBE seperti terlihat pada Tabel 15 di bawah ini.

Tabel 15  
Contoh Pengisian Formulir 3.0 Penilaian Risiko SPBE Bagian Evaluasi Risiko SPBE

Evaluasi Risiko PBE	
Keputusan Penanganan Risiko SPBE (Ya/Tidak)	Prioritas Penanganan Risiko SPBE
Ya	1
Ya	2

### D. Penanganan Risiko SPBE

Penanganan Risiko SPBE merupakan proses untuk memodifikasi penyebab Risiko SPBE. Penanganan Risiko SPBE dilakukan dengan mengidentifikasi berbagai opsi yang mungkin diterapkan dan memilih satu atau lebih opsi penanganan Risiko SPBE. Informasi yang dicantumkan pada penanganan Risiko SPBE meliputi:

#### 1. Prioritas Risiko

Prioritas Risiko SPBE diurutkan berdasarkan Besaran Risiko SPBE. Risiko SPBE yang memiliki prioritas lebih tinggi ditunjukkan dengan nilai Besaran Risiko SPBE yang lebih tinggi.

## 2. Rencana Penanganan Risiko SPBE

Rencana penanganan Risiko SPBE merupakan agenda kegiatan untuk menangani Risiko SPBE agar mencapai Selera Risiko SPBE yang telah ditetapkan. Rencana penanganan Risiko SPBE dilakukan dengan mengidentifikasi hal-hal sebagai berikut:

### a) Opsi Penanganan Risiko SPBE

Opsi penanganan Risiko SPBE, berisikan alternatif yang dipilih untuk menangani Risiko SPBE. Opsi penanganan Risiko SPBE dilakukan dengan mengidentifikasi berbagai opsi yang mungkin untuk diterapkan. Opsi penanganan Risiko SPBE terbagi menjadi dua, yaitu penanganan Risiko SPBE Positif dan penanganan Risiko SPBE Negatif. Adapun opsi yang ditentukan pada pedoman ini meliputi:

#### 1) Opsi Penanganan Risiko Positif

##### (a) Eskalasi Risiko

Eskalasi risiko dipilih jika Risiko SPBE berada di luar atau melampaui wewenang. Opsi ini dilakukan dengan memindahkan tanggung jawab penanganan Risiko SPBE ke unit kerja yang lebih tinggi.

##### (b) Eksploitasi Risiko

Eksploitasi risiko dipilih jika Risiko SPBE dapat dipastikan terjadi. Opsi ini dilakukan dengan cara memanfaatkan Risiko SPBE tersebut semaksimal mungkin.

##### (c) Peningkatan Risiko

Peningkatan risiko dilakukan dengan cara meningkatkan level kemungkinan dan/atau level dampak dari Risiko SPBE.

##### (d) Pembagian Risiko

Pembagian risiko dipilih jika Risiko SPBE tidak dapat ditangani secara langsung dan membutuhkan pihak lain untuk menangani Risiko SPBE tersebut. Pembagian risiko dilakukan dengan bekerja sama dengan dengan pihak lain.

##### (e) Penerimaan Risiko

Penerimaan risiko dipilih jika upaya penanganan lebih tinggi dibandingkan manfaat yang didapat atau kemungkinan terjadinya kecil. Opsi ini dilakukan dengan cara membiarkan Risiko SPBE terjadi apa adanya.

#### 2) Opsi Penanganan Risiko Negatif

##### (a) Eskalasi Risiko

Eskalasi risiko dipilih jika Risiko SPBE berada di luar atau melampaui wewenang. Opsi ini dilakukan dengan memindahkan tanggung jawab penanganan Risiko SPBE ke unit kerja yang lebih tinggi.

##### (b) Mitigasi Risiko

Mitigasi risiko dilakukan dengan cara mengurangi level kemungkinan dan/atau level dampak dari Risiko SPBE.

##### (c) Transfer Risiko

Transfer risiko dipilih jika terdapat kekurangan sumber daya untuk mengelola Risiko SPBE. Opsi ini dilakukan dengan cara mengalihkan kepemilikan risiko kepada pihak lain untuk melakukan pengelolaan dan pertanggungjawaban terhadap Risiko SPBE.

##### (d) Penghindaran Risiko

Penghindaran risiko dilakukan dengan mengubah perencanaan, penganggaran, program, dan kegiatan, atau aspek lainnya untuk mencapai sasaran SPBE.

- (e) **Penerimaan Risiko**  
Penerimaan risiko dipilih jika biaya dan usaha penanganan lebih tinggi dibandingkan manfaat yang didapat, kemungkinan terjadinya sangat kecil atau dampak sangat tidak signifikan. Opsi ini dilakukan dengan cara membiarkan risiko terjadi apa adanya.
- b) **Rencana Aksi Penanganan Risiko**  
Rencana aksi penanganan risiko merupakan rancangan kegiatan tindak lanjut untuk menangani Risiko SPBE.
- c) **Keluaran**  
Keluaran merupakan hasil dari rencana aksi penanganan Risiko SPBE.
- d) **Jadwal Implementasi**  
Jadwal implementasi merupakan jadwal pelaksanaan dari setiap rencana aksi penanganan Risiko SPBE.
- e) **Penanggung Jawab**  
Penanggung jawab berisikan nama unit yang bertanggung jawab dan unit pendukung dari setiap rencana aksi penanganan Risiko SPBE.

Tabel 16  
Contoh Pengisian Formulir 4.0 Rencana Penanganan Risiko SPBE Bagian Rencana Penanganan

Rencana Penanganan				
Opsi Penanganan Risiko SPBE	Rencana Aksi Penanganan Risiko SPBE	Keluaran	Jadwal Implementasi	Penanggung Jawab
Eksplorasi Risiko	Melakukan sosialisasi dan asistensi kepada K/L/D	Kegiatan sosialisasi dan asistensi	Triwulan I	Asisten Deputi SPBE
Mitigasi Risiko	Rekrutmen evaluator eksternal baru	Penambahan jumlah evaluator eksternal	Triwulan I	Asisten Deputi SPBE

### 3. Risiko Residual

Risiko residual merupakan Risiko SPBE yang tersisa dari Risiko SPBE yang telah ditangani. Dalam melakukan penanganan terhadap risiko residual, dilakukan pengulangan proses penilaian risiko sampai dengan risiko residual tersebut berada di bawah Selera Risiko SPBE. Penetapan risiko residual ini dapat ditetapkan berdasarkan expert judgement.

### E. Pemantauan dan Reviu

Pemantauan bertujuan untuk memonitor faktor-faktor atau penyebab yang mempengaruhi Risiko SPBE dan kondisi lingkungan Instansi Pusat dan Pemerintah Daerah. Selain itu, pemantauan dilakukan guna memonitor pelaksanaan rencana aksi penanganan Risiko SPBE. Hasil pelaksanaan pemantauan dapat menjadi dasar untuk melakukan penyesuaian kembali proses Manajemen Risiko SPBE. Pemantauan dilakukan berdasarkan setiap triwulan, semester, tahun, atau sewaktu-waktu (insidental) sesuai dengan kesepakatan dari masing-masing Instansi Pusat dan Pemerintah Daerah.

Reviu bertujuan untuk mengontrol kesesuaian dan ketepatan seluruh pelaksanaan proses Manajemen Risiko SPBE sesuai dengan ketentuan yang berlaku. Reviu dilakukan sesuai dengan kesepakatan dari masing-masing Instansi Pusat dan Pemerintah Daerah.

#### F. Pencatatan dan Pelaporan

Pencatatan merupakan kegiatan atau proses pendokumentasian suatu aktivitas dalam bentuk tulisan dan dituangkan dalam dokumen. Pelaporan merupakan kegiatan yang dilakukan untuk menyampaikan hal-hal yang berhubungan dengan hasil pekerjaan yang telah dilakukan selama satu periode tertentu.

Proses Manajemen Risiko SPBE dan keluaran yang dihasilkan perlu dicatat dan dilaporkan dengan mekanisme yang tepat. Pencatatan dan pelaporan bertujuan untuk mengkomunikasikan aktivitas Manajemen Risiko SPBE serta keluaran yang dihasilkan, menyediakan informasi untuk pengambilan keputusan, meningkatkan kualitas aktivitas Manajemen Risiko SPBE, serta mengawal interaksi dengan pemangku kepentingan termasuk tanggung jawab serta akuntabilitas terhadap Manajemen Risiko SPBE.

Pencatatan dan pelaporan Manajemen Risiko SPBE terdiri dari:

1. Pencatatan dan Pelaporan Periodik  
Pencatatan dan pelaporan periodik merupakan kegiatan yang dilakukan secara berulang pada waktu yang telah ditentukan.
2. Pencatatan dan Pelaporan Insidental  
Pencatatan dan pelaporan insidental merupakan kegiatan yang dilakukan pada waktu tertentu sesuai dengan kebutuhan.

#### G. Dokumen Manajemen Risiko SPBE

1. Pakta Integritas Manajemen Risiko SPBE  
Pakta Integritas Manajemen Risiko SPBE merupakan dokumen pernyataan atau janji untuk berkomitmen menjalankan Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah. Dokumen Pakta Integritas dapat dilihat pada Formulir 1.0 Pakta Integritas.
2. Dokumen Proses Risiko SPBE  
Dokumen Proses Risiko SPBE merupakan dokumen pendukung pelaksanaan proses penetapan konteks, penilaian, dan penanganan Risiko SPBE. Dokumen Proses Risiko SPBE terdiri dari:
  - a) Formulir Konteks Risiko SPBE
  - b) Formulir Konteks Risiko SPBE merupakan dokumen dari aktivitas penetapan konteks pada proses Manajemen Risiko SPBE. Formulir ini dapat dilihat pada Formulir 2.0.
  - c) Formulir Penilaian Risiko SPBE
  - d) Formulir Penilaian Risiko SPBE merupakan dokumen dari aktivitas penilaian Risiko SPBE pada proses Manajemen Risiko SPBE. Formulir ini dapat dilihat pada Formulir 3.0.
  - e) Formulir Rencana Penanganan Risiko SPBE
  - f) Formulir Rencana Penanganan Risiko SPBE merupakan dokumen dari aktivitas penanganan Risiko SPBE pada proses Manajemen Risiko SPBE. Formulir ini dapat dilihat pada Formulir 4.0.
3. Dokumen Proses Pengendalian Risiko SPBE  
Dokumen Proses Pengendalian Risiko SPBE merupakan dokumen pendukung pelaksanaan proses komunikasi dan konsultasi, serta pelaporan Risiko SPBE. Dokumen Proses Pengendalian Risiko SPBE terdiri dari:
  - a) Dokumen Kegiatan Komunikasi dan Konsultasi  
Dokumen Kegiatan Komunikasi dan Konsultasi merupakan dokumen dari aktivitas pelaksanaan kegiatan komunikasi dan konsultasi. Dokumen dapat berbentuk notulensi dan laporan atau dokumen lainnya yang dihasilkan dari pelaksanaan kegiatan komunikasi dan konsultasi.
  - b) Dokumen Laporan Pemantauan

Dokumen Laporan Pemantauan merupakan dokumen dari aktivitas pelaksanaan kegiatan pemantauan Risiko. Dalam pedoman ini menggunakan 2 format laporan yaitu laporan pemantauan triwulan dan laporan pemantauan tahunan.

- c) Laporan pemantauan triwulan menggambarkan kondisi pelaksanaan dalam waktu setiap tiga bulan terkait rencana aksi penanganan yang meliputi besaran/level Risiko SPBE saat ini dan proyeksi Risiko SPBE, penanganan yang telah dilakukan, rencana penanganan, penanggung jawab, dan waktu pelaksanaan.
- d) Laporan pemantauan tahunan merangkum laporan triwulan I sampai dengan triwulan IV dengan berfokus pada tendensi besaran Risiko SPBE dan memberikan rekomendasi penanganan Risiko SPBE yang dapat digunakan sebagai masukan pelaksanaan proses Manajemen Risiko SPBE pada tahun selanjutnya.

Format laporan pemantauan triwulan dan tahunan dapat dilihat pada Formulir 5.0.

Gambar 3. Contoh Pengisian Formulir 5.0 Laporan Pemantauan Risiko SPBE Triwulan I

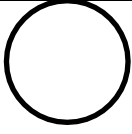
<b>Laporan Pemantauan Risiko SPBE Triwulan I</b>		
<div style="display: flex; align-items: center; margin-bottom: 10px;"> <div style="border: 1px solid black; border-radius: 50%; width: 30px; height: 30px; margin-right: 10px;"></div> <div> <p>Nama Unit : Deputi Bidang Kelembagaan dan Tata Laksana</p> <p>Sasaran : Meningkatkan kualitas penyelenggaraan Sistem Pemerintahan Berbasis Elektronik</p> <p>Risiko : Terdapat K/L/D yang tidak dievaluasi karena kurangnya jumlah evaluator eksternal sehingga terjadi penurunan</p> </div> </div>		
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; padding: 5px;"><b>Besaran/Level Risiko SPBE Saat ini dan Proyeksi Risiko SPBE</b></th> </tr> </thead> <tbody> <tr> <td style="padding: 10px;"> <p>Risiko SPBE pada awal tahun berada pada Level Risiko SPBE "sedang" dengan Besaran Risiko SPBE sebesar 14 dimana kemungkinan terjadinya Risiko SPBE tersebut sekitar 15% dalam satu periode (Kadang-Kadang Terjadi) dan berdampak pada penurunan kinerja hingga 50% (Cukup Signifikan).</p> <p style="text-align: center;">Risiko SPBE tersebut pada triwulan I telah berada pada Level Risiko SPBE "rendah" dengan Besaran Risiko SPBE sebesar 10 dimana kemungkinan terjadinya Risiko SPBE tersebut sekitar 15% dalam satu periode (Kadang- Kadang Terjadi) dan berdampak pada penurunan kinerja hingga 20% (Kurang Signifikan).</p> <p style="text-align: center;">Risiko SPBE tersebut kedepannya tidak dilakukan penanganan, karena sudah selesai.</p> </td> </tr> </tbody> </table>	<b>Besaran/Level Risiko SPBE Saat ini dan Proyeksi Risiko SPBE</b>	<p>Risiko SPBE pada awal tahun berada pada Level Risiko SPBE "sedang" dengan Besaran Risiko SPBE sebesar 14 dimana kemungkinan terjadinya Risiko SPBE tersebut sekitar 15% dalam satu periode (Kadang-Kadang Terjadi) dan berdampak pada penurunan kinerja hingga 50% (Cukup Signifikan).</p> <p style="text-align: center;">Risiko SPBE tersebut pada triwulan I telah berada pada Level Risiko SPBE "rendah" dengan Besaran Risiko SPBE sebesar 10 dimana kemungkinan terjadinya Risiko SPBE tersebut sekitar 15% dalam satu periode (Kadang- Kadang Terjadi) dan berdampak pada penurunan kinerja hingga 20% (Kurang Signifikan).</p> <p style="text-align: center;">Risiko SPBE tersebut kedepannya tidak dilakukan penanganan, karena sudah selesai.</p>
<b>Besaran/Level Risiko SPBE Saat ini dan Proyeksi Risiko SPBE</b>		
<p>Risiko SPBE pada awal tahun berada pada Level Risiko SPBE "sedang" dengan Besaran Risiko SPBE sebesar 14 dimana kemungkinan terjadinya Risiko SPBE tersebut sekitar 15% dalam satu periode (Kadang-Kadang Terjadi) dan berdampak pada penurunan kinerja hingga 50% (Cukup Signifikan).</p> <p style="text-align: center;">Risiko SPBE tersebut pada triwulan I telah berada pada Level Risiko SPBE "rendah" dengan Besaran Risiko SPBE sebesar 10 dimana kemungkinan terjadinya Risiko SPBE tersebut sekitar 15% dalam satu periode (Kadang- Kadang Terjadi) dan berdampak pada penurunan kinerja hingga 20% (Kurang Signifikan).</p> <p style="text-align: center;">Risiko SPBE tersebut kedepannya tidak dilakukan penanganan, karena sudah selesai.</p>		
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; padding: 5px;"><b>Penanganan yang telah dilakukan</b></th> </tr> </thead> <tbody> <tr> <td style="text-align: center; padding: 5px;">Rekrutmen evaluator eksternal.</td> </tr> </tbody> </table>	<b>Penanganan yang telah dilakukan</b>	Rekrutmen evaluator eksternal.
<b>Penanganan yang telah dilakukan</b>		
Rekrutmen evaluator eksternal.		

Rencana Penanganan	Penanggung jawab	Waktu Pelaksanaan
Melakukan	Asisten Deputi SPBE	Triwulan I



pemantauan terhadap kegiatan evaluasi SPBE.		
---	--	--

Gambar 4. Contoh Pengisian Formulir 5.0 Laporan Pemantauan Risiko SPBE Tahunan

<b>Laporan Pemantauan Risiko SPBE Tahunan</b>	
	<p>Nama Unit : Deputi Bidang Kelembagaan dan Tata Laksana  Sasaran : Meningkatnya kualitas penyelenggaraan Sistem Pemerintahan Berbasis Elektronik  Risiko : Terdapat K/L/D yang tidak dievaluasi karena kurangnya jumlah evaluator eksternal sehingga terjadi penurunan kinerja</p>
<b>Besaran/Level Risiko SPBE Saat ini</b>	
<p>Risiko SPBE pada awal tahun berada pada Level Risiko SPBE "sedang" dengan Besaran Risiko SPBE sebesar 14.  Risiko SPBE tersebut pada triwulan I, II, III, dan IV telah berada pada Level Risiko SPBE "rendah" dengan Besaran Risiko SPBE sebesar 10.</p>	
<b>Penanganan yang telah dilakukan</b>	
<ol style="list-style-type: none"> <li>1. Rekrutmen evaluator eksternal termasuk pelatihan bagi evaluator eksternal.</li> <li>2. Pemantauan terhadap kegiatan evaluasi SPBE.</li> </ol>	
Rekomendasi	<p>Untuk mengantisipasi terjadinya Risiko SPBE yang serupa, perlu dipastikan jumlah evaluator eksternal yang dibutuhkan untuk pelaksanaan evaluasi SPBE sesuai dengan analisis beban kerja.</p>

Rencana Penanganan	Penanggung jawab	Waktu Pelaksanaan
Melakukan pemantauan terhadap kegiatan evaluasi SPBE.	Asisten Deputi SPBE	Triwulan IV

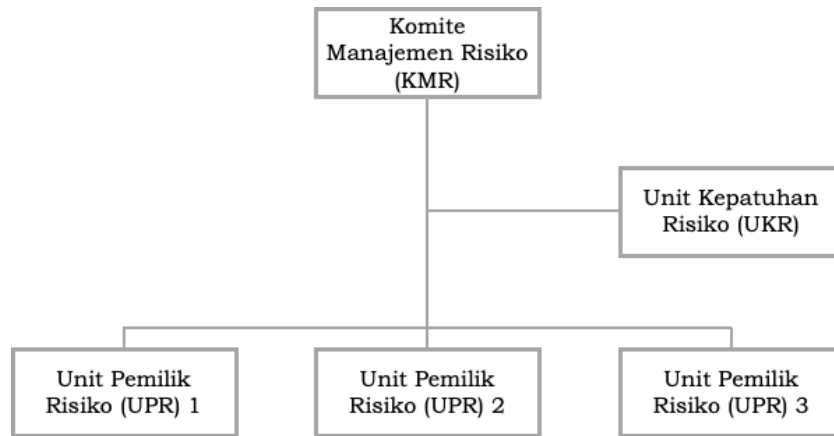
Manajemen Risiko SPBE merupakan tanggung jawab bersama pada semua tingkatan di lingkungan Instansi Pusat dan Pemerintah Daerah. Agar proses dan pengukuran dalam Manajemen Risiko SPBE dapat dilaksanakan dengan baik, maka diperlukan tata kelola Manajemen Risiko SPBE yang mengatur tugas dan tanggung jawab dari struktur Manajemen Risiko SPBE, dan budaya sadar Risiko SPBE yang dapat menggerakkan pegawai ASN menerapkan Manajemen Risiko SPBE.

#### H. Struktur Manajemen Risiko SPBE

Struktur Manajemen Risiko SPBE terdiri atas:

1. Komite Manajemen Risiko (KMR) SPBE yang memiliki fungsi penetapan kebijakan strategis terkait Manajemen Risiko SPBE.
2. Unit Pemilik Risiko (UPR) SPBE yang memiliki fungsi pelaksanaan Manajemen Risiko SPBE.
3. Unit Kepatuhan Risiko (UKR) SPBE yang memiliki fungsi pengawasan terhadap pelaksanaan Manajemen Risiko SPBE.

Gambar 5 mengilustrasikan struktur Manajemen Risiko SPBE seperti di bawah ini



Gambar 5. Struktur Manajemen Risiko SPBE

Struktur Manajemen Risiko SPBE merupakan struktur *ex-officio* yang menjalankan tugas tambahan terkait Manajemen Risiko SPBE. Apabila Instansi Pusat dan Pemerintah Daerah telah memiliki kebijakan manajemen risiko bagi organisasi, struktur Manajemen Risiko SPBE hendaknya mengadopsi struktur manajemen risiko yang telah ada tersebut untuk keterpaduan pelaksanaan manajemen risiko secara menyeluruh.

Di dalam penerapan Manajemen Risiko SPBE, struktur Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah dapat memiliki struktur yang berbeda satu sama lain. Perbedaan struktur Manajemen Risiko SPBE dapat dipengaruhi oleh ukuran organisasi, kompleksitas tugas, dan/atau tingkat risiko di Instansi Pusat dan Pemerintah Daerah. Instansi Pusat dan Pemerintah Daerah yang memiliki ukuran organisasi yang besar, kompleksitas tugas yang tinggi, dan/atau tingkat risiko yang tinggi memerlukan pengendalian Risiko SPBE yang lebih ketat melalui struktur Manajemen Risiko SPBE yang lebih berjenjang.

##### 1. Komite Manajemen Risiko (KMR) SPBE

Komite Manajemen Risiko SPBE yang disingkat KMR SPBE dibentuk dan ditetapkan oleh masing-masing pimpinan Instansi Pusat dan kepala daerah, dan memiliki anggota yang terdiri atas pejabat Instansi Pusat dan Pemerintah Daerah yang memiliki kewenangan pengambilan keputusan dan penetapan kebijakan strategis terkait Manajemen Risiko SPBE. KMR SPBE memiliki tugas menyelenggarakan perumusan dan penetapan kebijakan, pengendalian, pemantauan, dan evaluasi penerapan kebijakan Manajemen Risiko SPBE. Dalam melaksanakan tugasnya, KMR SPBE menyelenggarakan fungsi sebagai berikut:

- a) penyusunan dan penetapan kebijakan Manajemen Risiko SPBE;
- b) penyusunan dan penetapan kerangka kerja dan pedoman pelaksanaan Manajemen Risiko SPBE;
- c) penyusunan dan penetapan pakta integritas Manajemen Risiko SPBE;
- d) penyusunan dan penetapan konteks Risiko SPBE;

- e) pengendalian proses Risiko SPBE melalui komunikasi dan konsultasi, pencatatan dan pelaporan, serta pemantauan dan evaluasi terhadap penerapan Manajemen Risiko SPBE; dan
- f) pelaksanaan komitmen pimpinan dan penerapan budaya sadar Risiko SPBE.

2. Unit Pemilik Risiko (UPR) SPBE

Unit Pemilik Risiko SPBE yang disingkat UPR SPBE merupakan unit kerja di Instansi Pusat dan Pemerintah Daerah yang bertanggung jawab langsung kepada pimpinan Instansi Pusat dan kepala daerah. UPR SPBE memiliki tugas melaksanakan penerapan Manajemen Risiko SPBE pada unit kerja tertinggi sampai terendah. UPR SPBE terdiri atas unsur:

- a) Pemilik Risiko SPBE merupakan pejabat yang bertanggung jawab atas pelaksanaan penerapan Manajemen Risiko SPBE di unit organisasi tersebut;
- b) Koordinator Risiko SPBE merupakan pejabat/pegawai yang ditunjuk oleh Pemilik Risiko SPBE untuk bertanggung jawab atas pelaksanaan koordinasi penerapan Manajemen Risiko SPBE kepada semua pemangku kepentingan baik internal maupun eksternal UPR SPBE; dan
- c) Pengelola Risiko SPBE merupakan pejabat/pegawai yang ditunjuk oleh Pemilik Risiko SPBE untuk bertanggung jawab atas pelaksanaan operasional Manajemen Risiko SPBE pada unit-unit kerja yang berada di bawah UPR SPBE.

Dalam melaksanakan tugasnya, UPR SPBE menjalankan fungsi sebagai berikut:

- a) penyusunan dan penetapan penilaian Risiko SPBE dan rencana pelaksanaan Manajemen Risiko SPBE termasuk rencana kontinjensi penanganan Risiko SPBE;
- b) pelaksanaan koordinasi penerapan Manajemen Risiko SPBE kepada semua pemangku kepentingan;
- c) pelaksanaan operasional Manajemen Risiko SPBE yang efektif melalui komunikasi dan konsultasi, pencatatan dan pelaporan, serta pemantauan dan evaluasi; dan
- d) pelaksanaan pembinaan budaya sadar Risiko SPBE melalui sosialisasi, bimbingan, pelatihan, dan supervisi penerapan Manajemen Risiko SPBE;

3. Unit Kepatuhan Risiko (UKR) SPBE

Unit Kepatuhan Risiko SPBE yang disingkat UKR SPBE merupakan unit organisasi di Instansi Pusat dan Pemerintah Daerah yang melaksanakan fungsi pengawasan intern di Instansi Pusat dan Pemerintah Daerah (Aparat Pengawasan Intern Pemerintah-APIP). UKR SPBE memiliki tugas melaksanakan pengawasan terhadap penerapan kebijakan Manajemen Risiko SPBE di semua UPR SPBE. Dalam melaksanakan tugasnya, UKR SPBE menjalankan fungsi sebagai berikut:

- a) penyusunan kebijakan pengawasan terhadap penerapan Manajemen Risiko SPBE;
- b) pelaksanaan pengawasan intern terhadap penerapan Manajemen Risiko SPBE di semua UPR SPBE melalui audit, reviu, pemantauan, evaluasi, dan kegiatan pengawasan lainnya;
- c) pelaksanaan konsultasi dan asistensi kepada UPR SPBE dalam penerapan Manajemen Risiko SPBE;
- d) penyusunan dan penyampaian rekomendasi terhadap efektivitas penerapan Manajemen Risiko SPBE kepada KMR SPBE dan UPR SPBE; dan
- e) pelaksanaan konsultasi dan asistensi kepada UPR dalam pembinaan budaya sadar Risiko SPBE.

## I. Budaya Sadar Risiko SPBE

Budaya sadar Risiko SPBE merupakan perilaku ASN yang mengenal, memahami, dan mengakui kemungkinan terjadinya Risiko SPBE, baik positif maupun negatif, yang ditindaklanjuti dengan upaya yang berfokus pada penerapan Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah. ASN harus peka terhadap faktor-faktor dan peristiwa yang mungkin berpengaruh terhadap tujuan dan sasaran penerapan SPBE di Instansi Pusat dan Pemerintah Daerah. Dengan menyadari adanya Risiko SPBE, ASN dapat merencanakan dan mempersiapkan tindakan atau penanganan Risiko SPBE secepatnya. Keterlibatan ASN di dalam budaya sadar Risiko SPBE akan memberikan nilai tambah dan meningkatkan efektivitas penerapan Manajemen Risiko SPBE yang pada akhirnya berdampak pada peningkatan kualitas penerapan SPBE di Instansi Pusat dan Pemerintah Daerah.

### 1. Faktor Keberhasilan

Faktor-faktor yang dapat mendukung keberhasilan dalam menciptakan budaya sadar Risiko SPBE antara lain:

#### a) Kepemimpinan

KMR SPBE harus dapat menunjukkan sikap kepemimpinan, yaitu konsisten dalam perkataan dan tindakan, mampu mendorong atau menggerakkan ASN dalam penerapan budaya sadar Risiko SPBE, mampu menempatkan Manajemen Risiko SPBE sebagai agenda penting di dalam setiap pengambilan keputusan yang terkait dengan penerapan SPBE, dan memiliki komitmen yang kuat menerapkan Manajemen Risiko SPBE melalui penyediaan sumber daya yang cukup, baik anggaran, SDM, kebijakan, pedoman, maupun strategi penerapannya di Instansi Pusat dan Pemerintah Daerah.

#### b) Keterlibatan Semua Pihak

Budaya sadar Risiko SPBE melibatkan semua ASN yang terkait secara langsung maupun tidak langsung dengan penerapan SPBE, baik ASN yang berada pada KMR SPBE, UPR SPBE, maupun UKR SPBE, karena mereka yang paling memahami terjadinya Risiko SPBE dan cara penanganannya dalam level strategis maupun operasional.

#### c) Komunikasi

Komunikasi tentang pentingnya Manajemen Risiko SPBE harus dapat disampaikan kepada setiap ASN yang terlibat dalam penerapan SPBE melalui penyediaan saluran komunikasi yang variatif dan efektif. Tidak hanya KMR SPBE menyampaikan informasi terkait kebijakan Manajemen Risiko kepada ASN, tetapi juga ASN dapat menyampaikan informasi Risiko SPBE kepada pimpinan di setiap jenjang termasuk kepada KMR SPBE. Saluran komunikasi ini dapat diwujudkan melalui rapat-rapat pengambilan keputusan, berbagai pertemuan dalam proses Manajemen Risiko SPBE, dan penyampaian informasi melalui saluran komunikasi elektronik seperti surat elektronik, sistem naskah dinas elektronik, sistem aplikasi manajemen risiko, video conference, dan lain sebagainya.

#### d) Daya Responsif

Dalam budaya sadar Risiko SPBE, Risiko SPBE dieskalasi kepada pihak yang bertanggung jawab agar dapat ditangani dengan cepat. Sikap responsif ini sangat penting untuk mencegah ancaman yang dapat menghambat tercapainya tujuan penerapan SPBE ataupun meraih peluang untuk mempercepat tercapainya tujuan penerapan SPBE termasuk peningkatan kualitasnya. ASN yang responsif akan lebih siap beradaptasi terhadap perubahan

dan penyelesaian masalah yang rumit dalam penerapan SPBE.

e) Sistem Penghargaan

KMR SPBE hendaknya memahami secara langsung permasalahan yang dialami oleh ASN pada pelaksanaan tugas UPR SPBE dan UKR SPBE, serta menjadikan pencapaian kinerja Risiko SPBE sebagai salah satu indikator dalam pemberian penghargaan dan sanksi.

f) Integrasi Proses

Proses Manajemen Risiko SPBE hendaknya diintegrasikan dengan proses manajemen di Instansi Pusat dan Pemerintah Daerah sehingga tidak dipandang sebagai tambahan beban pekerjaan. Integrasi proses dapat dilakukan dengan menyelaraskan proses Manajemen Risiko SPBE sebagai satu kesatuan dari setiap proses kegiatan, proses manajemen risiko, dan proses manajemen kinerja Instansi Pusat dan Pemerintah Daerah.

g) Program Kegiatan Berkelanjutan

Agar budaya sadar Risiko SPBE dapat diterima oleh ASN, KMR SPBE hendaknya menyusun program kegiatan budaya sadar Risiko SPBE secara sistematis dan terencana, seperti kegiatan edukasi, berbagi pengetahuan, dan kunjungan kerja/supervisi ke UPR SPBE.

2. Langkah-Langkah Pengembangan

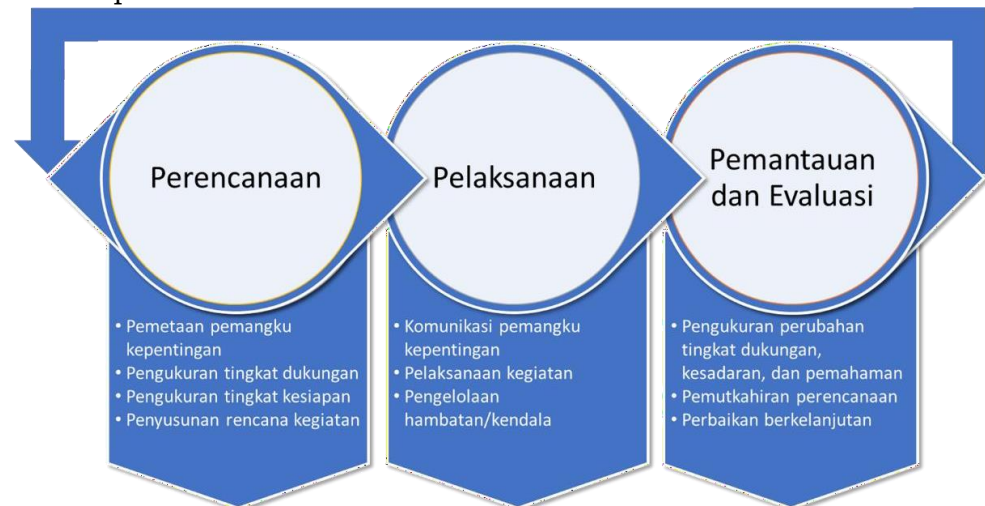
Pengembangan budaya sadar Risiko SPBE dapat dilakukan melalui langkah-langkah berikut ini:

a) Menyusun perencanaan kegiatan budaya sadar Risiko SPBE;

b) Melaksanakan kegiatan budaya sadar Risiko SPBE; dan

c) Melakukan pemantauan dan evaluasi pelaksanaan kegiatan budaya sadar Risiko SPBE.

Langkah-langkah pengembangan budaya sadar Risiko SPBE dapat dilihat pada Gambar 6 di bawah ini.



Gambar 6. Langkah Pengembangan Budaya Sadar Risiko SPBE

Perencanaan kegiatan budaya sadar Risiko SPBE difokuskan pada:

a) Pemetaan pemangku kepentingan terhadap pelaksanaan Manajemen Risiko SPBE.

Tujuan dari pemetaan pemangku kepentingan adalah untuk melakukan penilaian terhadap pemangku kepentingan terkait peran dan kapasitas mereka dalam mempengaruhi keberhasilan penerapan budaya sadar Risiko SPBE, serta untuk menyusun prioritas kegiatan budaya sadar Risiko SPBE berdasarkan tingkat kekuatan, posisi penting, ataupun pengaruh dari pemangku kepentingan. Dalam hal ini, pemangku kepentingan dapat diidentifikasi dengan merujuk pada struktur Manajemen Risiko SPBE yang mencakup KMR SPBE, UPR SPBE, dan UKR SPBE..

- b) Pengukuran tingkat dukungan pemangku kepentingan terhadap budaya sadar Risiko SPBE.

Hal ini menjadi penting untuk mengelola kegiatan budaya sadar Risiko SPBE secara efektif. Dukungan pemangku kepentingan dapat digolongkan ke dalam tiga kategori, yaitu: sangat mendukung secara konsisten, mendukung secara tidak konsisten, dan tidak mendukung atau resistan terhadap budaya sadar Risiko SPBE.

- c) Pengukuran tingkat kesiapan budaya sadar Risiko SPBE. Pengukuran ini biasanya menggunakan kuesioner yang disampaikan kepada pemangku kepentingan, baik secara sampel maupun semua populasi. Pengukuran dapat difokuskan antara lain pada komitmen, manfaat/dampak, pemahaman/kesadaran, tata cara/prosedur pelaksanaan, dan partisipasi dari pemangku kepentingan terhadap penerapan Manajemen Risiko SPBE.
- d) Penyusunan rencana kegiatan budaya sadar Risiko SPBE.

Rencana kegiatan yang tepat disusun dengan mempertimbangkan sumber daya yang tersedia di Instansi Pusat dan Pemerintah Daerah seperti anggaran, waktu, sarana dan prasarana, SDM pelaksana, peserta, dan metode pelaksanaan. Metode pelaksanaan kegiatan budaya sadar Risiko SPBE mencakup antara lain pelatihan, seminar, sosialisasi, kelompok diskusi, berbagi pengetahuan dan pengalaman, konsultasi, pembimbingan/pendampingan, dan supervisi.

Pelaksanaan kegiatan budaya sadar Risiko SPBE difokuskan pada implementasi rencana kegiatan budaya sadar Risiko SPBE, yaitu:

- a) Melakukan komunikasi kepada pemangku kepentingan.

Sebelum melaksanakan rencana kegiatan budaya sadar Risiko SPBE, rencana tersebut perlu dikomunikasikan kepada pemangku kepentingan dengan memberikan alasan-alasan yang rasional agar mendapatkan dukungan pelaksanaan oleh pemangku kepentingan.

- b) Mengelola hambatan/kendala.

Dalam pelaksanaan kegiatan budaya sadar Risiko SPBE, kendala-kendala yang terjadi agar dikelola dengan baik agar tujuan dari kegiatan tersebut dapat dicapai.

Pemantauan dan evaluasi kegiatan budaya sadar Risiko SPBE ditujukan untuk meningkatkan budaya sadar Risiko SPBE melalui perbaikan berkelanjutan. Pelaksanaan pemantauan dan evaluasi difokuskan pada:

- a) Pengukuran perubahan tingkat dukungan, kesadaran, dan pemahaman dari pemangku kepentingan terhadap penerapan Manajemen Risiko SPBE.

Pengukuran terkait hal ini dapat dilakukan melalui pengumpulan dan analisis umpan balik dari pemangku kepentingan dengan cara supervisi ke unit-unit para pemangku kepentingan. Hasil analisis selanjutnya digunakan untuk memutakhirkan tingkat dukungan, kesadaran, dan pemahaman dari pemangku kepentingan, serta memberikan saran-saran perbaikan terhadap kegiatan budaya sadar Risiko SPBE.

- b) Pemutakhiran rencana kegiatan budaya sadar Risiko SPBE.

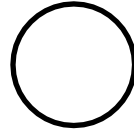
Rencana kegiatan budaya sadar Risiko SPBE dilakukan pemutakhiran berdasarkan saran-saran perbaikan dengan tetap mempertimbangkan ketersediaan sumber daya yang dimiliki oleh Instansi Pusat dan Pemerintah Daerah.

- c) Pelaksanaan perbaikan berkelanjutan.

Rencana kegiatan budaya sadar Risiko SPBE yang telah dimutakhirkan dilaksanakan melalui langkah ke dua di atas

sehingga mencapai peningkatan budaya sadar Risiko SPBE.

Formulir 1.0. Pakta Integritas Manajemen Resiko SPBE



**<Logo Instansi Pusat / Pemerintah Daerah>**

PAKTA INTEGRITAS MANAJEMEN RISIKO SPBE

<NOMOR PIAGAM>

<NAMA UPR>

<NAMA INSTANSI PUSAT / PEMERINTAH DAERAH>

<TAHUN PENERAPAN MANAJEMEN RISIKO SPBE>

Dalam rangka pencapaian sasaran SPBE pada <Nama UPR SPBE>, saya menyatakan bahwa:

1. Penetapan konteks, identifikasi, analisis, evaluasi, dan rencana penanganan Risiko SPBE telah sesuai dengan ketentuan Manajemen Risiko SPBE yang berlaku di <Nama Instansi Pusat atau Pemerintah Daerah>;
2. Rencana penanganan Risiko SPBE yang merupakan bagian yang tidak terpisahkan dari pakta integritas ini akan dilaksanakan oleh seluruh jajaran dalam unit yang saya pimpin;
3. Pemantauan dan reviu akan dilaksanakan secara berkala untuk meningkatkan efektivitas Manajemen Risiko SPBE.

<Tempat dan  
Tanggal  
Penetapan>

<Jabatan  
Pimpinan  
UPR>

<TTD>

<Nama Pimpinan  
UPR>

**BAB II**  
**PEDOMAN MANAJEMEN KEAMANAN INFORMASI**  
**SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK**

**I. PENDAHULUAN**

Kebijakan umum keamanan informasi memuat kebijakan keamanan informasi yang akan menjadi acuan dalam kebijakan spesifik, pedoman, prosedur, risk assessment maupun proses keamanan informasi lainnya. Kebijakan spesifik akan digunakan oleh bagian teknis dalam menyelesaikan tanggung jawab keamanan informasi. Pedoman dan prosedur digunakan untuk mengimplementasikan kebijakan yang telah ditetapkan dan sifatnya anjuran. Hal tersebut berbeda dengan kebijakan yang sifatnya keharusan.

Kebijakan umum keamanan informasi memiliki kesamaan tingkat dengan kebijakan di Pemerintah Kabupaten Jombang yang lainnya dan dipatuhi oleh semua pengguna. Berbeda dengan kebijakan spesifik yang hanya berlaku untuk Perangkat Daerah tertentu sesuai dengan bidangnya. Begitupula dengan pedoman dan prosedur, pedoman dan prosedur dilaksanakan oleh Perangkat Daerah tertentu.

**II. DEFINISI**

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. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.
3. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
4. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
5. Instansi Pusat adalah kementerian, lembaga pemerintah nonkementerian, kesekretariatan lembaga negara, kesekretariatan lembaga nonstruktural, dan Lembaga pemerintah lainnya.
6. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
7. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
8. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang melakukan tugas atau fungsi Layanan SPBE.
9. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.
10. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran Layanan SPBE.
11. 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.
12. Application Programming Interface yang selanjutnya disingkat API adalah sekumpulan perintah, fungsi, serta protokol yang mengintegrasikan dua bagian dari aplikasi atau dengan aplikasi yang berbeda secara bersamaan.
13. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.



14. Pusat Data Nasional adalah sekumpulan Pusat Data yang digunakan secara bergantian oleh Instansi Pusat dan Pemerintah Daerah, dan saling terhubung.

### III. KEBIJAKAN PENYELENGGARAAN

#### A. Ruang lingkup keamanan informasi

Ruang lingkup keamanan informasi meliputi:

1. Keamanan informasi seperti keamanan database, dokumentasi sistem, manual pengguna, prosedur pendukung;
2. Keamanan aset perangkat lunak seperti keamanan perangkat lunak aplikasi, perangkat lunak sistem, perkakas pengembangan, dan utilitas;
3. Keamanan aset fisik meliputi keamanan perangkat komputer, perangkat jaringan;
4. Keamanan layanan meliputi keamanan layanan komputasi dan komunikasi;
5. Keamanan sumber daya manusia beserta kualifikasi, keterampilan dan pengalaman;

#### B. Keamanan informasi

Keamanan informasi merupakan tanggung jawab dari semua pihak yang terkait pada Pemerintah Kabupaten Jombang meliputi:

1. Bupati Jombang;
2. Wakil Bupati Jombang;
3. Sekretaris Daerah;
4. Asisten Pemerintah dan Kesra;
5. Asisten Perekonomian;
6. Asisten Umum;
7. Staf Ahli Bupati;
8. Inspektorat;
9. Sekretariat DPRD;
10. Sekretariat Daerah;
11. Dinas Daerah (Dinas, Badan, Satpol Pamong Praja dan Pemadam Kebakaran);
12. Kecamatan/ Kelurahan Kabupaten Jombang;
13. Badan dan Lembaga Daerah lainnya;
14. Serta pihak luar yang berhubungan dengan Pemerintah Kabupaten Jombang.

Pengecualian terhadap kepatuhan tersebut disetujui oleh pemilik aset informasi terkait dan Bupati Jombang.

#### C. Urgensi Keamanan informasi

Keamanan informasi menjadi hal yang penting bagi Pemerintah Kabupaten Jombang karena beberapa hal berikut:

1. Memberikan information assurance bagi stakeholder utama Pemerintah Kabupaten Jombang.
2. Meningkatkan assurance atas aset informasi terhadap risiko keamanan melalui proteksi yang cukup dan berkelanjutan. Risiko tersebut memiliki dampak langsung maupun tidak langsung bagi negara.
3. Meningkatkan kepatuhan terhadap undang-undang dan peraturan terkait keamanan informasi yang ada di Indonesia maupun internasional.
4. Meningkatkan kepercayaan publik, stakeholder terhadap Pemerintah Kabupaten Jombang.
5. Meningkatkan respon terhadap pelanggaran atau insiden keamanan informasi.

#### D. Tujuan keamanan informasi

Tujuan keamanan informasi Pemerintah Kabupaten Jombang sebagai berikut:

1. Memastikan kerahasiaan terhadap aset informasi Pemerintah Kabupaten Jombang;
2. Memastikan ketersediaan dan integritas informasi bagi stakeholder,
3. Memastikan kepatuhan terhadap hukum, undang-undang dan peraturan yang berlaku;
4. Memastikan kapabilitas organisasi untuk melanjutkan operasi atau layanannya ketika terjadi insiden keamanan.

#### E. Prinsip keamanan informasi

Prinsip keamanan informasi Pemerintah Kabupaten Jombang sebagai berikut:

1. Prinsip Kerahasiaan;  
Kemampuan akses atau modifikasi informasi diberikan hanya kepada pihak yang berwenang untuk tujuan yang jelas.
2. Prinsip Ketersediaan;  
Informasi dan aset TI yang dimiliki oleh Pemerintah Kabupaten Jombang tersedia untuk mendukung organisasi dalam rentang waktu yang disepakati bersama sesuai tujuan organisasi.
3. Prinsip Integritas;  
Informasi yang digunakan pengguna bisa dipercaya kebenarannya merefleksikan realitas sebenarnya, terutama informasi strategis.
4. Prinsip Akuntabilitas;  
Tanggung jawab dan akuntabilitas pemilik, penyedia dan pengguna sistem informasi dan pihak lain yang terkait dengan keamanan informasi harus dideskripsikan dengan jelas.
5. Prinsip Kesadaran;  
Pemilik, penyedia, pengguna sistem informasi dan pihak lain yang terkait memiliki pemahaman dan informasi yang cukup mengenai kebijakan, pedoman, prosedur, ukuran, praktek keamanan informasi.
6. Prinsip Integrasi;  
Kebijakan, pedoman, prosedur, ukuran dan praktek untuk keamanan informasi harus dikoordinasikan dan diintegrasikan antara satu dengan yang lainnya.
7. Prinsip Perbaikan Berkelanjutan;  
Keamanan informasi harus diperbaiki terus menerus mengikuti perkembangan risiko dan kebutuhan organisasi.

#### F. Pemantauan, Pengukuran, Analisis dan Evaluasi Keamanan Informasi

Sekretaris Daerah harus mengevaluasi kinerja keamanan informasi dan efektivitas Keamanan Informasi. serta harus menentukan beberapa hal antara lain:

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.

Sekretaris Daerah harus menyimpan informasi terdokumentasi yang memadai sebagai bukti hasil pemantauan dan pengukuran.

### G. Audit Internal

Inspektorat harus melakukan audit internal pada selang waktu terencana untuk memberikan informasi apakah Keamanan Informasi diimplementasikan dan dipelihara secara efektif serta sesuai dengan:

1. Persyaratan yang ditetapkan Bupati Jombang untuk Keamanan Informasinya;
2. Persyaratan Standar ISO 27001:2013; dan
3. Indeks KAMI.

Inspektorat juga diwajibkan untuk:

1. Merencanakan, menetapkan, menerapkan 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;
2. Menentukan kriteria audit dan ruang lingkup untuk setiap audit;
3. Memilih auditor dan melakukan audit yang menjamin objektivitas dan tidakberpihakan proses audit;
4. Memastikan bahwa hasil audit tersebut dilaporkan kepada manajemen yang relevan; dan
5. Menyimpan informasi terdokumentasi sebagai alat bukti dari program audit dan hasil audit.

### H. Peninjauan Manajemen

Bupati Jombang harus mereviu kebijakan SMKI minimal setiap 1 (satu) tahun sekali untuk memastikan kesesuaian, kecukupan dan efektivitas, Peninjauan manajemen harus mencakup beberapa pertimbangan antara lain:

1. Status tindakan dari reviu manajemen sebelumnya;
2. Perubahan isu eksternal dan internal yang relevan dengan Keamanan Informasi;
3. Umpan balik dari kinerja keamanan informasi, termasuk kecenderungan dalam hal:
  - a) Ketidaksesuaian dan tindakan korektif;
  - b) Hasil pemantauan dan pengukuran;
  - c) Hasil audit;
  - d) Pemenuhan terhadap sasaran keamanan informasi;
  - e) Umpan balik dari pihak yang berkepentingan;
  - f) Hasil penilaian risiko dan status rencana penanganan risiko; dan
  - g) Peluang untuk perbaikan berkelanjutan.

Keluaran dari peninjauan manajemen harus mencakup keputusan yang berkaitan dengan peluang perbaikan berkelanjutan dan setiap kebutuhan untuk perubahan SMKI. Sekretaris Daerah harus menyimpan informasi terdokumentasi sebagai bukti hasil peninjauan manajemen.

### I. Perbaikan Ketidaksesuaian dan Tindakan Korektif

Perbaikan Ketidaksesuaian dan Tindakan Korektif dilaksanakan oleh Sekretaris Daerah dengan cara sebagai berikut:

1. Bereaksi terhadap ketidaksesuaian, dan jika dapat diterapkan untuk mengambil tindakan untuk mengendalikan dan mengoreksinya dan menangani konsekuensinya;
2. Mengevaluasi kebutuhan tindakan untuk menghilangkan penyebab ketidaksesuaian, agar hal itu tidak terulang atau terjadi di tempat lain, dengan cara:
  - a) Meninjau ketidaksesuaian;
  - b) Menentukan penyebab ketidaksesuaian; dan
  - c) Menentukan apakah ada ketidaksesuaian serupa, atau berpotensi terjadi kembali;
3. Melaksanakan tindakan apapun yang diperlukan;

4. Mereviu efektivitas tindakan korektif apapun yang diambil; dan
5. Membuat perubahan pada keamanan informasi,

Jika diperlukan tindakan korektif harus sesuai dengan efek dari ketidaksesuaian yang ditemui. Sekretaris Daerah harus menyimpan informasi terdokumentasi sebagai bukti dari Sifat ketidaksesuaian dan tindakan berikutnya yang diambil, dan Hasil dari setiap tindakan korektif.

#### J. Dokumen Kebijakan Keamanan Informasi

Dokumen Kebijakan Keamanan Informasi harus mendapatkan persetujuan dari Bupati Jombang. Dokumen tersebut harus dipublikasikan dan dikomunikasikan ke seluruh pegawai dan pihak eksternal terkait. Dokumen kebijakan keamanan informasi tersebut termasuk prinsip, kebijakan, prosedur dan standar teknis keamanan.

#### K. Review Kebijakan Keamanan Informasi

Kebijakan keamanan informasi harus direview secara kontinu dan sistematis. Review tersebut akan digunakan untuk perbaikan kebijakan keamanan informasi. Review tersebut dilakukan oleh (Chief Information Security Officer / CISO) dan disampaikan ke Komite Keamanan Informasi (KKI) untuk mendapatkan persetujuan revisi bila diperlukan. Proses review tersebut harus mendapatkan dukungan dari Kepala Pemerintah Kabupaten Jombang.

#### L. Tanggung Jawab Keamanan Informasi

Tanggung Jawab Keamanan Informasi memuat organisasi beserta tanggung jawab masing-masing bagian dalam organisasi tersebut. Bagian ini terbagi menjadi pengorganisasian keamanan informasi (Chief Information Security Officer / CISO), tanggung jawab penanggung jawab utama keamanan informasi, tanggung jawab komite keamanan informasi, tanggung jawab Kepala Perangkat Daerah atau pejabat eselon II, tanggung jawab pelaksana keamanan informasi, dan proses reviu independen.

##### 1. Pengorganisasian Keamanan Informasi

Organisasi keamanan informasi Pemerintah Kabupaten Jombang terdiri dari:

- a) Penanggung Jawab Eksekutif (Code Chief Information Officer/ GCIO);  
Dipimpin oleh Sekretaris Daerah untuk menentukan prinsip, aksioma dan kebijakan keamanan informasi, menjamin ketersediaan, keakuratan, ketepatan, dan keamanan informasi yang dibutuhkan oleh organisasi untuk mencapai tujuan organisasi, serta mendapatkan laporan dari GCISO, Komite Risiko, dan Komite Audit untuk memastikan prinsip, aksioma, kebijakan dan pelaksanaan keamanan informasi diterapkan.
- b) Penanggung Jawab Utama Keamanan Informasi (Government Chief Information Security Officer/ GCISO);  
Dijabat oleh Kepala Dinas Komunikasi dan Informatika yang bertanggung jawab atas aspek keamanan informasi di lingkungan Pemerintah Kabupaten Jombang;
- c) Komite Keamanan Informasi (KKI);  
Komite yang dipimpin oleh GCISO dan anggotanya meliputi semua Kepala Perangkat Daerah. KKI merupakan Komite yang dibentuk untuk membahas dan memutuskan sejumlah aspek yang terkait dengan keamanan dalam pengembangan, implementasi, pengoperasian, monitoring, pemeliharaan dan peningkatan Tata Kelola Keamanan Informasi Pemerintah Kabupaten Jombang.
- d) Manajer Keamanan Informasi;  
Dijabat oleh Kepala Bidang Statistik dan Persandian yang bertanggung jawab atas aspek pengelolaan keamanan informasi,

- dan keamanan non fisik dalam organisasi.
- e) Manajer Keamanan Fisik;  
Dijabat oleh Kepala Sub Bagian Umum dan Kepegawaian, yang bertanggung jawab mengelola keamanan fasilitas fisik dalam organisasi
  - f) Bagian Operasi dan Administrasi Keamanan Informasi;  
Ditugaskan kepada Seksi Persandian yang bertanggung jawab untuk mengelola pelaksanaan keamanan informasi sesuai dengan arahan yang telah ditetapkan.
  - g) Pemilik Aset Informasi;  
Ditugaskan kepada seluruh Asisten, Kepala Badan, Kepala Dinas, Kepala Bagian, dan Kecamatan/ Kelurahan yang bertanggung jawab dalam mengimplementasikan tata kelola keamanan informasi pada informasi yang dimilikinya.
  - h) Bagian Manajemen Fasilitas;  
Ditugaskan kepada Perangkat Daerah yang bertanggung jawab dalam mengelola fasilitas fisik (Perangkat Keras) agar sesuai dengan kebijakan keamanan informasi.
  - i) Bagian Penjaga Keamanan;  
Ditugaskan kepada Perangkat Daerah yang bertanggung jawab dalam menjaga keamanan fasilitas fisik organisasi.
  - j) Bagian Kepatuhan Keamanan Informasi;  
Ditugaskan kepada Seksi Infrastruktur Teknologi Informasi yang bertanggung jawab dalam memastikan teknologi yang diterapkan telah sesuai dengan kebijakan, standar teknis, prosedur, dan arsitektur organisasi.
  - k) Pelaksana Keamanan Informasi;  
Pejabat dan Pegawai serta pihak eksternal yang mengakses aset informasi atau memberikan layanan aset informasi kepada Pemerintah Kabupaten Jombang, merupakan pelaksanaan keamanan informasi, sehingga bertanggung jawab untuk mengimplementasikan Tata Kelola keamanan informasi sesuai dengan tugas dan fungsi masing-masing.
  - l) Peninjauan Independen;  
Ditugaskan kepada Inspektorat untuk bertanggung jawab dalam melakukan peninjauan independen atas tata kelola keamanan informasi. Mencakup peninjauan implementasi kebijakan, pedoman dan prosedur keamanan informasi untuk menjamin efektivitasnya.

2. Kepemimpinan dan Komitmen Penanggung Jawab Eksekutif  
 Penanggung Jawab Eksekutif (Code Chief Information Officer/GCIO) dan Penanggung Jawab Utama Keamanan Informasi (Code Chief Information Security Officer/GCISO) harus menunjukkan kepemimpinan dan komitmen terkait Keamanan Informasi dengan cara:
  - a) Memastikan kebijakan keamanan informasi dan sasaran keamanan informasi ditetapkan dan selaras dengan arah strategis Pemerintah Kabupaten Jombang.
  - b) Memastikan persyaratan Keamanan Informasi terintegrasi ke dalam proses organisasi.
  - c) Memastikan tersedianya sumber daya yang dibutuhkan untuk pelaksanaan Keamanan Informasi.
  - d) Mengkomunikasikan pentingnya manajemen keamanan informasi yang efektif dan kesesuaian dengan persyaratan Keamanan Informasi.
  - e) Memastikan bahwa pelaksanaan Keamanan Informasi mencapai manfaat yang diharapkan.
  - f) Memberikan arahan dan dukungan pada personel untuk berkontribusi dalam efektivitas pelaksanaan Keamanan Informasi.
  - g) Mempromosikan perbaikan berkelanjutan; dan
  - h) Mendukung peran manajemen yang relevan lainnya untuk menunjukkan kepemimpinannya ketika diterapkan pada wilayah tanggung jawabnya.
  
3. Tanggung Jawab Penanggung Jawab Eksekutif (Government Chief Information Officer/ GCIO)  
 Penanggung Jawab Eksekutif bertanggung jawab memberikan arahan strategis keamanan informasi.  
 Penanggung Jawab Eksekutif mempunyai peran sebagai berikut:
  - a) Memberikan dukungan terhadap keamanan informasi;
  - b) Mereview dan menyetujui prinsip keamanan informasi;
  - c) Menyetujui anggaran keamanan informasi;
  - d) Menerima dan menindaklanjuti laporan manajemen terkait keamanan informasi.
  
4. Tanggung Jawab Komite Keamanan Informasi (KKI)  
 KKI merupakan Komite yang dibentuk untuk membahas dan memutuskan sejumlah aspek yang terkait dengan pengembangan, implementasi, pengoperasian, monitoring, pemeliharaan dan peningkatan tata Kelola keamanan informasi.  
 Mekanisme koordinasi dalam KKI dilakukan melalui pertemuan tatap muka secara berkala atau melalui media komunikasi lain seperti email atau social media internal Pemerintah Kabupaten Jombang.  
 Komite Keamanan Informasi mempunyai peran sebagai berikut:
  - a) Melakukan revisi kebijakan keamanan informasi yang disampaikan oleh GCISO dan disahkan oleh Bupati Jombang.
  - b) Membahas dan memutuskan pelaksanaan rewiu independen atas kebijakan keamanan informasi;
  - c) Menyepakati klasifikasi aset informasi Pemerintah Kabupaten Jombang, Klasifikasi aset informasi tersebut disahkan Bupati Jombang.
  - d) Menyepakati sanksi yang akan dikenakan apabila terjadi pelanggaran.

5. Tanggung Jawab Penanggung Jawab Utama Keamanan Informasi (Code Chief Information Security Officer/ GCISO)  
GCISO bertanggung jawab membantu GCIO dalam memimpin pengelolaan keamanan informasi di lingkungan Pemerintah Kabupaten Jombang.  
GCISO mempunyai peran sebagai berikut:
- a) Melakukan peninjauan manajemen atas kebijakan keamanan informasi secara berkala.
  - b) Menyampaikan usulan revisi kebijakan keamanan informasi, untuk selanjutnya dibahas oleh Komite Keamanan Informasi sebelum mendapat persetujuan dan pengesahan Bupati Jombang.
  - c) Memberikan masukan atas sanksi yang akan diberikan kepada setiap pelanggaran keamanan informasi.
  - d) Melakukan publikasi dan sosialisasi kendali risiko keamanan informasi kepada Staf Ahli, Inspektur, Perangkat Daerah, Kantor Badan Setda, Kecamatan/ Kelurahan dan pihak eksternal Pemerintah Kabupaten Jombang.
  - e) Memberikan masukan dan melakukan koordinasi dengan GCIO dalam pengelolaan akses aset informasi Pemerintah Kabupaten Jombang.
6. Tanggung Jawab Manajer Keamanan Informasi  
Manajer keamanan informasi bertanggung jawab untuk mengelola keamanan informasi, dan keamanan non fisik dalam organisasi. Manajer Keamanan Informasi mempunyai peran sebagai berikut:
- a) Mendefinisikan standar teknis dan non teknis, prosedur, dan panduan keamanan informasi;
  - b) Membantu Inspektorat dan Komite Keamanan Informasi dalam mendefinisikan dan mengimplementasikan kendali, proses, dan perangkat-perangkat pendukung supaya mematuhi kebijakan dan mengelola risiko keamanan informasi;
  - c) Mereviu dan memonitor kepatuhan terhadap kebijakan dan berkontribusi pada proses audit internal dan control self assessment (CSA);
  - d) Mengumpulkan, menganalisa, dan memberikan saran terkait metrik keamanan informasi dan insiden;
  - e) Mendukung Inspektorat dalam melakukan penyelidikan dan remediasi insiden keamanan informasi atau pelanggaran kebijakan lainnya;
  - f) Mengorganisasi kampanye kesadaran keamanan untuk pegawai Pemerintah Kabupaten Jombang dalam meningkatkan budaya keamanan dan mengembangkan pemahaman yang luas akan persyaratan ISO/IEC 27001;
  - g) Mengkoordinir implementasi kebijakan keamanan informasi selain keamanan fasilitas fisik;
  - h) Memastikan keberadaan dan implementasi kendali teknis, fisik, dan prosedural. Salah satunya dengan memastikan kendali diterapkan dengan tepat oleh seluruh pegawai Pemerintah Kabupaten Jombang. Manajer Keamanan Informasi memastikan:
    - 1) Pegawai Pemerintah Kabupaten Jombang diinformasikan kewajiban-kewajibannya untuk melaksanakan kebijakan keamanan informasi;
    - 2) Pegawai Pemerintah Kabupaten Jombang mematuhi kebijakan keamanan informasi dan mendukung secara aktif kendali-kendali keamanan informasi tersebut;
    - 3) Pegawai Pemerintah Kabupaten Jombang dimonitor untuk

menilai tingkat kepatuhan terhadap kebijakan keamanan informasi dan menilai penerapan kendali-kendali keamanan informasi tersebut.

- i) Memberikan arahan, dukungan dan alokasi sumberdaya dalam rangka memastikan perlindungan secara tepat aset-aset informasi;
  - j) Menginformasikan Manajemen Keamanan Informasi dan/atau Inspektorat jika ada pelanggaran kebijakan (pelanggaran yang sudah terjadi atau pelanggaran yang baru dicurigai dan berpengaruh terhadap aset pihak terkait);
  - k) Melakukan evaluasi kepatuhan terhadap kebijakan melalui proses Control Self-Assessment (CSA) dan audit internal secara periodik.
7. Tanggung Jawab Manajer Keamanan Fisik  
Manajer Keamanan Fisik bertanggung jawab untuk mengelola keamanan fasilitas fisik dalam organisasi.  
Manajer Keamanan Fisik mempunyai peran sebagai berikut:
- a) Melakukan implementasi dan manajemen akses kontrol fisik pada masing-masing fasilitas organisasi;
  - b) Melakukan implementasi dan penjagaan kendali lingkungan yang tepat untuk memastikan terdapat lingkungan yang sesuai dengan kebijakan keamanan informasi;
  - c) Mengelola dan memelihara fasilitas fisik sesuai dengan kebijakan keamanan informasi;
  - d) Memberikan otorisasi akses ke area aman organisasi;
  - e) Memastikan fasilitas fisik dan perlengkapan yang ada di dalamnya terlindung dari gangguan catu daya dan gangguan fisik lainnya;
  - f) Mengelola fasilitas fisik agar sesuai dengan kebijakan keamanan informasi;
  - g) Memastikan semua peralatan dan perlengkapan fisik pendukung dilakukan pengaturan sesuai keamanan informasi.
8. Tanggung Jawab Bagian Operasi dan Administrasi Keamanan Informasi  
Bagian Operasi dan Administrasi bertanggung jawab mengelola pelaksanaan keamanan informasi sesuai dengan arahan yang telah ditetapkan.  
Bagian Operasi dan Administrasi Keamanan Informasi mempunyai peran sebagai berikut:
- a) Mengidentifikasi infrastruktur yang memiliki risiko tinggi, menilai kerentanannya dan melakukan tindakan yang tepat dalam mengendalikan risiko pada tingkat operasional;
  - b) Manajemen kejadian keamanan informasi yang dihasilkan oleh semua perangkat operasional TI;
  - c) Manajemen insiden keamanan informasi yang akan menyebabkan kerusakan atau mengancam keamanan informasi.
9. Tanggung Jawab Pemilik Aset Informasi  
Pemilik Aset Informasi bertanggung jawab untuk mengimplementasikan tata kelola keamanan informasi pada informasi yang dimilikinya.  
Pemilik Aset Informasi mempunyai peran sebagai berikut:
- a) Melakukan proses klasifikasi dan perlindungan aset informasi secara tepat;
  - b) Menentukan dan memberikan pendanaan pada kendali protektif yang sesuai;
  - c) Memberikan hak akses pada aset informasi yang sesuai dengan klasifikasi dan kebutuhan organisasi;
  - d) Melakukan atau memberikan kuasa kepada pihak ketiga terkait proses penilaian risiko keamanan informasi untuk memastikan kebutuhan keamanan informasi didefinisikan dan



- didokumentasikan secara tepat;
- e) Memastikan proses peninjauan akses sistem/data diselesaikan tepat waktu;
- f) Memantau kepatuhan kebijakan keamanan informasi yang akan berpengaruh terhadap aset informasi Pemerintah Kabupaten Jombang.

#### 10. Tanggung Jawab Bagian Manajemen Fasilitas

Bagian Manajemen Fasilitas bertanggung jawab dalam mengelola fasilitas fisik agar sesuai dengan kebijakan keamanan informasi.

Bagian Manajemen Fasilitas mempunyai peran sebagai berikut:

- a) Melakukan perencanaan pengembangan fasilitas yang memperhatikan aspek kenyamanan dan memastikan pelaksanaannya sesuai dengan perencanaan tersebut;
- b) Menyediakan fasilitas fisik dalam pelaksanaan kebijakan keamanan informasi;
- c) Menyediakan fasilitas keamanan yang mendukung tugas operasional petugas keamanan;
- d) Melakukan pemeliharaan terhadap fasilitas listrik, saluran air, AC, kabel telekomunikasi agar terhindar dari kondisi yang dapat membahayakan orang, data dan informasi yang ada di dalam gedung, dan fasilitas itu sendiri.

#### 11. Tanggung Jawab Bagian Penjaga Keamanan

Bagian Penjaga Keamanan bertanggung jawab dalam menjaga keamanan fasilitas fisik organisasi.

Bagian Penjaga Keamanan mempunyai peran sebagai berikut.

- a) Memberikan perlindungan bagi gedung, fasilitas dan semua pegawai, tamu dan pihak-pihak yang berkepentingan kegiatan kriminal dan penyusupan;
- b) Melakukan kegiatan pencegahan dengan cara melakukan aset dan pengawasan keamanan untuk mencegah terjadinya kegiatan aset dan kejadian-kejadian yang dapat membahayakan semua orang dalam area yang dapat menyebabkan kerusakan gedung dan fasilitas terkait;
- c) Merespon dengan segera setiap ada alarm tanda bahaya diaktifkan;
- d) Melaporkan segala aktivitas pengamanan kepada atasan dan melaporkan segala aktivitas hasil pengamatan yang mencurigakan tetapi di luar kewenangannya kepada aset;
- e) Melakukan pemeriksaan kepada setiap orang dan barang yang masuk ke area perkantoran;
- f) Melakukan pencatatan semua orang yang masuk dan keluar area.

#### 12. Tanggung Jawab Bagian Kepatuhan Keamanan Informasi

Bagian Kepatuhan Keamanan Informasi bertanggung jawab memastikan teknologi yang diterapkan telah sesuai dengan kebijakan, standar teknis, prosedur, dan arsitektur organisasi.

Bagian Kepatuhan Keamanan Informasi mempunyai peran sebagai berikut:

- a) Memantau penerapan teknologi agar bisa dipastikan selaras dengan kebijakan organisasi;
- b) Melakukan peninjauan dan menilai keamanan informasi secara periodik;
- c) Mengidentifikasi dan merekomendasikan tindakan terhadap pelanggaran agar tetap sesuai dengan kebijakan organisasi;
- d) Merekomendasikan best practice manajemen keamanan informasi dan implementasinya dalam organisasi.

#### 13. Tanggung Jawab Pelaksana Keamanan Informasi

Pelaksana Keamanan Informasi bertanggung jawab untuk mengimplementasikan tata kelola keamanan informasi.

Pelaksana Keamanan Informasi mempunyai peran sebagai berikut:

- a) Melindungi kerahasiaan, integritas dan ketersediaan aset informasi yang menjadi wewenang dan tanggung jawabnya masing-masing dengan memperhatikan klasifikasi informasi dan mematuhi kebijakan, pedoman dan prosedur keamanan informasi;
- b) Mengimplementasikan keamanan informasi sesuai dengan bagian masing-masing;
- c) Melaporkan setiap insiden atau pelanggaran keamanan informasi kepada GCISO.

#### 14. Reviu Independen

Secara berkala atau apabila diperlukan, dilakukan reviu independen atas tata kelola keamanan informasi. Peninjauan tersebut mencakup peninjauan implementasi kebijakan, pedoman dan prosedur keamanan informasi untuk menjamin efektivitasnya. Peninjauan independen dapat dilakukan oleh Inspektorat atau pihak independen lain yang ditunjuk sesuai kebijakan keamanan informasi.

## IV. STANDAR PENYELENGGARAAN

### A. Manajemen Risiko Keamanan Informasi

#### 1. Ruang Lingkup dan Tujuan

Ruang lingkup manajemen risiko meliputi identifikasi risiko, analisa dan evaluasi risiko, identifikasi dan evaluasi aset ative penanganan risiko, persetujuan pimpinan atas manajemen risiko serta pernyataan pelaksanaan manajemen risiko.

Tujuan manajemen risiko yaitu:

- a) Mendukung tata kelola keamanan informasi;
- b) Kepatuhan terhadap ISO 27001;
- c) Persiapan business continuity plan;
- d) Persiapan incident response plan;
- e) Penyusunan persyaratan keamanan informasi.

#### 2. Kebijakan Manajemen Risiko Keamanan Informasi

Manajemen risiko terdiri dari beberapa tahapan yaitu pembentukan konteks, identifikasi risiko, analisa dan evaluasi risiko, identifikasi 85 evaluasi aset ative penanganan risiko, persetujuan pimpinan dan pernyataan penerapan manajemen keamanan informasi.

Berikut kebijakan pada masing-masing tahapan tersebut.

- a) Pembentukan Konteks;
  - 1) Menentukan lingkup dan batasan manajemen risiko sesuai dengan operasi, struktur, lokasi, aset, dan teknologi yang ada di Pemerintah Kabupaten Jombang.
  - 2) Merupakan kriteria yang akan digunakan untuk mengevaluasi risiko keamanan informasi di Pemerintah Kabupaten Jombang.
- b) Identifikasi Risiko;
  - 1) Identifikasi aset informasi sesuai dengan lingkup manajemen risiko dan pemilik dari aset tersebut;
  - 2) Identifikasi ancaman atas aset informasi tersebut;
  - 3) Identifikasi kerentanan sebagai hasil ancaman tersebut;
  - 4) Identifikasi dampak dari hilangnya kerahasiaan, integritas dan ketersediaan serta independensi yang mungkin terjadi atas aset informasi tersebut.
- c) Analisis dan Evaluasi Risiko;
  - 1) Perkiraan dampak yang diterima oleh Pemerintah Kabupaten Jombang jika terjadi suatu kegagalan keamanan informasi,

- termasuk juga konsekuensi atas hilangnya kerahasiaan, integritas dan ketersediaan informasi;
- 2) Perkiraan kemungkinan munculnya kegagalan keamanan akibat adanya ancaman, kerentanan, dan dampak yang berkaitan dengan aset informasi tersebut dan pengendalian yang dilakukan saat ini;
  - 3) Perkirakan tingkatan untuk setiap risiko;
  - 4) Tentukan apakah risiko dapat diterima atau memerlukan Tindakan lebih lanjut menggunakan kriteria risiko yang wajar yang telah ditetapkan;
- d) Identifikasi dan Evaluasi Alternatif Penanganan Risiko;
- 1) Melakukan pengendalian yang memadai atas risiko tersebut;
  - 2) Menerima risiko tersebut sesuai dengan kebijakan Pemerintah Kabupaten Jombang;
  - 3) Menghindari risiko tersebut;
  - 4) Memilih tujuan dan rancangan pengendalian sebagai bentuk penanganan risiko, yang didasarkan kepada standar SNI ISO/IEC 27001:2009, ISO/IEC 27005:2008, PP60/2008 SPIP dan standar lain.
- e) Persetujuan Pimpinan;
- 1) Persetujuan dari Pimpinan Pemerintah Kabupaten Jombang atas hasil analisis risiko keamanan informasi dan risk treatment plan;
  - 2) Otorisasi Pimpinan Pemerintah Kabupaten Jombang untuk menerapkan dan melaksanakan manajemen risiko keamanan informasi.
- f) Pernyataan Penerapan Manajemen Keamanan Informasi (Statement of Applicability / SOA);
- 1) Tujuan pengendalian dan rancangan pengendalian yang dipilih serta alasan pemilihan pengendalian tersebut;
  - 2) Tujuan pengendalian dan rancangan pengendalian yang dilaksanakan saat ini;
  - 3) Pengecualian untuk setiap tujuan pengendalian dan rancangan pengendalian dari standar yang akan disertifikasi serta alasan pengecualiannya.

## B. PENGELOLAAN HAK AKSES

### 1. Ruang Lingkup dan Tujuan

Ruang lingkup pengelolaan hak akses yaitu akses fisik maupun logik terhadap informasi elektronik maupun non elektronik oleh pihak internal maupun eksternal.

Tujuan pengelolaan hak akses yaitu untuk mengendalikan akses terhadap informasi yang dimiliki Pemerintah Kabupaten Jombang sehingga informasi hanya bisa diakses oleh pihak yang berwenang saja. Pengelolaan hak akses meliputi pemberian hak akses, pemberian hak akses kepada pihak eksternal, pengendalian akses jaringan dan sistem operasi.

## 2. Kebijakan Pengelolaan Hak Akses

Pengelolaan hak akses dibagi tiga yaitu pemberian hak akses, pemberian hak akses kepada pihak eksternal, pengendalian akses jaringan dan sistem operasi. Berikut kebijakan pada masing-masing bagian tersebut.

### a) Pengelolaan Hak Akses;

Pengelolaan hak akses dibagi tiga yaitu pemberian hak akses, pemberian hak akses kepada pihak eksternal, pengendalian akses jaringan dan sistem operasi. Berikut kebijakan pada masing-masing bagian tersebut.

### b) Pemberian Hak Akses;

#### 1) Pemberian hak akses atas informasi dilakukan dengan tata cara umum sebagai berikut:

- a) Pihak-pihak yang membutuhkan akses terhadap suatu informasi mengajukan permohonan hak akses kepada pemilik informasi secara tertulis;
- b) Pemilik informasi harus memastikan bahwa pihak-pihak pengguna yang membutuhkan akses terhadap informasi telah menandatangani perjanjian kerahasiaan sesuai dengan ketentuan yang ada;
- c) Untuk informasi yang berbentuk non-elektronis, persetujuan diberikan oleh pemilik informasi untuk disampaikan kepada pengguna sebagai pemberitahuan;
- d) Untuk informasi yang berbentuk non-elektronis, persetujuan diberikan oleh pemilik informasi untuk disampaikan kepada pengguna sebagai pemberitahuan serta ditindaklanjuti pemberian hak akses kepada pengguna terhadap informasi secara elektronik.

#### 2) Pengelola informasi menindak lanjuti pemberian hak akses informasi dengan ketentuan sebagai berikut:

- a) Memberikan atau membuka akses apabila seluruh pedoman sudah dipenuhi, serta berhak untuk membatasi hak akses dari setiap pengguna sesuai dengan kebutuhan yang telah ditentukan dan sesuai dengan perizinan yang diberikan oleh pemilik informasi;
- b) Menjaga catatan pengelolaan hak akses serta memastikan bahwa pihak-pihak yang memiliki hak akses istimewa telah dikendalikan dengan memadai;
- c) Memverifikasi pemberian password baru, password pengganti, dan password sementara, memastikan bahwa pengguna hak akses telah menerima password yang diberikan, dan password dari vendor selama proses pemasangan sistem dan/atau piranti lunak harus segera diganti;
- d) Melakukan peninjauan secara periodik terhadap hak akses informasi, termasuk pemeriksaan tingkatan akses yang diberikan dan penghapusan atau pemblokiran terhadap kelebihan penerbitan hak akses, dan harus segera merubah atau memblokir hak akses apabila pengguna pindah jabatan ataupun pindah kerja/keluar dari Pemerintah Kabupaten Jombang.

#### 3) Setelah hak akses diberikan, setiap pemilik hak akses informasi elektronik (User ID dan Password) diharuskan:

- a) Mengganti password segera setelah menerima hak atas akses informasi dengan segera mengubah password sementara Ketika pertama log-in;
- b) Menjaga kerahasiaan password dengan tidak menuliskan

password pada kertas, komputer, dan/atau media lain yang tidak dilindungi dan mudah dibaca oleh pihak yang tidak berkepentingan;

- c) Mengubah password dengan segera apabila terdapat indikasi mencurigakan atau masalah pada sistem;
  - d) Menggunakan password dengan kriteria: mudah dihafal, tidak mudah ditebak orang lain, gunakan kombinasi angka, huruf kecil, tanda baca dan huruf besar;
  - e) Mengganti password secara berkala, untuk password akun tertentu (akun khusus atau akun yang kritis) harus lebih sering diganti, dan tidak menggunakan kembali password yang pernah digunakan;
  - f) Menggunakan password dinas yang berbeda dengan password untuk kebutuhan pribadi (contohnya membedakan email (surel) pribadi dengan surel kantor).
- c) Pemberian Hak Akses kepada Pihak Eksternal;
- Pemilik informasi sebagai pihak yang memberikan izin atas permintaan akses informasi kepada pihak eksternal harus memperhatikan hal-hal sebagai berikut:
- 1) Permohonan tertulis pihak eksternal atas setiap jenis informasi yang akan diakses dan fasilitasnya;
  - 2) Akses fisik, akses logik oleh pengguna dan sambungan jaringan antara Pemerintah Kabupaten Jombang dengan pihak eksternal, baik akses on-site, off-site maupun remote-site;
  - 3) Klasifikasi keamanan informasi dengan mempertimbangkan nilai, sensitivitas informasi dan tingkat risiko Pemerintah Kabupaten Jombang;
  - 4) Pihak-pihak eksternal lain yang terlibat dalam penanganan aset informasi di Pemerintah Kabupaten Jombang dan pengendalian yang diperlukan untuk melindungi informasi yang tidak boleh diakses oleh pihak eksternal;
  - 5) Perbedaan pemahaman dan pengendalian yang dilakukan pihak eksternal dalam hal penyimpanan, pemrosesan, komunikasi, pertukaran, dan perubahan informasi;
  - 6) Dampak hak akses tidak tersedia bagi pihak eksternal saat dibutuhkan atau dampak kesalahan informasi yang diterima oleh pihak eksternal.
- d) Pengendalian Akses Jaringan dan Sistem Operasi;
- 1) Mengendalikan akses ke jaringan data dan layanan yang ada di jaringan data. Pengendalian tersebut dengan menetapkan kriteria yang harus dipenuhi, pihak yang diperbolehkan mengakses jaringan data, serta jaringan / layanan jaringan yang bisa diakses;
  - 2) Memperoleh kepastian mengenai sumber sambungan jaringan dengan mengotentifikasi pengguna sambungan jaringan tersebut. Pengendalian otentifikasi tambahan dapat diimplementasikan untuk pengendalian akses melalui jaringan lain;
  - 3) Menggunakan peralatan akses jaringan khusus yang hanya dapat digunakan bersama dengan teknik tertentu. Peralatan tersebut harus dapat mengidentifikasi jaringan yang mendapatkan izin untuk diakses dan harus selalu memastikan keamanan peralatan tersebut;
  - 4) Menetapkan domain jaringan berdasarkan pada penilaian risiko dan tingkat kebutuhan keamanan untuk setiap domain;

- 5) Memastikan bahwa penggunaan jaringan selalu dipantau, dibatasi, atau dilarang untuk tujuan tertentu. Tujuan tertentu tersebut antara lain email pribadi, pemindahan data yang tidak ada kaitannya dengan kegiatan Pemerintah Kabupaten Jombang, akses interaktif dan aplikasi interaktif yang dapat memindahkan data ke tempat lain;
- 6) Memastikan bahwa penggunaan jaringan bersama, khususnya yang keluar dari Pemerintah Kabupaten Jombang telah memiliki pengendalian tambahan terutama jika terdapat jaringan yang dapat digunakan bersama dengan pihak ketiga (pengguna diluar Pemerintah Kabupaten Jombang);
- 7) Berkaitan dengan pengelolaan komputer pengguna harus dipastikan bahwa:
  - a) Di setiap komputer pengguna telah menampilkan peringatan bahwa "komputer hanya dapat diakses oleh pihak yang mempunyai otorisasi";
  - b) Komputer pengguna tidak memperlihatkan karakter untuk password yang sedang dimasukkan pada saat log-on;
  - c) Komputer pengguna tidak menampilkan sistem atau aplikasi sampai proses log-on benar-benar selesai;
  - d) Layar komputer harus bersih pada saat istirahat (time-out). Aplikasi harus ditutup setelah jangka waktu tertentu apabila tidak digunakan.
- 8) Berkaitan dengan pengelolaan akun dan password, harus dipastikan bahwa:
  - a) Seluruh pegawai Pemerintah Kabupaten Jombang / pengguna selalu menggunakan user ID dan password untuk menjaga akuntabilitas informasi. Pengendalian "unique identifier" [user ID] berlaku pada seluruh jenis pengguna sistem informasi di Pemerintah Kabupaten Jombang;
  - b) User ID selalu digunakan sehingga aktivitas pengguna dan fungsi dapat dilacak, dibatasi dan dikendalikan;
  - c) Kepentingan pribadi atau diluar kegiatan Pemerintah Kabupaten Jombang tidak diperbolehkan menggunakan akun yang sama dengan akun untuk kegiatan Pemerintah Kabupaten Jombang;
  - d) Pada keadaan tertentu penggunaan ID bersama untuk grup atau pekerjaan tertentu diperbolehkan setelah mendapatkan persetujuan Manajer Keamanan Informasi;
  - e) Terdapat rekaman pengguna, penggunaan password, serta catatan penggunaan password yang sama dan atau berulang;
  - f) Penyimpanan password para pengguna di tempat atau sistem terpisah dari data sistem aplikasi, serta terlindung pada saat pembuatan, penyimpanan dan pengirimannya;
  - g) Setiap pengguna diwajibkan untuk menggunakan pedoman identifikasi, otentifikasi, dan otorisasi dalam menggunakan utilitas sistem operasi. Penggunaan utilitas sistem operasi dibatasi dan harus terdapat rekaman/log dari seluruh penggunaannya;
  - h) Seluruh akun yang sudah tidak digunakan harus dihapus/ dibuang/ dinonaktifkan;
  - i) Terdapat batas minimum dan maksimum waktu penggunaan akses pada sistem informasi di Pemerintah Kabupaten Jombang;
- 9) Memastikan penggunaan fasilitas mobile computer dan alat

komunikasi untuk kepentingan pribadi tidak diizinkan;

- 10) Menentukan peralatan komunikasi yang tepat dan dapat digunakan di Pemerintah Kabupaten Jombang, termasuk metode pengamanan akses jarak jauh, serta piranti lunak dan piranti keras pendukungnya;
- 11) Seluruh pegawai Pemerintah Kabupaten Jombang / pengguna disarankan untuk tidak meninggalkan seluruh piranti mobile computer dan alat komunikasi tanpa mendapat penjagaan dan perhatian seperti di mobil, kamar hotel, conference center, tempat rapat.

### C. KRIPTOGRAFI

#### 1. Ruang Lingkup dan Tujuan

Tujuan dari kebijakan terkait teknologi kriptografi adalah untuk memastikan penggunaan teknologi kriptografi yang sesuai dan efektif untuk melindungi kerahasiaan, keaslian dan/atau integritas dari informasi, serta penggunaan teknologi kriptografi dalam pengolahan dan penyimpanan informasi di dalam lingkungan Pemerintah Kabupaten Jombang.

#### 2. Kebijakan Kriptografi

- a) Kontrol kriptografi dapat digunakan untuk menjamin kerahasiaan dan integritas dari informasi sensitif di lingkungan Perangkat Daerah.
- b) Kontrol kriptografi dapat mencakup namun tidak terbatas pada:
  - 1) Enkripsi informasi dan jaringan komunikasi.
  - 2) Pemeriksaan integritas informasi, seperti hashing
  - 3) Otentikasi identitas
  - 4) Digital signatures.
- c) Implementasi dari kontrol kriptografi harus mempertimbangkan klasifikasi dari informasi yang akan diamankan.
- d) Pemilihan kontrol kriptografi harus mempertimbangkan:
  - 1) Jenis dari kontrol kriptografi.
  - 2) Kekuatan dari algoritma kriptografi; dan
  - 3) Panjang dari kunci kriptografi.
- e) Implementasi dari kontrol kriptografi harus secara berkala ditinjau untuk memastikan kecukupan dan kesesuaian dari kontrol tersebut dalam mengamankan kerahasiaan dan integritas dari informasi.
- f) Pengelolaan dari kunci kriptografi harus dikendalikan secara ketat dan dibatasi hanya pada personil yang terotorisasi.
- g) Pengelolaan dari kunci kriptografi didasarkan pada prinsip dual custody untuk mengurangi risiko penyalahgunaan.

### D. PENGENDALIAN ASPEK SUMBER DAYA MANUSIA

#### 1. Ruang Lingkup dan Tujuan

Ruang lingkup pengendalian aspek SDM yaitu proses pemeriksaan dan verifikasi latar belakang (screening) calon pegawai, sosialisasi peran dan tanggung jawab dalam keamanan informasi termasuk perjanjian kerahasiaan, pendidikan dan pelatihan peningkatan keamanan informasi, dan perubahan dan/atau penghapusan hak akses informasi dan pengembalian aset informasi jika ada pemberhentian, perubahan, atau berakhirnya perjanjian kerja. Tujuan pengendalian aspek SDM yaitu:

- a) Memastikan bahwa seluruh pegawai Pemerintah Kabupaten Jombang memahami peran dan tanggung jawab mereka terhadap keamanan informasi untuk mengurangi risiko terjadinya pencurian, kecurangan, dan penyalahgunaan aset informasi dan fasilitas pengolahnya;
- b) Memastikan bahwa seluruh pegawai Pemerintah Kabupaten

Jombang waspada terhadap ancaman keamanan informasi sehingga mereka sadar akan peran dan tanggungjawab mereka untuk mengurangi risiko terjadinya insiden karena faktor kelalaian manusia;

- c) Memastikan bahwa proses pemberhentian atau perubahan pegawai Pemerintah Kabupaten Jombang dilakukan dengan cara yang benar.

## 2. Kebijakan Pengendalian Aspek Sumber Daya Manusia

Pengendalian Aspek SDM dibagi enam adalah proses pemeriksaan dan verifikasi latar belakang (Screening), sosialisasi peran dan tanggung jawab dalam keamanan informasi, perjanjian kerahasiaan, pendidikan dan pelatihan peningkatan keamanan informasi, pengembalian aset informasi, dan perubahan dan/atau penghapusan hak akses informasi.

Berikut kebijakan pada masing-masing bagian tersebut:

- a) Proses pemeriksaan dan verifikasi latar belakang (Screening);
  - 1) Melakukan proses verifikasi dan pemeriksaan mengenai latar belakang untuk semua calon pegawai Pemerintah Kabupaten Jombang untuk memastikan bahwa latar belakang mereka telah memenuhi persyaratan sesuai peraturan hukum perundang-undangan dan etika, serta sesuai dengan persyaratan yang ditetapkan oleh Pemerintah Kabupaten Jombang;
  - 2) Proses pemeriksaan dan verifikasi latar belakang (screening) harus meliputi informasi-informasi berikut:
    - a) Keterangan mengenai karakter yang dimiliki, baik secara individu maupun organisasi;
    - b) Keterangan mengenai daftar riwayat hidup yang lengkap;
    - c) Konfirmasi mengenai kualifikasi pendidikan dan akademis;
    - d) Keterangan mengenai kompetensi;
    - e) Keterangan mengenai catatan kriminal (jika ada); dan
    - f) Kegiatan dalam dunia maya termasuk cracking.
- b) Sosialisasi Peran dan Tanggungjawab dalam Keamanan Informasi;
  - 1) Memberikan arahan yang memadai kepada para pegawai Pemerintah Kabupaten Jombang, mengenai peran dan tanggungjawab mereka terhadap keamanan informasi sebelum hak akses diberikan kepada mereka.
  - 2) Memotivasi pegawai Pemerintah Kabupaten Jombang agar memiliki rasa kesadaran akan peran dan tanggungjawab mereka terhadap keamanan informasi sehingga dapat memenuhi semua kebijakan keamanan informasi di lingkungan Pemerintah Kabupaten Jombang.
- c) Perjanjian Kerahasiaan;
  - 1) Memastikan bahwa seluruh pegawai Pemerintah Kabupaten Jombang menyetujui peran dan tanggungjawab keamanan informasi yang diberikan kepada mereka dengan menandatangani surat perjanjian yang menyatakan kesanggupan menjaga kerahasiaan dan larangan penyingkapan untuk jenis aset informasi yang bersifat sensitif bagi Pemerintah Kabupaten Jombang.
  - 2) Seluruh pegawai Pemerintah Kabupaten Jombang setiap tahun harus menandatangani perjanjian kerahasiaan sebagai bagian dari perjanjian kerja pegawai.
  - 3) Memastikan bahwa seluruh rekanan penyedia barang dan jasa di Pemerintah Kabupaten Jombang telah menyetujui



peran dan tanggungjawab keamanan informasi yang diberikan kepada mereka dengan menandatangani surat perjanjian yang menyatakan kesanggupan menjaga kerahasiaan dan larangan penyingkapan untuk jenis aset informasi yang bersifat sensitif bagi Pemerintah Kabupaten Jombang.

- 4) Memastikan bahwa seluruh komisi dan instansi yang menjadi rekan kerja Pemerintah Kabupaten Jombang telah menyetujui peran dan tanggungjawab keamanan informasi yang diberikan kepada mereka dengan menandatangani surat perjanjian yang menyatakan kesanggupan menjaga kerahasiaan dan larangan penyingkapan untuk jenis aset informasi yang bersifat sensitif bagi Pemerintah Kabupaten Jombang dan yang dilarang menurut peraturan perundangan yang berlaku.
- 5) Hal-hal yang harus diperhatikan dalam perjanjian kerahasiaan antara lain adalah sebagai berikut:
  - a) Setiap butir perjanjian yang disetujui tidak mengandung kesalahpahaman dan Pemerintah Kabupaten Jombang mendapat jaminannya dan sesuai dengan kebijakan keamanan informasi yang berlaku;
  - b) Pedoman perlindungan informasi serta mekanisme dan pengendalian atas perlindungan fisik yang dibutuhkan termasuk pengendalian untuk memastikan perlindungan dari penyalahgunaan aplikasi;
  - c) Pengendalian untuk memastikan pengembalian atau penghancuran aset informasi yang penting dan rahasia pada saat berakhirnya perjanjian;
  - d) Kerahasiaan, keintegritasan, dan ketersediaan terhadap hak kekayaan intelektual dan hak cipta, dan pembatasan untuk penggandaan dan penyingkapan informasi;
  - e) Struktur pelaporan yang jelas dan format pelaporan yang telah disetujui mengenai keamanan informasi, termasuk pengaturan untuk masalah perubahan yang jelas dan spesifik;
  - f) Perbedaan alasan, persyaratan, dan keuntungan yang didapat dan dibutuhkan oleh pihak-pihak yang memiliki hak akses atas informasi;
  - g) Persyaratan untuk mengurus daftar personil yang diizinkan menggunakan jasa layanan yang tersedia, termasuk juga hak khusus mereka dalam hal penggunaan dan pernyataan bahwa seluruh akses yang tidak memiliki persetujuan adalah dilarang;
  - h) Pengaturan mengenai pelaporan, pengumuman, dan penyelidikan atas kasus keamanan informasi dan pelanggaran keamanan, termasuk juga pelanggaran atas persyaratan;
  - i) Hak untuk mengawasi, mencabut, dan semua aktivitas yang bersinggungan dengan aset informasi Pemerintah Kabupaten Jombang termasuk proses untuk mencabut hak akses atau memotong sambungan antara dua sistem;
  - j) Hak untuk mengaudit semua bentuk tanggungjawab yang telah ditetapkan dalam perjanjian, di mana audit dilakukan oleh pihak ketiga, dan mengakumulasikan hak dasar bagi para auditor;
  - k) Keterlibatan pihak ketiga dengan subkontraktor, dan implementasi dari pengendalian keamanan terhadap subkontraktor termasuk rencana antisipasi untuk kemungkinan terjadinya / timbulnya keinginan dari

pihak ketiga untuk mengakhiri perjanjian sebelum waktunya;

- 1) Dokumentasi terakhir/terbaru mengenai daftar aset, lisensi, perjanjian atau hak yang berhubungan dengan pihak ketiga, termasuk negosiasi ulang untuk suatu perjanjian jika persyaratan keamanan di lingkungan Pemerintah Kabupaten Jombang berubah.
- d) Pendidikan dan Pelatihan Peningkatan Keamanan Informasi;
- Merancang dan memberikan pendidikan dan pelatihan di seluruh lingkungan Pemerintah Kabupaten Jombang secara rutin dengan tujuan sebagai berikut:
- 1) Membangun kesadaran akan keamanan informasi;
  - 2) Mengenali masalah-masalah keamanan informasi dan kasus-kasus yang mungkin terjadi;
  - 3) Mengantisipasi adanya perubahan dalam kebijakan atau pedoman yang berlaku.
- e) Sanksi atas Pelanggaran Pengendalian Keamanan Informasi;
- 1) Melakukan proses pendisiplinan kepada seluruh pegawai Pemerintah Kabupaten Jombang, yang terbukti melakukan pelanggaran keamanan informasi dengan memberikan sanksi sesuai dengan tingkat pelanggaran yang dilakukan;
  - 2) Merancang dan menentukan bentuk-bentuk sanksi yang akan diberikan dan sebisa mungkin proses pendisiplinan ini dapat dijadikan alat pencegahan untuk mengantisipasi atau meminimalisir terjadinya pelanggaran terhadap kebijakan keamanan informasi;
  - 3) Mengambil tindakan tegas jika pegawai Pemerintah Kabupaten Jombang terbukti melakukan pelanggaran terhadap persyaratan, kebijakan, dan pedoman keamanan informasi yang berlaku.
- f) Pengembalian Aset Informasi;
- 1) Memastikan bahwa setiap perjanjian kerja untuk para pegawai Pemerintah Kabupaten Jombang yang dibuat telah mencakup ketentuan mengenai tanggungjawab dan tugas yang terkait dengan keamanan informasi yang harus diselesaikan sesaat setelah pemberhentian / perubahan dilakukan;
  - 2) Jika seorang pegawai Pemerintah Kabupaten Jombang yang akan memasuki tahap pemberhentian / perubahan penugasan memiliki informasi atau pengetahuan yang cukup banyak dan penting bagi keperluan dan tujuan Pemerintah Kabupaten Jombang, harus dipastikan bahwa informasi dan pengetahuan itu telah didokumentasikan dan disampaikan kepada secara lengkap dan jelas;
  - 3) Pada proses pemberhentian, perubahan, atau berakhimyasana perjanjian, harus dipastikan bahwa setiap pegawai Pemerintah Kabupaten Jombang telah mengembalikan seluruh aset informasi yang selama ini menjadi kewenangannya kepada Pemerintah Kabupaten Jombang dengan memindahkan setiap aset informasi dari media pribadi ke media milik Pemerintah Kabupaten Jombang atau dengan menghapuskannya dari media pribadi tersebut.
- g) Penghapusan dan/atau Perubahan Hak Akses;
- 1) Memastikan bahwa semua hak akses yang dimiliki oleh pegawai Pemerintah Kabupaten Jombang telah dihapuskan sesaat setelah pemberhentian, perubahan, atau berakhirnya perjanjian kerja;
  - 2) Hak akses yang harus dihapuskan meliputi: akses fisik, akses

- logis, kunci, kartu identitas, fasilitas pengolah informasi, dll.
- 3) Penghapusan hak akses sesaat sebelum memasuki pemberhentian atau perubahan penugasan dilakukan dengan memperhatikan hal-hal berikut:
    - a) Inisiatif dan alasan dilakukannya pemberhentian atau perubahan;
    - b) Tanggungjawab terakhir atau terkini dari pegawai Pemerintah Kabupaten Jombang;
    - c) Nilai dari aset informasi terkini yang dapat diakses oleh pegawai Pemerintah Kabupaten Jombang.
  - 4) Melakukan antisipasi bagi pegawai Pemerintah Kabupaten Jombang, kontraktor, dan pihak pengguna yang merasa tidak puas dengan pemberhentian tersebut dan mungkin melakukan pencurian aset informasi yang penting dan sensitif;
  - 5) Melakukan tindakan pengarahan kepada kelompok yang masih memiliki hak akses terhadap aset informasi untuk tidak lagi berbagi informasi kepada pegawai yang sudah tidak memiliki hak akses karena adanya pemberhentian atau perubahan penugasan untuk hak akses secara kelompok.

#### E. PENGAMANAN PENGEMBANGAN DAN PEMELIHARAAN SISTEM INFORMASI

##### 1. Ruang Lingkup dan Tujuan

Ruang lingkup pengamanan pengembangan dan pemeliharaan sistem operasi yaitu pertimbangan keamanan dalam pengembangan dan pemeliharaan, pengendalian aplikasi, penggunaan enkripsi, pengamanan kode sumber, file sistem dan data pengujian, manajemen perubahan, pengendalian kebocoran informasi dan kelemahan teknis.

Tujuan pengamanan pengembangan dan pemeliharaan sistem informasi yaitu untuk memastikan keamanan menjadi bagian integral dari sistem informasi.

##### 2. Kebijakan Pengamanan Pengembangan dan Pemeliharaan Sistem Informasi

Pengamanan pengembangan dan pemeliharaan sistem informasi terdiri dari beberapa kebijakan yaitu pertimbangan keamanan dalam pengembangan dan pemeliharaan, pengendalian aplikasi, penggunaan enkripsi, pengamanan kode sumber, file sistem dan data pengujian, manajemen perubahan, pengendalian kebocoran informasi dan kelemahan teknis. Berikut kebijakan pada masing-masing bagian tersebut:

###### a) Pertimbangan Keamanan dalam Pengembangan dan Pemeliharaan;

Dalam pengembangan dan pemeliharaan, pertimbangan berikut harus diperhatikan.

- 1) Nilai aset informasi dan kemungkinan gangguan terhadap aktivitas Pemerintah Kabupaten Jombang karena kegagalan sistem informasi;
- 2) Integrasi sistem dengan sistem yang dimiliki Pemerintah Kabupaten Jombang;
- 3) Kriteria keamanan dalam kontrak dengan vendor;
- 4) Penilaian risiko terhadap produk yang tidak memenuhi persyaratan keamanan yang diperlukan dan menentukan kendali alternatif untuk meminimalkan risiko;
- 5) Review keamanan pada fitur-fitur tambahan. Apabila dapat meningkatkan risiko keamanan informasi maka fitur tersebut sebaiknya tidak digunakan;

- 6) Evaluasi keamanan oleh pihak ketiga apabila diperlukan.
- b) Pengendalian Aplikasi;

Aplikasi yang ada di Pemerintah Kabupaten Jombang harus memiliki pengendalian memadai, minimal mampu melakukan validasi data masukan, validasi pemrosesan, dan validasi data keluaran. Validasi tersebut dilakukan dengan menerapkan hal-hal berikut.

- 1) Pemeriksaan data masukan, data referensi (nama, alamat, nomor referensi), dan parameter lainnya, termasuk dokumen sumber data masukan dari perubahan yang tidak diotorisasi;
- 2) Pemeriksaan secara berkala terhadap isi key field dan data field untuk menegaskan validasi dan integritas data;
- 3) Pedoman khusus dalam menghadapi kesalahan validasi (apabila terjadi kesalahan), serta pengujian kewajaran data masukan;
- 4) Penetapan tanggung-jawab untuk setiap pegawai/personel yang terlibat dalam proses pemasukan data;
- 5) Pencatatan/perekaman seluruh kegiatan proses pemasukan data;
- 6) Penggunaan pengujian dan pemvalidasi secara otomatis yang digunakan untuk mengurangi risiko kesalahan dalam memasukkan data dan mencegah buffer overrun / overflow dan code injection;
- 7) Perancangan dan implementasi aplikasi diharuskan dapat meminimalisasi risiko kesalahan dalam pemrosesan informasi;
- 8) Program aplikasi yang digunakan beroperasi dengan benar pada waktu yang telah ditentukan dan jika terjadi kesalahan maka pemrosesan berikutnya segera dihentikan;
- 9) Validasi hasil keluaran, yang meliputi pengujian kewajaran data keluaran, tanggung-jawab untuk setiap pegawai /personel yang terlibat dalam pemrosesan data keluaran dan catatan atas aktivitas proses validasi data keluaran.

## c) Penggunaan Enkripsi;

Pada pengembangan aplikasi, informasi yang ada di aplikasi Pemerintah Kabupaten Jombang harus disandi sesuai dengan tingkatan klasifikasi keamanan informasi dan kunci enkripsi telah dikelola dengan baik sesuai dengan peraturan perundang-undangan, dengan melaksanakan hal-hal sebagai berikut:

- 1) Menerapkan enkripsi pada informasi yang sensitif/kritikal baik selama penyimpanan maupun pemindahan untuk memastikan kerahasiaan;
- 2) Menggunakan tanda tangan digital atau kode otentifikasi pada pesan yang sensitif/ kritikal baik selama penyimpanan maupun pemindahan untuk memastikan integritas/otentifikasi;
- 3) Menggunakan teknik kriptografi untuk membuktikan terjadi atau tidaknya suatu kejadian atau tindakan untuk memastikan non repudiasi.

## d) Pengamanan Kode Sumber, File Sistem, dan Data Pengujian

Pengamanan kode sumber, file sistem dan data pengujian dengan memastikan bahwa:

- 1) kode sumber aplikasi, file-file sistem dan data pengujian aplikasi telah dikendalikan dengan baik;
- 2) instalasi atas aplikasi hanya dilakukan oleh pihak yang berhak, sesuai pedoman; dan
- 3) perubahan atas berbagai paket aplikasi harus diminimalisir dan dikendalikan dengan baik, antara lain dengan melaksanakan hal berikut:
  - 4) Penggunaan sistem operasi dengan kode yang sah;
  - 5) Pemutakhiran piranti lunak, aplikasi dan program dilakukan oleh pegawai yang terlatih dan telah mendapat otorisasi;
  - 6) Analisa risiko terkait apabila menggunakan piranti lunak (software) yang tidak mendapat dukungan /bantuan pelayanan dari vendor;
  - 7) Pemastian vendor yang mensuplai piranti lunak (software) dapat membantu apabila dibutuhkan dan aktivitas pemeliharaan oleh vendor tersebut harus senantiasa dipantau;
  - 8) Pengujian piranti lunak atau aplikasi harus dilakukan dan strategi rollback harus dapat dilakukan sebelum mengubah sistem yang telah diimplementasikan;
  - 9) Pedoman yang digunakan dalam sistem aplikasi pada lingkungan operasional juga diterapkan pada lingkungan pengujian sistem aplikasi, dan harus dilakukan pemisahan otorisasi setiap informasi operasi yang di duplikat (copy) ke sistem pengujian aplikasi, serta informasi mengenai data pengujian harus segera dihapuskan setelah pengujian selesai dilakukan;
- 10) Penjagaan data kode sumber (source code) secara ketat dan kode sumber tersebut tidak boleh berada dalam lingkungan operasional;
- 11) Pembatasan akses pegawai pendukung / tambahan / sementara pada bagian sistem informasi terhadap kumpulan data kode sumber (source code);
- 12) Pemeliharaan, penduplikasian, pemutakhiran kumpulan kode sumber (source code) dan dokumen terkait, yang hanya bisa dilakukan setelah mendapatkan otorisasi dari petugas yang berwenang;
- 13) Pemeliharaan rekaman hasil pemeriksaan/audit yang

berhubungan dengan akses kumpulan program sumber.

e) Manajemen Perubahan;

Keamanan dalam manajemen perubahan dilakukan dengan beberapa hal berikut:

- 1) Persetujuan resmi harus dilakukan sebelum pelaksanaan perubahan dan penjagaan dokumen persetujuan perubahan dari pihak yang terkait;
- 2) Pemberitahuan harus dilakukan ketika akan ada perubahan sehingga dapat direviu dan diuji sebelumnya dan perubahan tersebut dimasukkan dalam rencana keberlangsungan / Pemerintah Kabupaten Jombang;
- 3) Pemilihan waktu yang tepat dalam perubahan sehingga tidak mengganggu operasi;
- 4) Perubahan dokumentasi pendukung ketika diperlukan dan apabila dilakukan perubahan dokumentasi pendukung, dokumentasi sebelumnya harus segera ditarik atau dimusnahkan;
- 5) Perjanjian lisensi piranti lunak, perjanjian penjaminan dengan pihak lain (escrow arrangement) dalam hal terjadi kegagalan/kebangkrutan pihak outsource, penjaminan kualitas dan keamanan piranti lunak,

f) Pengendalian Kebocoran Informasi dan Kelemahan Teknikal;

Pengendalian kebocoran informasi dan kelemahan teknikal dilakukan dengan beberapa hal berikut:

- 1) Penetapan kelompok atau perorangan yang bertanggung-jawab untuk memantau kelemahan-kelemahan yang ada pada seluruh sistem informasi Pemerintah Kabupaten Jombang, termasuk mengamati media dan komunikasi yang berada diluar area Pemerintah Kabupaten Jombang untuk menghindari informasi yang terselubung, memantau secara berkala terhadap pegawai Pemerintah Kabupaten Jombang maupun aktivitas sistem, memantau penggunaan sumber daya yang ada pada sistem komputer, melakukan pencegahan penggunaan jaringan akses yang tidak terotorisasi untuk melacak saluran terselubung / tersembunyi;
- 2) Pengelolaan informasi spesifik yang sangat dibutuhkan dalam membantu mengatasi penyerangan, termasuk daftar vendor piranti lunak, nomor versi piranti lunak, daftar instalasi piranti lunak ke sistem yang ada, dan orang yang bertanggung-jawab terhadap piranti lunak tersebut;
- 3) Penetapan peranan dan tanggung jawab monitoring serangan, penilaian risiko terhadap serangan, penutupan celah, pembaharuan (update) piranti lunak yang ada;

**BAB III**  
**PEDOMAN MANAJEMEN DATA**  
**SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK**

**I. PENDAHULUAN**

Data adalah catatan atas kumpulan fakta atau deskripsi berupa angka, karakter, simbol, gambar, peta, tanda, isyarat, tulisan, suara, dan/atau bunyi, yang merepresentasikan keadaan sebenarnya atau menunjukkan suatu ide, objek, kondisi, atau situasi. Metadata adalah informasi dalam bentuk struktur dan format yang baku untuk menggambarkan data, menjelaskan data, serta memudahkan pencarian, penggunaan, dan pengelolaan informasi data.

Satu Data Indonesia Tingkat Kabupaten Jombang adalah kebijakan tata kelola data pemerintah daerah untuk menghasilkan data yang akurat, mutakhir, terpadu, dan dapat dipertanggungjawabkan, serta mudah diakses dan dibagipakai antar Perangkat Daerah, Badan Usaha Milik Daerah, Instansi Vertikal, Instansi Provinsi dan Instansi Pusat melalui pemenuhan Standar Data, Metadata, Interoperabilitas Data, dan menggunakan Kode Referensi dan Data Induk. Portal Satu Data Indonesia Tingkat Kabupaten Jombang adalah media bagi-pakai data di tingkat pemerintah daerah yang dapat diakses melalui pemanfaatan teknologi informasi dan komunikasi.

Pengaturan Satu Data Indonesia Tingkat Kabupaten Jombang dimaksudkan untuk mengatur penyelenggaraan tata kelola data yang dihasilkan oleh Perangkat Daerah, Badan Usaha Milik Daerah dan Instansi Vertikal untuk mendukung perencanaan, pelaksanaan, evaluasi, dan pengendalian pembangunan. Pengaturan Satu Data Indonesia Tingkat Kabupaten Jombang bertujuan untuk:

1. memberikan acuan pelaksanaan dan pedoman bagi Perangkat 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 dibagi pakaikan antar Perangkat Daerah sebagai dasar perencanaan, pelaksanaan, evaluasi, dan pengendalian pembangunan;
3. mendorong keterbukaan dan transparansi data sehingga tercipta perencanaan dan perumusan kebijakan pembangunan yang berbasis pada data; dan
4. mendukung sistem statistik nasional sesuai Peraturan Perundang-undangan.

**II. DEFINISI**

1. Satu Data Indonesia Tingkat Kabupaten Jombang adalah kebijakan tata kelola data pemerintah daerah untuk menghasilkan data yang akurat, mutakhir, terpadu, dan dapat dipertanggungjawabkan, serta mudah diakses dan dibagipakaikan antar Perangkat Daerah, Badan Usaha Milik Daerah, Instansi Vertikal, Instansi Provinsi dan Instansi Pusat melalui pemenuhan Standar Data, Metadata, Interoperabilitas Data, dan menggunakan Kode Referensi dan Data Induk
2. Data adalah catatan atas kumpulan fakta atau deskripsi berupa angka, karakter, simbol, gambar, peta, tanda, isyarat, tulisan, suara, dan/atau bunyi, yang merepresentasikan keadaan sebenarnya atau menunjukkan suatu ide, objek, kondisi, atau situasi.
3. Data Statistik adalah data berupa angka tentang karakteristik atau ciri khusus suatu populasi yang diperoleh dengan cara pengumpulan, pengolahan, penyajian, dan analisis

4. Statistik Dasar adalah statistik yang pemanfaatannya ditujukan untuk keperluan yang bersifat luas, baik pemerintah maupun masyarakat, yang memiliki ciri-ciri lintas sektoral, berskala nasional maupun regional dan/atau makro
5. Statistik Sektoral adalah statistik yang pemanfaatannya ditujukan untuk memenuhi kebutuhan instansi pemerintah tertentu dalam rangka penyelenggaraan tugas-tugas pemerintah dan tugas pembangunan yang merupakan tugas pokok instansi pemerintah yang bersangkutan
6. Statistik Khusus adalah statistik yang pemanfaatannya ditujukan untuk memenuhi kebutuhan intern dari suatu instansi/perusahaan swasta dalam rangka penyelenggaraan riset atau penelitian.
7. Standar Data adalah standar yang mendasari data tertentu yang meliputi konsep, definisi, cakupan, klasifikasi, ukuran, satuan dan asumsi.
8. Produsen Data adalah Organisasi Perangkat Daerah yang memiliki tugas, fungsi dan kewenangan menurut peraturan perundang-undangan untuk menghasilkan data.
9. Walidata adalah Organisasi Perangkat Daerah yang bertugas menyelenggarakan penyusunan, pengumpulan, dan/atau pengolahan dan penyebarluasan data.
10. Pembina Data adalah Organisasi Perangkat Daerah yang memiliki tugas, fungsi dan kewenangan menurut peraturan perundang-undangan untuk menghasilkan data.
11. Pengguna Data adalah Perangkat Daerah, Badan Usaha Milik Daerah, Instansi Vertikal, Instansi Provinsi. Instansi Pusat perseorangan, kelompok orang, atau badan hukum yang menggunakan data.
12. Metadata adalah informasi dalam bentuk struktur dan format yang baku untuk menggambarkan data, menjelaskan data, serta memudahkan pencarian, penggunaan, dan pengelolaan informasi data.
13. Interoperabilitas & Data adalah kemampuan data untuk dibagipakaikan antar sistem elektronik yang saling berinteraksi.
14. Kode Referensi adalah tanda berisi karakter yang mengandung atau menggambarkan makna, maksud, atau norma tertentu sebagai rujukan identitas data yang bersifat unik.
15. Data Induk adalah data yang merepresentasikan objek dalam proses bisnis pemerintah yang ditetapkan sesuai dengan ketentuan dalam Peraturan Bupati ini untuk digunakan bersama.
16. Forum Satu Data Indonesia Tingkat Kabupaten Jombang adalah wadah komunikasi dan Koordinasi untuk penyelenggaraan Satu Data Indonesia Tingkat Kabupaten Jombang
17. Data Warehouse adalah fasilitas dalam pengelolaan serta pemeliharaan data yang didapatkan dari sistem maupun aplikasi operasional.
18. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan, dan pemulihan data
19. Portal Satu Data Indonesia Tingkat Kabupaten Jombang adalah media bagi-pakai data di tingkat pemerintah daerah yang dapat diakses melalui pemanfaatan teknologi informasi dan komunikasi.

### **III. KEBIJAKAN PENYELENGGARAAN**

Pengaturan Satu Data Indonesia Tingkat Kabupaten Jombang dimaksudkan untuk mengatur penyelenggaraan tata kelola data yang dihasilkan oleh Perangkat Daerah, Badan Usaha Milik Daerah dan Instansi Vertikal untuk mendukung perencanaan, pelaksanaan, evaluasi, dan pengendalian pembangunan. Pengaturan Satu Data Indonesia Tingkat Kabupaten Jombang bertujuan untuk:

1. memberikan acuan pelaksanaan dan pedoman bagi Perangkat 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 dibagi pakaikan antar Perangkat Daerah sebagai dasar perencanaan, pelaksanaan, evaluasi, dan pengendalian pembangunan;
3. mendorong keterbukaan dan transparansi data sehingga tercipta perencanaan dan perumusan kebijakan pembangunan yang berbasis pada data; dan
4. mendukung sistem statistik nasional sesuai Peraturan Perundang-undangan.

#### A. Prinsip Satu Data

Satu Data Indonesia Tingkat Kabupaten Jombang harus dilakukan berdasarkan prinsip sebagai berikut:

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.

Standar Data yang digunakan sebagai ukuran dalam penentuan kualitas data yang dihasilkan oleh Produsen Data terdiri atas:

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

Standar Data lintas Perangkat Daerah mengacu pada Standar Data yang ditetapkan oleh Pembina Data tingkat pusat.

#### B. Metadata

Informasi dalam Metadata harus mengikuti struktur yang baku dan format yang baku. Struktur yang baku merujuk pada bagian informasi tentang data yang harus dicakup dalam Metadata. Format yang baku merujuk pada spesifikasi atau standar teknis dari Metadata. Struktur yang baku dan format yang baku untuk data lintas Perangkat Daerah mengacu pada struktur yang baku dan format yang baku yang ditetapkan oleh Pembina Data tingkat pusat.

#### C. Interoperabilitas Data

Data yang dibuat Untuk memenuhi kaidah Interoperabilitas Data memiliki beberapa kriteria sebagai berikut:

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

#### D. Kode Referensi dan Data Induk

Kode referensi dan/atau data induk mengacu pada Kode referensi dan data induk yang ditetapkan Pembina Data Tingkat Pusat.

#### E. Penyelenggara Satu Data Indonesia

Pengelola Pelaksanaan Sistem Pengelolaan Satu Data dilaksanakan oleh Tim Pengelola Satu Data tingkat daerah dilaksanakan oleh Tim Pengelola Satu Data tingkat Kabupaten Jombang. Tim Pengelola Satu Data Indonesia tingkat Kabupaten Jombang bertugas:

1. melaksanakan komunikasi dan koordinasi dalam pelaksanaan Sistem Pengelolaan Satu Data Indonesia;
2. merumuskan dan menyepakati kebijakan teknis Sistem Pengelolaan Satu Data Indonesia;
3. mengidentifikasi dan mengelola daftar produsen data untuk sistem pengelolaan Satu Data Indonesia, serta menetapkan kewenangan dan tanggung jawab untuk menerbitkan data agar dapat digunakan secara maksimal dan manfaatnya dapat disebarluaskan;
4. merumuskan bahan harmonisasi kebijakan Pemerintah Daerah mengenai pelaksanaan kebijakan Satu Data Indonesia;
5. menyiapkan dan menyampaikan laporan pelaksanaan Pengelolaan Satu Data Indonesia tingkat daerah secara berkala kepada Kabupaten Jombang.

Tim Pengelola Satu Data Indonesia tingkat Kabupaten Jombang dalam melaksanakan tugasnya terdiri dari:

1. Pembina Data

Pembina Data terdiri dari BAPPEDA, Badan Pusat Statistik Daerah sebagai Pembina Data Statistik dan Pembina Data Geospasial yaitu salah satu Perangkat Daerah yang diberikan penugasan sebagai Pengelola Simpul Jaringan Pemerintah Daerah dalam jaringan Informasi Geospasial Nasional. Pembina Data mempunyai tugas memberikan rekomendasi dalam proses perencanaan pengumpulan data dan melakukan pembinaan penyelenggaraan Satu Data Indonesia Tingkat Kabupaten Jombang sesuai dengan ketentuan peraturan perundang-undangan. Pembina Data memiliki tugas sebagai berikut:

- a) memastikan pelaksanaan Sistem Pengelolaan Satu Data daerah tingkat Kabupaten Jombang sebagaimana disebutkan pada Peraturan Bupati Jombang ini sesuai dengan Peraturan Perundang-undangan
- b) bersama dengan Produsen Data dan Walidata, menentukan standar data dan format metadata;
- c) membakukan standar data dan format metadata termasuk menetapkan norma, standar, prosedur, dan kriteria yang dapat menjadi rujukan;
- d) melakukan koordinasi mengenai penyelenggaraan data yang menjadi kebutuhan internal Produsen Data dengan Walidata untuk mencegah duplikasi data;
- e) memeriksa, mengharmonisasikan, merekomendasikan Kode Referensi kepada walidata dan kode referensi lintar produsen data.

2. Walidata

Walidata adalah Kepala DISKOMINFO. Walidata memiliki tugas sebagai berikut:

- a) menyusun standar data dan format metadata, dan daftar istilah disusun untuk data yang disusun, dikumpulkan dan diolah oleh Produsen Data melalui koordinasi bersama Pembina Data;
- b) pengumpulan, pengolahan, verifikasi dan validasi, diseminasi serta analisis data;
- c) menerima dan menghimpun data yang disampaikan oleh Produsen Data;
- d) memastikan metadata melekat pada data yang disampaikan oleh Produsen Data;
- e) memastikan metadata yang melekat pada data sesuai dengan

- format yang dibakukan oleh Pembina Data;
- f) memastikan data yang disampaikan oleh Produsen Data sesuai dengan Format yang dibakukan oleh Pembina Data;
  - g) memastikan data yang dihasilkan oleh pihak non pemerintah, baik yang menggunakan Anggaran Pendapatan dan Belanja Negara atau Anggaran Pendapatan dan Belanja Daerah sesuai dengan ketentuan Interoperabilitas Data;
  - h) melakukan koordinasi mengenai penyelenggaraan data yang menjadi kebutuhan internal Produsen Data dengan Pembina data, Walidata di Produsen Data lain, dan pihak non pemerintah;
  - i) memperhatikan kebutuhan Data Produsen Data lain dan masyarakat dan merekomendasikan penyusunan, pengumpulan dan pengolahan data tersebut kepada Produsen Data;
  - j) merencanakan penanganan dan penyimpanan data untuk memastikan pengelolaan dan pemeliharaan data, sehingga investasi terhadap data dan manfaatnya dapat diperoleh secara maksimal untuk kepentingan pembangunan kota dan masyarakatnya.
3. Walidata Pendukung
- Walidata Pendukung terdiri atas:
- a) Walidata Pendukung Teknis;
  - b) Walidata Pendukung Verifikator Prinsip Satu Data; dan
  - c) Walidata Pendukung Validator konten.
- Walidata Pendukung memiliki tugas sebagai berikut:
- a) memeriksa kesesuaian data yang disampaikan oleh Produsen Data sesuai dengan prinsip Satu Data Indonesia Tingkat Kabupaten Jombang;
  - b) menyebarluaskan data dan Metadata di portal Satu Data Indonesia, portal Satu Data Indonesia Tingkat Kabupaten Jombang, dan media lainnya sesuai dengan ketentuan peraturan perundang-undangan dan perkembangan ilmu pengetahuan dan teknologi; dan
  - c) membantu Pembina Data dalam membina Produsen Data;
4. Produsen Data
- Produsen Data adalah Perangkat Daerah, Badan Usaha Milik Daerah dan Instansi Vertikal di lingkup Pemerintah Kabupaten Jombang. Produsen Data memiliki tugas sebagai berikut:
- a) menyusun, mengumpulkan, dan mengolah data termasuk data yang bersumber dari pihak non pemerintah sesuai dengan standar data, dan ketentuan interoperabilitas data;
  - b) menetapkan status klasifikasi data pada saat proses pengumpulan;
  - c) mengaji kesesuaian data yang diperoleh berdasarkan kriteria yang telah ditentukan, meliputi skala, resolusi, reliabilitas, akurasi, klasifikasi dan integritas;
  - d) menyampaikan data kepada Walidata beserta metadata yang melekat pada data tersebut secara periodik dan berkala sesuai dengan kebutuhan;
  - e) memberikan masukan kepada Walidata terkait pelaksanaan kebijakan Sistem Pengelolaan Satu Data; dan
  - f) memastikan terjaganya hak intelektual dan hak cipta data, terutama data yang diperoleh dari pihak eksternal dan menindaklanjuti rekomendasi dari Walidata atas kebutuhan
  - g) memberikan masukan kepada Pembina Data mengenai Standar Data, Metadata, dan Interoperabilitas Data;
  - h) menghasilkan Data sesuai dengan prinsip Satu Data Indonesia Tingkat Kabupaten Jombang; dan
  - i) menyampaikan data beserta Metadata kepada Walidata

#### **IV. STANDAR PENYELENGGARAAN**

##### **A. Forum Satu Data Indonesia Tingkat Kabupaten Jombang**

Pembina Data, Walidata, dan Walidata Pendukung berkomunikasi dan berkoordinasi secara berkala melalui Forum Satu Data Indonesia Tingkat Kabupaten Jombang yang dikoordinasikan oleh Kepala Badan yang menyelenggarakan fungsi penunjang urusan pemerintahan bidang perencanaan. Koordinator Forum Satu Data Indonesia Tingkat Kabupaten Jombang melaporkan hasil pemantauan dan evaluasi kepada Bupati paling sedikit 1 (satu) kali dalam 1 (satu) tahun. Forum Satu Data Indonesia Tingkat Kabupaten Jombang dalam pelaksanaan tugasnya dapat menyertakan Produsen Data dan/atau pihak lain yang terkait, termasuk selain pemerintah. Forum Satu Data Indonesia Tingkat Kabupaten Jombang berkomunikasi dan berkoordinasi dalam penyelenggaraan Satu Data Indonesia Tingkat Kabupaten Jombang mengenai beberapa hal antara lain:

1. penentuan daftar data dalam yang akan dikumpulkan pada tahun selanjutnya;
2. penentuan data yang akan disimpan dalam data. warehouse;
3. lokasi pusat data daerah;
4. pembatasan akses data yang diusulkan oleh Produsen Data dan Walidata penyebarluasan data membahas pembatasan akses data;
5. praktik tata kelola penyelenggaraan Satu Data Indonesia Tingkat Kabupaten Jombang;
6. penentuan waktu pelaksanaan rapat Forum Satu Data Indonesia Tingkat Kabupaten Jombang secara teratur, dan
7. pemantauan dan evaluasi penyelenggaraan Satu Data Indonesia Tingkat Kabupaten Jombang secara berkala dalam rangka pencapaian perencanaan Satu Data Indonesia Tingkat Kabupaten Jombang.

##### **B. Sekretariat Satu Data Indonesia Tingkat Kabupaten Jombang**

Forum Satu Data Indonesia Tingkat Kabupaten Jombang dalam pelaksanaan tugasnya dibantu oleh Sekretariat Satu Data Indonesia Tingkat Kabupaten Jombang. Sekretariat Satu Data Indonesia Tingkat Kabupaten Jombang bersifat *ex-officio*, yang secara fungsional dilaksanakan oleh Badan Perencanaan Pembangunan Daerah (BAPPEDA) yang menyelenggarakan fungsi penunjang urusan pemerintahan bidang perencanaan dalam pelaksanaan tugasnya dapat merekrut tenaga ahli perseorangan, institusi, dan/atau badan usaha. Sekretariat Satu Data Indonesia tingkat Kabupaten Jombang memiliki tugas sebagai berikut:

1. memberikan dukungan dan pelayanan teknis operasional dan administratif kepada Forum Satu Data Indonesia tingkat Kabupaten Jombang;
2. melaksanakan tugas lain yang diberikan oleh Forum Satu Data Indonesia Tingkat Kabupaten Jombang
3. mengelola Portal Data

##### **C. Perencanaan Data**

Forum Satu Data Indonesia Tingkat Kabupaten Jombang dan/atau atas rekomendasi Pembina Data melaksanakan perencanaan data berupa penentuan daftar data yang akan dikumpulkan di tahun selanjutnya. Daftar data mengacu pada daftar data yang ditentukan oleh instansi pusat. Penentuan daftar data yang akan dikumpulkan di tahun selanjutnya dilakukan dengan menghindari duplikasi. Penentuan daftar data dilakukan berdasarkan:

1. arsitektur Sistem Pemerintahan Berbasis Elektronik Pemerintah Daerah;
2. kesepakatan Forum Satu Data Indonesia Tingkat Kabupaten Jombang; dan/atau
3. rekomendasi Pembina Data.

Daftar data yang akan dikumpulkan memuat Produsen Data untuk masing-masing data dan jadwal rilis dan/atau pemutakhiran data. Daftar data yang akan dikumpulkan dapat digunakan sebagai dasar dalam perencanaan dan penganggaran bagi Perangkat Daerah. Daftar data dikomunikasikan oleh Forum Satu Data Indonesia Tingkat Kabupaten Jombang kepada seluruh anggota Penyelenggara Satu Data Indonesia Tingkat Kabupaten Jombang.

#### D. Pengumpulan Data

Data yang dikumpulkan oleh Produsen Data disertai dengan Metadata. Produsen Data menyampaikan Data yang telah dikumpulkan kepada Walidata. Walidata menginformasikan Data yang telah diterima kepada Walidata Pendukung Verifikator Prinsip Satu Data Indonesia Tingkat Kabupaten Jombang dan Validator Konten. Produsen Data melakukan pengumpulan data sesuai dengan berdasarkan beberapa ketentuan sebagai berikut:

1. Standar Data;
2. daftar data yang telah ditentukan dalam Forum Satu Data Indonesia Tingkat Kabupaten Jombang; dan
3. jadwal pemutakhiran data atau rilis data.

#### E. Pemeriksaan Data

Walidata dengan dibantu oleh Walidata Pendukung Verifikator prinsip Satu Data memeriksa kesesuaian Data yang dihasilkan oleh Produsen Data dengan prinsip Satu Data Indonesia Tingkat Kabupaten Jombang. Walidata dibantu oleh Walidata Pendukung Validator Konten memeriksa keakuratan konten data yang dihasilkan oleh Produsen Data. Apabila Data yang disampaikan oleh Produsen Data belum sesuai dengan prinsip Satu Data Indonesia Tingkat Kabupaten Jombang, Walidata mengembalikan data tersebut kepada Produsen Data. Produsen Data dapat memperbaiki data sesuai hasil pemeriksaan.

#### F. Penyimpanan Data

Walidata dengan dibantu oleh Walidata Pendukung Teknis menyimpan Data yang telah memenuhi prinsip Satu Data Indonesia Tingkat Kabupaten Jombang ke dalam Data Warehouse yang tersimpan di pusat data Daerah. Data yang disimpan dalam Data Warehouse dibahas dalam Forum Satu Data Indonesia Tingkat Kabupaten Jombang. Data yang disimpan berupa satuan-satuan data yang terintegrasi. Data yang disimpan dalam Data Warehouse menjadi referensi dalam penentuan kecerdasan bisnis dalam mengambil keputusan

#### G. Penyebarluasan Data

Walidata melaksanakan penyebarluasan data dibantu Walidata Pendukung Teknis menyebarluaskan membutuhkan integrasi data. Penyebarluasan Data merupakan kegiatan pemberian akses, pendistribusian, dan pertukaran data. Hasil penyebarluasan data dikomunikasikan oleh Walidata ke seluruh anggota penyelenggara Satu Data Indonesia Tingkat Kabupaten Jombang. Penyebarluasan data dilakukan melalui Portal Satu Data Indonesia, Portal Satu Data Indonesia Tingkat Kabupaten Jombang, dan media lainnya sesuai dengan ketentuan peraturan perundang-undangan dan perkembangan ilmu pengetahuan dan teknologi.

Pemerintah Daerah menyediakan akses data kepada Pengguna Data melalui Portal Satu Data Indonesia Tingkat Kabupaten Jombang.

Produser Data dan Walidata dapat mengajukan pembahasan pembatasan akses data tertentu kepada Forum Satu Data Indonesia Tingkat Kabupaten Jombang dengan hasil yang disampaikan kepada Bupati. Portal Satu Data Indonesia Tingkat Kabupaten Jombang yang dikelola oleh Walidata dengan menyediakan beberapa akses antara lain:

1. Kode Referensi;
2. Data Induk;
3. Data;
4. Metadata;
5. Data Prioritas; dan
6. jadwal rilis dan/atau pemutakhiran Data.

#### H. Partisipasi Pihak Lain

Pemerintah Daerah dapat bekerjasama dengan 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 yang wilayah kerjanya berada di Kabupaten Jombang. Kerjasama dengan lembaga negara dan badan hukum publik tidak mengurangi wewenang dan independensi tugas dan fungsi masing-masing pihak sesuai dengan ketentuan peraturan perundang-undangan. Masyarakat dari kalangan manapun yang tidak terkecuali dapat berpartisipasi dalam pengawasan dan pengumpulan data Satu Data Indonesia Tingkat Kabupaten Jombang. Pelaku usaha yang meliputi Swasta, BUMN, Wiraswasta, dan lainnya dapat berpartisipasi dalam pengawasan dan pengumpulan data Satu Data Indonesia Tingkat Kabupaten Jombang.

**BAB IV**  
**PEDOMAN MANAJEMEN ASET TEKNOLOGI INFORMASI DAN**  
**KOMUNIKASI**  
**SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK**

**I. PENDAHULUAN**

Kebijakan akuntansi merupakan instrumen penting dalam penerapan akuntansi akrual. Dokumen yang ditetapkan dalam peraturan kepala daerah ini harus dipedomani dengan baik oleh fungsi-fungsi akuntansi, baik di SKPKD maupun di SKPD. Selain itu, dokumen ini juga seyogyanya dipedomani oleh pihak-pihak lain seperti perencana dan tim anggaran pemerintah daerah. Memperhatikan sifatnya yang strategis, penyusunan kebijakan akuntansi harus menjadi perhatian semua pihak. Dalam pembahasannya, perlu dijelaskan setiap dampak dari metode yang dipilih, baik pada proses penganggaran, penatausahaan maupun pelaporan. Dengan demikian, kebijakan akuntansi yang dihasilkan menjadi operasional serta dapat diantisipasi implementasinya.

Praktek selama ini menunjukkan banyak kebijakan akuntansi disusun dengan menuliskan kembali hampir seluruh isi standar akuntansi pemerintahan. Praktek seperti ini menimbulkan inefisiensi karena adanya pengulangan (redundancy) antara SAP yang diatur oleh peraturan pemerintah dan kebijakan akuntansi yang diatur oleh peraturan kepala daerah. Oleh karena itu Peraturan Bupati Jombang Nomor 80 Tahun 2020 mengatur kebijakan akuntansi pemerintah daerah mengambil unsur-unsur pokok dari SAP, lalu mengatur perlakuan akuntansi untuk aset tetap meliputi definisi, pengakuan, klasifikasi, pengukuran, penyajian dan pengungkapan aset tetap.

**II. DEFINISI**

1. Aset tetap adalah aset berwujud yang mempunyai masa manfaat lebih dari 12 (dua belas) bulan untuk digunakan, atau dimaksudkan untuk digunakan dalam kegiatan pemerintah daerah atau dimanfaatkan oleh masyarakat umum.
2. Biaya perolehan adalah jumlah kas atau setara kas yang telah dan yang masih wajib dibayarkan atau nilai wajar imbalan lain yang telah dan yang masih wajib diberikan untuk memperoleh suatu aset pada saat perolehan atau konstruksi sampai dengan aset tersebut dalam kondisi dan tempat yang siap untuk dipergunakan.
3. Masa manfaat adalah: a. Periode suatu aset diharapkan digunakan untuk aktivitas pemerintahan dan/atau pelayanan publik; atau b. Jumlah produksi atau unit serupa yang diharapkan diperoleh dari aset untuk aktivitas pemerintahan dan/atau pelayanan publik.
4. Penambahan Masa Manfaat adalah bertambahnya tahun/waktu pemanfaatan aset tetap dalam periode aset diharapkan dapat dimanfaatkan/difungsikan/digunakan karena adanya rehabilitasi sedang/berat.
5. Nilai sisa aset adalah jumlah netto yang diharapkan dapat diperoleh pada akhir masa manfaat suatu aset setelah dikurangi taksiran biaya pelepasan.
6. Nilai tercatat (carrying amount) aset adalah nilai buku aset tetap, yang dihitung dari biaya perolehan suatu aset setelah dikurangi akumulasi penyusutan.
7. Nilai wajar adalah nilai tukar aset tetap atau penyelesaian kewajiban antar pihak yang memahami dan berkeinginan untuk melakukan transaksi wajar.
8. Penyusutan adalah alokasi yang sistematis atas nilai suatu aset tetap yang dapat disusutkan (depreciable assets) selama masa manfaat aset

yang bersangkutan.

9. Akumulasi Penyusutan adalah pos di neraca yang mengurangi nilai dari aset tetap.
10. Kapitalisasi adalah penentuan nilai pembukuan terhadap semua belanja untuk memperoleh aset tetap hingga siap pakai, untuk meningkatkan kapasitas/efisiensi, dan atau memperpanjang umur teknisnya dalam rangka menambah nilai-nilai aset tersebut.
11. Nilai Satuan Minimum Kapitalisasi Aset Tetap adalah pengeluaran pengadaan baru atau penambahan nilai aset tetap dari hasil pengembangan, reklasifikasi, renovasi, perbaikan atau restorasi.
12. Hibah atau donasi adalah perolehan atau penyerahan aset tetap dari atau kepada pihak ketiga tanpa memberikan imbalan.
13. Pemeliharaan adalah kegiatan atau tindakan yang dilakukan agar semua aset/barang milik daerah selalu dalam keadaan baik dan siap untuk digunakan secara berdaya guna dan berhasil guna.
14. Rehabilitasi ringan adalah perbaikan aset tetap yang rusak sebagian dengan tanpa meningkatkan kualitas dan atau kapasitas dengan maksud dapat digunakan sesuai dengan kondisi semula, termasuk belanja barang yang direncanakan untuk penggantian komponen aset tetap yang tercatat dalam bentuk satuan set/unit, misalnya pengadaan keyboard, mouse, motherboard yang direncanakan untuk mengganti salah satu komponen komputer yang telah tercatat dalam satuan set/unit.
15. Restorasi adalah perbaikan aset tetap yang rusak dengan tetap mempertahankan arsitekturnya.
16. Renovasi adalah bagian kegiatan pemeliharaan yang berupa penggantian aset tetap dengan meningkatkan umur/masa manfaat, kapasitas, mutu produksi dan standar kinerja sehingga menambah nilai aset.
17. Overhaul adalah kegiatan penambahan, perbaikan, dan/atau penggantian bagian peralatan mesin dengan maksud meningkatkan masa manfaat, serta mempertahankan dan/atau meningkatkan kualitas dan/atau kapasitas.
18. Reklasifikasi adalah perubahan Aset Tetap dari pencatatan dalam pembukuan karena perubahan klasifikasi.
19. Overlay adalah perbaikan permukaan dengan menggunakan Lapisan Aspal dengan ketebalan tertentu seperti ATB (Asphalt Treated Base) atau Asphalt Concrete (AC).
20. Aset Tetap-Renovasi adalah biaya renovasi atas aset tetap yang bukan miliknya dan biaya partisi suatu ruangan kantor yang bukan miliknya.
21. Pencatatan di luar pembukuan (Ekstrakomptabel) adalah penatausahaan Aset Tetap untuk nilai Aset Tetap di bawah nilai minimal kapitalisasi atau Aset Tetap yang karena sifatnya, tidak perlu dilaporkan dalam Laporan Barang Milik Daerah.
22. Konstruksi dalam pengerjaan adalah aset-aset tetap yang sedang dalam proses pembangunan.
23. Kontrak Konstruksi adalah perikatan yang dilakukan secara khusus untuk konstruksi suatu aset atau suatu kombinasi yang berhubungan erat satu sama lain atau saling tergantung dalam hal rancangan, teknologi dan fungsi atau tujuan atau penggunaan utama.
24. Kontraktor adalah suatu entitas yang mengadakan kontrak untuk membangun aset atau memberikan jasa konstruksi untuk kepentingan entitas lain sesuai dengan spesifikasi yang ditetapkan dalam kontrak konstruksi.
25. Uang Muka Kerja adalah jumlah yang diterima oleh kontraktor sebelum pekerjaan dilakukan dalam rangka kontrak konstruksi.
26. Klaim adalah jumlah yang diminta kontraktor kepada pemberi kerja sebagai penggantian biaya-biaya yang tidak termasuk dalam nilai kontrak.
27. Pemberi Kerja adalah entitas yang mengadakan kontrak konstruksi



dengan pihak ketiga untuk membangun atau memberikan jasa konstruksi.

28. Retensi adalah jumlah termin (progress billing) yang belum dibayar hingga pemenuhan kondisi yang ditentukan dalam kontrak untuk pembayaran jumlah tersebut.
29. Termin (Progress Billing) adalah jumlah yang ditagih untuk pekerjaan yang dilakukan dalam suatu kontrak baik yang telah dibayar ataupun yang belum dibayar oleh pemberi kerja.

### III. KEBIJAKAN PENYELENGGARAAN

#### A. Klasifikasi

1. Aset tetap diklasifikasikan berdasarkan kesamaan dalam sifat atau fungsinya dalam aktivitas operasi entitas. Klasifikasi aset tetap adalah sebagai berikut:

- a) Tanah

Sesuai dengan sifat dan peruntukannya, tanah dapat diklasifikasikan lebih lanjut menjadi dua kelompok besar, yaitu

- 1) tanah untuk gedung dan bangunan, dan
- 2) tanah untuk bukan gedung dan bangunan, seperti tanah untuk jalan, irigasi, jaringan, tanah lapangan, tanah hutan, tanah untuk pertanian, dan tanah untuk perkebunan.

- b) Peralatan dan Mesin

Peralatan dan Mesin dapat diklasifikasikan sesuai dengan jenisnya, seperti alat perkantoran, komputer, alat angkutan (darat, air dan udara), alat komunikasi, alat kedokteran, alat-alat berat, alat bengkel, alat olahraga dan rambu-rambu.

- c) Gedung dan Bangunan

- 1) Gedung dan bangunan mencakup seluruh gedung dan bangunan yang diperoleh dengan maksud untuk dipakai dalam kegiatan operasional pemerintah dan dalam kondisi siap dipakai. Gedung dan Bangunan dapat diklasifikasikan menurut jenisnya, seperti gedung perkantoran, rumah dinas, bangunan tempat ibadah, bangunan menara, monumen/bangunan bersejarah, gudang, gedung museum, dan rambu-rambu. Termasuk dalam jenis gedung dan bangunan ini adalah taman yang melekat pada gedung dan semua jenis pagar.

- 2) Gedung bertingkat pada dasarnya terdiri dari komponen bangunan fisik, komponen penunjang utama yang berupa mechanical engineering (lift, instalasi listrik beserta generator, dan sarana pendingin Air Conditioning), dan komponen penunjang lain yang antara lain berupa saluran air dan telepon. Masing-masing komponen mempunyai masa manfaat yang berbeda, sehingga umur penyusutannya berbeda, serta memerlukan pola pemeliharaan yang berbeda pula. Perbedaan masa manfaat dan pola pemeliharaan menyebabkan diperlukannya sub-akun pencatatan yang berbeda untuk masing-masing komponen gedung bertingkat, misalnya untuk Gedung terdiri dari Bangunan Fisik, Taman, Jalan dan Tempat Parkir, Pagar Instalasi AC, Instalasi Listrik dan Generator, Lift, Penyediaan Air, Saluran Air Bersih dan Air Limbah, Saluran Telepon.

- d) Jalan, Irigasi dan Jaringan

Jalan, irigasi dan jaringan mencakup jalan, irigasi, dan jaringan yang dibangun oleh pemerintah daerah serta dimiliki dan/atau dikuasai oleh pemerintah daerah dan dalam kondisi siap dipakai. Aset ini mempunyai karakteristik sebagai berikut:

- 1) Merupakan bagian dari satu sistem atau jaringan;

- 2) Sifatnya khusus dan tidak ada alternatif lain penggunaannya;
- 3) Tidak dapat dipindah-pindahkan; dan
- 4) Terdapat batasan-batasan untuk pelepasannya.

Aset tetap ini dapat diklasifikasikan lebih lanjut menjadi misalnya jalan, jembatan, waduk, saluran irigasi, instalasi distribusi air, instalasi pembangkit listrik, instalasi distribusi listrik, saluran transmisi gas, instalasi distribusi gas, jaringan telepon dan sebagainya.

e) Aset Tetap Lainnya

Aset tetap lainnya mencakup aset tetap yang tidak dapat dikelompokkan ke dalam kelompok aset tetap di atas, yang diperoleh dan dimanfaatkan untuk kegiatan operasional pemerintah daerah dan dalam kondisi siap dipakai.

Aset yang termasuk dalam klasifikasi Aset Tetap Lainnya adalah Koleksi perpustakaan/buku dan non buku, barang bercorak kesenian/kebudayaan/olah raga, hewan, ikan dan tanaman. Termasuk dalam kategori Aset Tetap Lainnya adalah Aset Tetap-Renovasi, yaitu biaya renovasi atas aset tetap yang bukan miliknya, dan biaya partisi suatu ruangan kantor yang bukan miliknya.

f) Konstruksi Dalam Pengerjaan

Konstruksi dalam pengerjaan mencakup aset tetap yang sedang dalam proses pembangunan namun pada tanggal laporan keuangan belum selesai seluruhnya. Konstruksi Dalam Pengerjaan biasanya merupakan aset yang dimaksudkan digunakan untuk operasional pemerin daera atau dimanfaatkan oleh masyarakat dalam jangka panjang dan oleh karenanya diklasifikasikan dalam aset tetap. Konstruksi Dalam Pengerjaan ini apabila telah selesai dibangun dan sudah diserahterimakan akan direklasifikasi menjadi aset tetap sesuai dengan kelompok asetnya.

2. Pengadaan aset tetap yang ditujukan untuk diserahkan kepada masyarakat dalam rangka kegiatan pemerintahan diklasifikasikan sebagai persediaan.
3. Aset tetap yang tidak digunakan untuk keperluan operasional pemerintah tidak memenuhi definisi aset tetap dan harus disajikan di pos aset lainnya sesuai dengan nilai tercatatnya.

4. Aset Lainnya

Aset lainnya digunakan untuk mencatat aset lainnya yang tidak dapat dikelompokkan ke dalam aset tetap meliputi Aset Kondisi Rusak Berat, Aset yang dimanfaatkan Pihak Lain dan Aset Tidak Berwujud.

a) Aset Kondisi Rusak Berat diklasifikasikan berdasarkan kriteria :

- 1) Barang Bergerak Apabila kondisi barang tersebut tidak utuh dan tidak berfungsi lagi atau memerlukan perbaikan besar/penggantian bagian utama/komponen pokok, sehingga tidak ekonomis untuk diadakan perbaikan/rehabilitasi.

2) Barang Tidak Bergerak, diklasifikasikan :

(a) Tanah

Apabila kondisi tanah tersebut tidak dapat lagi dipergunakan dan/atau dimanfaatkan sesuai dengan peruntukannya karena adanya bencana alam, erosi dan sebagainya.

(b) Jalan dan Jembatan

Apabila kondisi fisik barang tersebut dalam keadaan tidak utuh/tidak berfungsi dengan baik dan memerlukan perbaikan dengan biaya besar.

(c) Bangunan

Apabila bangunan tersebut tidak utuh dan tidak dapat dipergunakan lagi. Aset Kondisi Rusak Berat selanjutnya akan dihentikan dari penggunaan aktif pemerintah daerah dan berdasarkan surat pernyataan dari pengguna barang akan dipindahkan ke pos aset lainnya sesuai dengan nilai tercatatnya. Aset tetap rusak berat yang diusulkan penghapusan tetapi belum ada Keputusan Kepala Daerah juga dimasukkan dalam Aset lainnya.

- b) Aset Yang Dimanfaatkan Pihak Lain  
merupakan aset tetap yang dibangun atau digunakan untuk menyelenggarakan kegiatan kerjasama/kemitraan.
- c) Aset Tidak Berwujud  
merupakan aset-aset non keuangan yang dapat diidentifikasi dan tidak mempunyai wujud fisik serta dimiliki untuk digunakan dalam menghasilkan barang atau jasa atau digunakan untuk tujuan lainnya termasuk hak atas kekayaan intelektual.

## B. Pengakuan

1. Aset tetap diakui pada saat manfaat ekonomi masa depan dapat diperoleh dan nilainya dapat diukur dengan handal. Pengakuan aset tetap sangat andal bila aset tetap telah diterima atau diserahkan hak kepemilikannya dan/atau pada saat penguasaannya berpindah.
2. Apabila perolehan aset tetap belum didukung dengan bukti secara hukum dikarenakan masih adanya suatu proses administrasi yang diharuskan, seperti pembelian tanah yang masih harus diselesaikan proses jual beli (akta) dan sertifikat kepemilikannya di instansi berwenang, maka aset tetap tersebut harus diakui pada saat terdapat bukti bahwa penguasaan atas aset tetap tersebut telah berpindah, misalnya telah terjadi pembayaran dan penguasaan atas sertifikat tanah atas nama pemilik sebelumnya.
3. Untuk dapat diakui sebagai aset tetap harus dipenuhi kriteria sebagai berikut:
  - a) berwujud;
  - b) mempunyai masa manfaat lebih dari 12 (dua belas) bulan;
  - c) biaya perolehan aset dapat diukur secara andal;
  - d) tidak dimaksudkan untuk dijual dalam operasi normal entitas; dan
  - e) diperoleh atau dibangun dengan maksud untuk digunakan;
 Nilai Rupiah pembelian barang material atau pengeluaran untuk pembelian barang tersebut memenuhi batasan minimal kapitalisasi aset tetap yang telah ditetapkan.
4. Dalam hal tanah belum ada bukti kepemilikan yang sah, namun dikuasai dan/atau digunakan oleh pemerintah, maka tanah tersebut tetap harus dicatat dan disajikan sebagai aset tetap tanah pada neraca pemerintah, serta diungkapkan secara memadai dalam Catatan atas Laporan Keuangan.
5. Dalam hal tanah dimiliki oleh pemerintah, namun dikuasai dan/atau digunakan oleh pihak lain, maka tanah tersebut tetap harus dicatat dan disajikan sebagai aset tetap tanah pada neraca pemerintah, serta diungkapkan secara memadai dalam Catatan atas Laporan Keuangan, bahwa tanah tersebut dikuasai atau digunakan oleh pihak lain.
6. Dalam hal tanah dimiliki oleh suatu entitas pemerintah, namun dikuasai dan/atau digunakan oleh entitas pemerintah yang lain, maka tanah tersebut dicatat dan disajikan pada neraca entitas pemerintah yang mempunyai bukti kepemilikan, serta diungkapkan secara memadai dalam Catatan atas Laporan Keuangan. Entitas pemerintah yang menguasai dan/atau menggunakan tanah cukup

mengungkapkan tanah tersebut secara memadai dalam Catatan atas Laporan Keuangan.

7. Perlakuan tanah yang masih dalam sengketa atau proses pengadilan:
  - a) Dalam hal belum ada bukti kepemilikan tanah yang sah, tanah tersebut dikuasai dan/atau digunakan oleh pemerintah;
  - b) Dalam hal pemerintah belum mempunyai bukti kepemilikan tanah yang sah, tanah tersebut dikuasai dan/atau digunakan oleh pihak lain;
  - c) Dalam hal bukti kepemilikan tanah ganda, namun tanah tersebut dikuasai dan/atau digunakan oleh pemerintah;
  - d) Dalam hal bukti kepemilikan tanah ganda, namun tanah tersebut dikuasai dan/atau digunakan oleh pihak lain;
 maka tanah tersebut tetap harus dicatat dan disajikan sebagai aset tetap tanah pada neraca pemerintah, serta diungkapkan secara memadai dalam Catatan atas Laporan Keuangan.
8. Pengakuan biaya renovasi atas aset tetap yang bukan milik adalah sebagai berikut:
  - a) Apabila renovasi aset tetap tersebut meningkatkan manfaat ekonomi dan sosial aset tetap misalnya perubahan fungsi gedung dari gudang menjadi ruangan kerja dan kapasitasnya naik, maka renovasi tersebut dikapitalisasi sebagai Aset Tetap-Renovasi.
  - b) Apabila manfaat ekonomi renovasi tersebut lebih dari satu tahun buku, maka biaya renovasi dikapitalisasi sebagai Aset Tetap-Renovasi.
  - c) Apabila jumlah nilai moneter biaya renovasi tersebut material dan memenuhi syarat maka pengeluaran tersebut dikapitalisasi sebagai Aset Tetap-Renovasi

#### **IV. STANDAR PENYELENGGARAAN**

##### **A. Pengukuran Aset Tetap**

##### **1. Biaya Perolehan**

- a) Aset tetap dinilai dengan biaya perolehan, apabila penilaian aset tetap dengan menggunakan biaya perolehan tidak memungkinkan maka nilai aset tetap didasarkan pada nilai wajar pada saat perolehan.
- b) Bila aset tetap diperoleh dengan tanpa nilai, biaya aset tersebut adalah sebesar nilai wajar pada saat aset tersebut diperoleh. Penggunaan nilai wajar tersebut bukan merupakan suatu proses penilaian kembali (revaluasi) dan tetap konsisten dengan biaya perolehan. Penilaian kembali yang dimaksud hanya diterapkan pada penilaian untuk periode pelaporan selanjutnya, bukan pada saat perolehan awal.
- c) Biaya perolehan adalah jumlah kas atau setara kas yang dibayarkan atau nilai wajar imbalan lain yang diberikan untuk memperoleh suatu aset pada saat perolehan atau konstruksi sampai dengan aset tersebut dalam keadaan kondisi dan tempat yang siap untuk dipergunakan.
- d) Biaya perolehan suatu aset tetap berdiri dari harga belinya atau konstruksinya, termasuk bea impor dan setiap biaya yang dapat didistribusikan/atribusi secara langsung dalam membawa aset tersebut ke kondisi yang membuat aset tersebut dapat bekerja untuk penggunaan yang dimaksudkan yang dikelompokkan berdasarkan jenis aset tetap sesuai dengan tabel pada Peraturan Bupati Jombang Nomor 80 Tahun 2020 berikut:

Tabel Komponen Biaya Perolehan Berdasarkan Jenis Aset Tetap

<b>Jenis</b>	<b>Komponen Biaya Perolehan</b>
--------------	---------------------------------

<b>Aset Tetap</b>	
Tanah	<p>Harga perolehan atau biaya pembebasan tanah, biaya yang dikeluarkan dalam rangka memperoleh hak, biaya pematangan, pengukuran atau penimbunan, dan biaya lainnya yang dikeluarkan maupun yang masih harus dikeluarkan sampai tanah tersebut siap pakai. Nilai tanah juga meliputi nilai bangunan tua yang terletak pada tanah yang dibeli tersebut jika bangunan tua tersebut dimaksudkan untuk dimusnahkan. Apabila perolehan tanah pemerintah dilakukan oleh panitia pengadaan, maka termasuk dalam harga perolehan tanah adalah honor panitia pengadaan/pembebasan tanah dan belanja perjalanan dinas dalam rangka perolehan tanah tersebut. Biaya yang terkait dengan peningkatan bukti kepemilikan tanah, misalnya dari status tanah girik menjadi sertifikat hak pengelolaan dikapitalisasi sebagai biaya perolehan tanah. Biaya yang timbul atas penyelesaian sengketa tanah, seperti biaya pengadilan dan pengacara tidak dikapitalisasi sebagai biaya perolehan tanah.</p>
Peralatan dan Mesin	<p>Harga pembelian, biaya pengangkutan, biaya instalasi, honorarium serta biaya langsung lainnya untuk memperoleh dan mempersiapkan sampai peralatan dan mesin tersebut siap digunakan</p>
Gedung dan bangunan	<p>Harga pembelian atau biaya konstruksi, termasuk biaya pengurusan IMB, notaris, honorarium dan pajak serta biaya langsung lainnya untuk memperoleh dan mempersiapkan sampai gedung dan bangunan tersebut siap digunakan. Jika tidak memungkinkan maka nilai aset didasarkan pada nilai wajar/taksiran pada saat aset tetap diperoleh. Apabila dibangun dengan cara kontrak maka nilai perolehan termasuk nilai kontrak, biaya perencanaan, biaya pengawasan, biaya konsultan dan biaya perijinan. Gedung dan bangunan yang diperoleh dari sumbangan (donasi) dicatat sebesar nilai wajar pada saat perolehan.</p>
Jalan, Irigasi dan Jaringan	<p>Harga perolehan atau biaya konstruksi, honorarium dan biaya lain yang dikeluarkan sampai jalan, irigasi dan jaringan tersebut siap pakai. Biaya perolehan untuk jalan, irigasi dan jaringan yang diperoleh melalui kontrak meliputi biaya perencanaan dan pengawasan, biaya perizinan, jasa konsultan, biaya pengosongan, pajak, kontrak konstruksi, dan pembongkaran. Jalan, Irigasi dan Jaringan yang diperoleh dari sumbangan (donasi) dicatat sebesar nilai wajar pada saat perolehan.</p>
Aset Tetap Lainnya	<p>Harga perolehan, honorarium, dan seluruh biaya yang dikeluarkan untuk memperoleh aset tersebut sampai siap pakai. Aset tetap lainnya dapat diperoleh melalui kontrak maupun swakelola. Biaya perolehan aset tetap lainnya yang diperoleh melalui kontrak meliputi pengeluaran nilai kontrak, biaya perencanaan dan pengawasan, serta biaya</p>

	perizinan. Hasil kajian dan penelitian yang menghasilkan laporan dicatat menjadi aset tetap lainnya berupa buku kepustakaan sebesar biaya penggandaan dan percetakan.
--	---

- e) Biaya perolehan dari masing – masing aset tetap yang diperoleh secara gabungan ditentukan dengan mengalokasikan harga gabungan tersebut berdasarkan perbandingan nilai wajar masing – masing aset yang bersangkutan.
- f) Biaya perolehan Aset Tetap yang di bangun dengan cara swakelola meliputi :
- 1) Biaya langsung untuk tenaga kerja, bahan baku;
  - 2) Biaya tidak langsung termasuk biaya perencanaan dan pengawasan, perlengkapan, tenaga listrik, sewa peralatan; dan
  - 3) Semua biaya lainnya yang terjadi berkenaan dengan pembangunan Aset tetap tersebut.
- g) Biaya administrasi dan biaya umum lainnya bukan merupakan suatu komponen biaya aset tetap sepanjang biaya tersebut tidak dapat diatribusikan secara langsung pada biaya perolehan aset atau membawa aset ke kondisi kerjanya.
- h) Pengukuran Aset tetap harus memperhatikan kebijakan pemerintah daerah mengenai ketentuan nilai satuan minimum kapitalisasi Aset Tetap. Jika nilai perolehan aset tetap di bawah nilai satuan minimum kapitalisasi maka atas aset tetap tersebut tidak dapat diakui dan disajikan sebagai aset tetap, namun tetap diungkapkan dalam Catatan atas Laporan Keuangan dan dicatat sebagai ekstra komptabel.
- i) Nilai satuan minimum kapitalisasi aset tetap untuk per satuan peralatan dan mesin serta aset tetap lainnya berupa hewan, barang bercorak kesenian/kebudayaan/olahraga dan biota perairan adalah lebih dari Rp.1.000.000,00 (Satu Juta Rupiah).
- j) Nilai satuan minimum kapitalisasi untuk aset tetap lainnya berupa bahan perpustakaan, barang koleksi non budaya serta tanaman ditetapkan sebesar lebih dari Rp. 300.000,00 (Tiga Ratus Ribu Rupiah).
- k) Nilai satuan minimum kapitalisasi aset tetap dikecualikan terhadap pengeluaran untuk tanah, gedung dan bangunan serta jalan/irigasi/jaringan.
2. Pengeluaran Setelah Perolehan (Subsequent Expenditures)
- a) Suatu pengeluaran setelah perolehan atau pengeluaran pemeliharaan akan dikapitalisasi jika memenuhi kriteria sebagai berikut:
- 1) Manfaat ekonomi atas aset tetap yang dipelihara :
    - (a) Bertambah ekonomis/efisien;
    - (b) Bertambah umur ekonomis;
    - (c) Bertambah volume; dan/atau
    - (d) Bertambah kapasitas produksi.
  - 2) Nilai pengeluaran belanja atas pemeliharaan aset tetap tersebut harus melebihi nilai satuan minimum kapitalisasi aset tetap. Nilai satuan minimum kapitalisasi adalah penambahan nilai aset tetap dari hasil pengembangan, rehabilitasi, renovasi dan restorasi. Nilai Satuan Minimum Kapitalisasi Aset Tetap menentukan apakah perolehan suatu aset harus dikapitalisasi atau tidak.
  - 3) Nilai satuan minimum kapitalisasi untuk pemeliharaan peralatan dan mesin per satuan barang ditetapkan sebagaimana yang terlampir pada Peraturan Bupati Nomor 80

Tahun 2020.

- 4) Nilai satuan minimum kapitalisasi untuk pemeliharaan Gedung dan bangunan ditetapkan dengan rincian sebagai berikut:

<b>Gedung dan Bangunan</b>	<b>Nilai Kapitalisasi (Rp.)</b>
Bangunan Gedung Tempat Kerja	30.000.000,00
Bangunan Gedung Tempat Tinggal	20.000.000,00
Bangunan Menara Perambuan	10.000.000,00
Tugu/ Tanda Batas	5.000.000,00
Candi/Tugu Peringatan/Prasasti	15.000.000,00

- 5) Nilai satuan minimum kapitalisasi untuk pemeliharaan jalan adalah untuk kerusakan lebih dari 15% (lima belas perseratus) dari kondisi awal jalan, sedangkan nilai satuan minimum kapitalisasi untuk pemeliharaan jaringan dan irigasi ditetapkan untuk kerusakan lebih dari 40% (empat puluh perseratus) dari kondisi awal bangunan dan saluran.
- 6) Tabel Penambahan Masa Manfaat Akibat Perbaikan, Renovasi, Pemeliharaan, Pengembangan dan Restorasi dapat dilihat pada lampiran Peraturan Bupati Jombang Nomor 80 Tahun 2020
- b) Untuk jenis aset tetap yang biaya pemeliharaannya tidak dikapitalisasi maka pada saat penganggaran dianggarkan dalam belanja barang dan jasa.
- c) Pengeluaran belanja pengadaan baru untuk aset yang memenuhi kriteria berwujud, mempunyai masa manfaat lebih dari 12 (dua belas) bulan biaya.
- d) Perolehan aset dapat diukur secara andal dan tidak dimaksudkan untuk dijual dalam operasi normal entitas dan diperoleh atau dibangun dengan maksud untuk digunakan, tetapi nilai dibawah kapitalisasi sebagaimana diatas maka pada saat penganggaran dianggarkan dalam belanja barang dan jasa dan dicatat secara terpisah dari daftar aset tetap (Extra Comptable).
- e) Nilai satuan minimum kapitalisasi atas perolehan aset tetap dari hasil pengembangan, reklasifikasi, renovasi, perbaikan atau restorasi untuk per satuan jenis aset atau harga per unit atas jenis aset bilamana tidak menambah umur maka tidak dikapitalisasi dan dianggarkan di belanja barang dan jasa.
- f) Penambahan masa manfaat aset tetap tidak boleh melebihi estimasi masa manfaat maksimal masing-masing aset tetap.
3. Kejadian Setelah Perolehan (Subsequent Events)
- a) Pertukaran Aset (Exchange of Assets)
- 1) Suatu aset tetap dapat diperoleh melalui pertukaran atau pertukaran sebagian aset tetap yang tidak serupa atau aset lainnya. Biaya dari pos semacam itu diukur berdasarkan nilai wajar aset yang diperoleh, yaitu nilai ekuivalen atas nilai tercatat aset yang dilepas setelah disesuaikan dengan jumlah setiap kas atau setara kas yang ditransfer/diserahkan.
  - 2) Suatu aset tetap hasil pertukaran dapat diakui apabila kepenguasaan atas aset telah berpindah dan nilai perolehan aset hasil pertukaran tersebut dapat diukur dengan andal. Pertukaran aset tetap dituangkan dalam Berita Acara Serah Terima (BAST). Berdasarkan BAST tersebut, pengguna barang menerbitkan Surat Keputusan (SK) Penghapusan terhadap

aset yang diserahkan. Berdasarkan BAST dan SK Penghapusan, pengelola/pengguna barang mengeluarkan aset tersebut dari neraca maupun dari daftar barang dan membukukan aset tetap pengganti.

- 3) Suatu aset tetap dapat diperoleh melalui pertukaran atas suatu aset yang serupa yang memiliki manfaat yang serupa dan memiliki nilai wajar yang serupa. Suatu aset tetap juga dapat dilepas dalam pertukaran dengan kepemilikan aset yang serupa. Dalam keadaan tersebut tidak ada keuntungan dan kerugian yang diakui dalam transaksi ini. Biaya aset yang baru diperoleh dicatat sebesar nilai tercatat (carrying amount) atas aset yang dilepas.
  - 4) Nilai wajar atas aset yang diterima tersebut dapat memberikan bukti adanya suatu pengurangan (impairment) nilai atas aset yang dilepas. Dalam kondisi seperti ini, aset yang dilepas harus diturun-nilai-bukukan (writtendown) dan nilai setelah diturunnilai bukukan (written down) tersebut merupakan nilai aset yang diterima. Contoh dari pertukaran atas aset yang serupa termasuk pertukaran bangunan, mesin, peralatan khusus, dan kapal terbang. Apabila terdapat aset lainnya dalam pertukaran, misalnya kas, maka hal ini mengindikasikan bahwa pos yang dipertukarkan tidak mempunyai nilai yang sama.
  - 5) Terhadap aset tetap yang diperoleh melalui pertukaran dengan aset tetap yang serupa, yang memiliki manfaat yang serupa dan memiliki nilai wajar yang serupa, maka aset yang baru diperoleh dicatat sebesar nilai tercatat (carrying amount) aset yang dilepas. Apabila terdapat aset lainnya dalam pertukaran, misalnya kas, maka hal ini mengindikasikan bahwa aset tetap yang dipertukarkan tidak mempunyai nilai yang sama. Dalam hal aset tetap yang dipertukarkan nilainya lebih tinggi daripada aset tetap pengganti dan terdapat kas yang diterima, maka kas tersebut diakui sebagai Pendapatan LRA dan Pendapatan-LO.
  - 6) Dalam hal terjadi pertukaran aset tetap, maka harus diungkapkan:
    - (a) Pihak yang melakukan pertukaran aset tetap;
    - (b) Jenis aset tetap yang diserahkan dan nilainya;
    - (c) Jenis aset tetap yang diterima beserta nilainya; dan
    - (d) Jumlah hibah selisih lebih dari pertukaran aset tetap
- b) Aset Donasi merupakan Aset tetap yang diperoleh dari :
- 1) sumbangan (donasi) harus dicatat sebesar nilai wajar pada saat perolehan.
  - 2) Sumbangan aset tetap didefinisikan sebagai transfer tanpa persyaratan suatu aset tetap ke suatu entitas, misalnya perusahaan non pemerintah memberikan bangunan yang dimilikinya untuk digunakan oleh satu unit pemerintah daerah. Tanpa persyaratan apapun. Penyerahan aset tetap tersebut akan sangat andal bila didukung dengan bukti perpindahan kepemilikannya secara hukum, seperti adanya akta hibah.
  - 3) Tidak termasuk aset donasi, apabila penyerahan aset tetap tersebut dihubungkan dengan kewajiban entitas lain kepada pemerintah daerah. Sebagai contoh, satu perusahaan swasta membangun aset tetap untuk pemerintah daerah dengan persyaratan kewajibannya kepada pemerintah daerah telah dianggap selesai. Perolehan aset tetap tersebut harus diperlakukan seperti perolehan aset tetap dengan pertukaran.



- 4) Apabila perolehan aset tetap memenuhi kriteria perolehan aset donasi, maka perolehan tersebut diakui sebagai pendapatan operasional.
- c) Penghentian dan Pelepasan Aset Tetap
- 1) Penghentian Aset Tetap.  
Apabila suatu aset tetap tidak dapat digunakan karena aus, ketinggalan jaman, tidak sesuai dengan kebutuhan organisasi yang makin berkembang, rusak berat, tidak sesuai dengan rencana umum tata ruang (RUTR), atau masa kegunaannya telah berakhir, maka aset tetap tersebut hakekatnya tidak lagi memiliki manfaat ekonomi masa depan, sehingga penggunaannya harus dihentikan. Aset tetap yang tidak digunakan dalam kegiatan operasional pemerintah, dengan kata lain dihentikan dari penggunaan aktif. Pada saat dokumen sumber untuk mengeluarkan aset tetap tersebut dari neraca telah diperoleh, maka aset tetap yang telah direklasifikasi menjadi aset lainnya tersebut dikeluarkan dari neraca. Aset tetap yang secara permanen dihentikan penggunaannya karena tidak lagi memiliki manfaat ekonomi di masa yang akan datang, seperti rusak berat, maka aset tetap tersebut dikeluarkan dari neraca.
  - 2) Pelepasan Aset Tetap.  
Pelepasan aset di lingkungan pemerintah lazim disebut sebagai pemindahtanganan. Apabila suatu aset tetap dilepaskan karena dipindahtanggankan, maka aset tetap yang bersangkutan harus dikeluarkan dari neraca. Sesuai dengan perundang-undangan di bidang pengelolaan BMD, pemerintah dapat melakukan pemindahtanganan dengan cara:
    - (a) Dijual
    - (b) Dipertukarkan
    - (c) D hibahkan
    - (d) Dijadikan penyertaan modal daerah.

Aset yang dilepaskan melalui penjualan, dikeluarkan dari neraca pada saat diterbitkan risalah lelang atau dokumen penjualan sesuai dengan ketentuan perundang-undangan. Aset tetap yang dihibahkan, dikeluarkan dari neraca pada saat telah diterbitkan berita acara serah terima hibah oleh entitas sebagai tindak lanjut persetujuan hibah Aset Tetap yang dipindahkan melalui mekanisme penyertaan modal daerah, dikeluarkan dari neraca pada saat diterbitkan penetapan penyertaan modal daerah.
  - 3) Aset Tetap Hilang.  
Aset tetap hilang harus dikeluarkan dari neraca sebesar nilai perolehannya.
4. Pengukuran Berikutnya (Subsequent Measurement)
- Aset tetap disajikan berdasarkan biaya perolehan aset tetap tersebut dikurangi akumulasi penyusutan. Apabila terjadi kondisi yang memungkinkan penilaian kembali, maka aset tetap akan disajikan dengan penyesuaian pada masing-masing akun aset tetap.
- a) Penyusutan
    - 1) Penyusutan adalah alokasi yang sistematis atas nilai suatu aset tetap yang dapat disusutkan (depreciable assets) selama masa manfaat aset yang bersangkutan.
    - 2) Tujuan utama dari penyusutan bukan untuk menumpuk sumber daya bagi pembayaran hutang atau penggantian aset tetap yang disusutkan. Tujuan dasarnya adalah menyesuaikan nilai aset tetap untuk mencerminkan nilai wajarnya. Di samping itu penyusutan juga dimaksudkan

- untuk menggambarkan penurunan kapasitas dan manfaat yang diakibatkan pemakaian aset tetap dalam kegiatan pemerintahan.
- 3) Penyusutan aset tetap bukan merupakan metode alokasi biaya untuk periode yang menerima manfaat aset tetap tersebut sebagaimana diberlakukan di sektor komersial. Penyesuaian nilai ini lebih merupakan upaya untuk menunjukkan pengurangan nilai karena pengkonsumsian potensi manfaat aset oleh karena pemakaian dan/atau pengurangan nilai karena keusangan dan lain-lain.
  - 4) Prasyarat yang perlu dipenuhi untuk menerapkan penyusutan, adalah :
    - (a) Identitas Aset yang Kapasitasnya Menurun
    - (b) Nilai yang Dapat Disusutkan
    - (c) Masa Manfaat dan Kapasitas Aset Tetap.
  - 5) Prosedur penyusutan:
    - (a) Identifikasi Aset Tetap yang Dapat Disusutkan
    - (b) Pengelompokan Aset
    - (c) Penetapan Nilai Wajar
    - (d) Aset Tetap
    - (e) Penetapan Nilai yang Dapat Disusutkan
    - (f) Penetapan Metode Penyusutan
    - (g) Perhitungan dan Pencatatan Penyusutan
  - 6) Nilai penyusutan untuk masing-masing periode diakui sebagai pengurang nilai tercatat aset tetap dalam neraca dan beban penyusutan dalam laporan operasional.
  - 7) Masa manfaat aset tetap yang dapat disusutkan harus ditinjau secara periodik dan jika terdapat perbedaan besar dari estimasi sebelumnya, penyusutan periode sekarang dan yang akan datang harus dilakukan penyesuaian.
  - 8) Penyesuaian nilai aset tetap dilakukan dengan berbagai metode yang sistematis sesuai dengan masa manfaat. Metode penyusutan yang digunakan harus dapat menggambarkan manfaat ekonomi atau kemungkinan jasa (service potential) yang akan mengalir ke pemerintah.
  - 9) Seluruh aset tetap disusutkan sesuai sifat dan karakteristik aset tersebut selain tanah dan konstruksi dalam pengerjaan.
  - 10) Aset tetap lainnya berupa hewan, tanaman, taman dan buku perpustakaan tidak dilakukan penyusutan secara periodik, melainkan diterapkan penghapusan pada aset tetap lainnya tersebut apabila sudah tidak dapat digunakan atau mati.
  - 11) Untuk penyusutan atas Aset Tetap-Renovasi dilakukan sesuai dengan umur ekonomik mana yang lebih pendek (which ever shorter) antara masa manfaat aset dengan masa pinjaman/sewa
  - 12) Perhitungan penyusutan aset tetap yang diperoleh tengah tahun menggunakan pendekatan tahunan yaitu penyusutan dapat dihitung satu tahun penuh meskipun diperoleh satu atau dua bulan bahkan satu hari.
  - 13) Metode penyusutan yang digunakan adalah metode garis lurus (straight line method), dimana metode ini menetapkan tarif penyusutan untuk masing-masing periode dengan jumlah yang sama. Adapun rumus dapat dilihat pada lampiran Peraturan Bupati Jombang Nomor 80 Tahun 2020.
  - 14) Dalam kebijakan ini yang menjadi nilai yang dapat disusutkan adalah nilai perolehan atau nilai wajar aset tetap. Dalam penghitungan penyusutan aset tetap tidak menerapkan nilai sisa/nilai residu.

- 15) Masa manfaat adalah periode suatu aset tetap yang diharapkan digunakan untuk aktivitas pemerintahan dan/atau pelayanan publik atau jumlah produksi atau unit serupa yang diharapkan diperoleh dari aset untuk aktivitas pemerintah dan/atau pelayanan publik.
  - 16) Masa manfaat aset tetap yang dapat disusutkan harus ditinjau secara periodik dan jika terdapat perbedaan besar dari estimasi sebelumnya, penyusutan periode sekarang dan yang akan datang harus dilakukan penyesuaian.
  - 17) Estimasi masa manfaat maksimal masing-masing aset tetap sesuai tabel pada lampiran Peraturan Bupati Nomor 80 Tahun 2020
- b) Penerapan Penyusutan Untuk Pertama Kalinya
- 1) Perhitungan penyusutan aset tetap untuk pertama kalinya dapat dikelompokkan menjadi 3 (tiga), yaitu:
    - (a) Aset yang diperoleh pada tahun dimulainya penerapan penyusutan
    - (b) Aset yang diperoleh setelah penyusunan neraca awal hingga satu tahun sebelum dimulainya penerapan penyusutan.
    - (c) Aset yang diperoleh sebelum penyusunan neraca awal.
  - 2) Dalam hal terjadi perubahan nilai aset tetap sebagai akibat penambahan atau pengurangan kuantitas dan/atau nilai aset tetap, maka penambahan atau pengurangan tersebut diperhitungkan dalam nilai yang dapat disusutkan.
    - (a) Pencatatan penyusutan pertama kali besar kemungkinan akan menghadapi permasalahan penetapan sisa masa manfaat dan masa manfaat yang sudah disusutkan, karena aset tetap sejenis yang akan disusutkan kemungkinan diperoleh pada tahun-tahun yang berbeda satu sama lain.
    - (b) Jika secara umum terhadap aset tetap jenis peralatan dan mesin seperti mobil ditetapkan memiliki masa manfaat selama 10 tahun dan penyusutannya memakai metode garis lurus dapat terjadi variasi permasalahan sisa masa manfaat dan masa manfaat yang disusutkan.
    - (c) Dengan variasi sisa masa manfaat dan masa manfaat yang sudah dilalui dan yang harus dijadikan penyusutan maka jumlah penyusutan adalah proporsional dengan masa manfaat yang dilalui dan harus dijadikan dasar penyusutan.
- Umur atau masa manfaat dihitung penyusutan aset tersebut pertama kali dengan 3 (tiga) kelompok sebagai berikut:
- (a) Aset yang diperoleh pada tahun dimulainya penerapan penyusutan, aset tersebut sudah disajikan dengan nilai perolehan.
  - (b) Aset yang diperoleh sebelum penyusunan neraca awal hingga satu tahun sebelum dimulainya penerapan penyusutan, aset tersebut sudah disajikan dengan nilai perolehan. Penyusutannya terdiri dari penyusutan tahun-tahun sebelumnya.
  - (c) Aset yang diperoleh sebelum penyusutan neraca awal. Aset-aset yang diperoleh lebih dari 1 (satu) tahun sebelum saat penyusunan neraca awal, maka aset tersebut disajikan dengan nilai wajar. Pada saat penyusunan neraca awal, penetapan hanya dilakukan untuk nilai asset saja tanpa diikuti dengan penetapan sisa masa manfaat aset. Akan tetapi tahun perolehan dapat diketahui secara

valid, sehingga untuk perhitungan penyusutannya masa manfaat ditetapkan dari tahun perolehan aset tersebut.

5. Pemanfaatan Aset Tetap Yang Sudah Seluruh Nilainya Disusutkan
  - a) Walaupun suatu aset sudah disusutkan seluruh nilai hingga nilai bukunya menjadi Rp.0 (nol rupiah), mungkin secara teknis aset itu masih dapat dimanfaatkan. Jika hal seperti ini terjadi, aset tetap tersebut tetap disajikan dengan menunjukkan baik nilai perolehan maupun akumulasi penyusutan.
  - b) Aset tersebut tetap dicatat dalam kelompok aset tetap yang bersangkutan dan dijelaskan dalam Catatan atas Laporan Keuangan.
  - c) Aset tetap yang telah habis masa penyusutannya dapat dihapuskan jika telah mendapat ijin penghapusbukuan dari Bupati.
6. Penilaian Kembali Aset Tetap (Revaluation)
  - a) Penilaian kembali atau revaluasi aset tetap pada umumnya tidak diperkenankan karena Standar Akuntansi Pemerintahan menganut penilaian aset berdasarkan biaya perolehan atau harga pertukaran. Penyimpangan dari ketentuan ini mungkin dilakukan berdasarkan ketentuan pemerintah yang berlaku secara nasional.
  - b) Dalam hal ini laporan keuangan harus menjelaskan mengenai penyimpangan dari konsep biaya perolehan di dalam penyajian aset tetap serta pengaruh penyimpangan tersebut terhadap gambaran keuangan suatu entitas. Selisih antara nilai revaluasi dengan nilai tercatat aset tetap dibukukan dalam akun ekuitas.

#### B. PENYAJIAN

1. Aset tetap disajikan sebagai bagian dari aset. Adapun bentuk penyajian aset tetap dalam Neraca Pemerintah Daerah dapat dilihat pada gambar berikut:

<b>PEMERINTAH PROVINSI/KABUPATEN/KOTA NERACA NERACA ASET TETAP</b>		
	(Dalam Rupiah)	
Uraian	20X1	20X0
<b>ASET</b>		
<b>ASET LANCAR</b>		
Kas di Kas Daerah	xxx	xxx
Kas di Bendahara Pengeluaran	xxx	xxx
Kas di Bendahara Penerimaan	xxx	xxx
Investasi Jangka Pendek	xxx	xxx
Piutang Pajak	xxx	xxx
Piutang Retribusi	xxx	xxx
Penyisihan Piutang	xxx	xxx
Belanja Dibayar Dimuka	xxx	xxx
Bagian Lancar Pinjaman kepada Perusahaan Negara	xxx	xxx
Bagian Lancar Pinjaman kepada Perusahaan Daerah	xxx	xxx
Bagian Lancar Pinjaman kepada Pemerintah Pusat	xxx	xxx
Bagian Lancar Pinjaman kepada Pemerintah Daerah Lainnya	xxx	xxx
Bagian Lancar Tagihan Penjualan Angsuran	xxx	xxx
Bagian Lancar Tuntutan Ganti Rugi	xxx	xxx
Piutang Lainnya	xxx	xxx
Persediaan		
<b>Jumlah Aset Lancar</b>		
<b>INVESTASI JANGKA PANJANG</b>	xxx	xxx
<b>Investasi Nonpermanen</b>	xxx	xxx
Pinjaman Jangka Panjang	xxx	xxx
Investasi dalam Surat Utang Negara	xxx	xxx
Investasi dalam Proyek Pembangunan	xxx	xxx
Investasi Nonpermanen Lainnya	xxx	xxx
<b>Jumlah Investasi Nonpermanen</b>	xxx	xxx
<b>Investasi Permanen</b>	xxx	xxx
Penyertaan Modal Pemerintah Daerah	xxx	xxx
Investasi Permanen Lainnya		
<b>Jumlah Investasi Permanen</b>		
<b>Jumlah Investasi Jangka Panjang</b>	xxx	xxx
<b>ASET TETAP</b>	xxx	xxx
Tanah	xxx	xxx
Peralatan dan Mesin	xxx	xxx
Gedung dan Bangunan	xxx	xxx
Jalan, Irigasi dan Jaringan	xxx	xxx
Aset Tetap Lainnya	xxx	xxx
Konstruksi dalam Pengerjaan		
Akumulasi Penyusutan		
<b>Jumlah Aset Tetap</b>	xxx	xxx
<b>DANA CADANGAN</b>	xxx	xxx
Dana Cadangan	xxx	xxx
<b>Jumlah Dana Cadangan</b>	xxx	xxx
<b>ASET LAINNYA</b>	xxx	xxx
Tagihan Penjualan Angsuran	xxx	xxx
Tuntutan Ganti Rugi	xxx	xxx
Kemitraan dengan Pihak Ketiga	xxx	xxx

Aset Tak Berwujud	xxx	xxx
Aset Lain-lain		
<b>Jumlah Aset Lainnya</b>		
<b>JUMLAH ASET</b>		

### C. Pengungkapan

1. Laporan keuangan harus mengungkapkan untuk masing-masing jenis aset tetap sebagai berikut:
  - a) Dasar penilaian yang digunakan untuk menentukan nilai tercatat (carrying amount);
  - b) Kebijakan akuntansi sebagai dasar kapitalisasi tanah, yang dalam hal tanah tidak ada nilai satuan minimum kapitalisasi;
  - c) Rekonsiliasi jumlah tercatat pada awal dan akhir periode yang menunjukkan:
    - (1) Penambahan (pembelian, hibah/donasi, pertukaran aset, reklasifikasi dan lainnya);
    - (2) Perolehan yang berasal dari pembelian direkonsiliasi dengan total belanja modal;
    - (3) Pengurangan (penjualan, hibah/donasi, pertukaran aset, reklasifikasi dan lainnya);
    - (4) Perubahan nilai (jika ada)
  - d) Informasi penyusutan, meliputi:
    - (1) Nilai penyusutan;
    - (2) Metode penyusutan yang digunakan dan alasan pilihan metode penyusutan;
    - (3) Masa manfaat atau tarif penyusutan yang digunakan;
    - (4) Nilai tercatat bruto dan akumulasi penyusutan pada awal dan akhir periode;
  - e) Laporan keuangan juga harus mengungkapkan:
    - (1) Eksistensi dan batasan hak milik atas aset tetap;
    - (2) Kebijakan akuntansi untuk kapitalisasi yang berkaitan dengan aset tetap;
    - (3) Jumlah pengeluaran pada pos aset tetap dalam konstruksi;
    - (4) Jumlah komitmen untuk akuisisi aset tetap.
    - (5) Aset bersejarah diungkapkan secara rinci, antara lain nama, jenis, kondisi dan lokasi aset dimaksud.
2. Jika aset tetap dicatat pada jumlah yang dinilai kembali, maka hal-hal berikut harus diungkapkan:
  - a) Dasar peraturan untuk menilai kembali aset tetap;
  - b) Tanggal efektif penilaian kembali;
  - c) Jika ada, nama penilai independen;
  - d) Hakikat setiap petunjuk yang digunakan untuk menentukan biaya pengganti;
  - e) Nilai tercatat setiap jenis aset tetap.

### D. Reklasifikasi dan Koreksi Aset Tetap

1. Reklasifikasi Aset Tetap
  - a) Reklasifikasi merupakan pemindahan kelompok aset tetap ke aset lainnya dalam akuntansi.
  - b) Aset tetap yang dihentikan dari penggunaan aktif pemerintah tidak memenuhi definisi aset tetap dan harus dipindahkan ke pos aset lainnya sesuai dengan nilai tercatatnya.
  - c) Suatu aset tetap yang dihentikan atau dihapuskan tidak memenuhi definisi aset tetap. Namun demikian, aset tersebut belum dapat dieliminasi dari neraca karena proses penghentian yang lebih dikenal sebagai pemindahtanganan dan penghapusan

masih berlangsung. Dengan kata lain, dokumen sumber untuk melakukan penghapusbukuan belum diterbitkan, sehingga mengatur bahwa aset dengan kondisi demikian harus dipindahkan dari aset tetap ke aset lainnya.

- d) Reklasifikasi aset tetap ke aset lainnya dapat dilakukan sepanjang waktu, tidak tergantung periode laporan

## 2. Koreksi Aset Tetap

- a) Koreksi adalah tindakan pembetulan akuntansi agar pos-pos yang tersaji dalam laporan keuangan entitas menjadi sesuai dengan yang seharusnya.
- b) Koreksi aset tetap dilakukan dengan menambah atau mengurangi akun aset tetap yang bersangkutan
- c) Koreksi meliputi koreksi sistemik dan koreksi non sistemik. Dari sisi transaksi, koreksi mencakup transaksi pendapatan, belanja, penerimaan, pengeluaran dan koreksi akun neraca. Dari periodenya, koreksi dapat dibedakan menjadi koreksi untuk tahun berjalan, koreksi periode lalu pada saat laporan keuangan periode terkait belum diterbitkan, dan koreksi periode lalu pada saat laporan keuangan periode terkait telah diterbitkan. Termasuk dalam lingkup koreksi adalah temuan pemeriksaan yang diharuskan untuk dikoreksi.
- d) Koreksi dilakukan oleh SKPD yang bersangkutan dan dilaporkan secara berjenjang, sampai dengan pemerintah daerah. Kadangkala untuk mengejar waktu penyampaian laporan keuangan, koreksi dapat dilakukan secara sentralistik di kantor pemerintah daerah, baru kemudian didistribusikan pada entitas akuntansi di bawahnya untuk melakukan penyesuaian.
- e) Koreksi aset tetap dapat dilakukan kapan saja, tidak tergantung pada periode pelaporan dan waktu penyusunan laporan. Pada umumnya koreksi aset tetap dilakukan pada saat ditemukan kesalahan.

## E. Hubungan Antara Belanja dan Perolehan Aset Tetap

Untuk menyikapi adanya ketidaksesuaian dalam penganggaran dan pelaporan keuangan pemerintahan, antara lain pengeluaran untuk pembelian aset tetap dianggarkan dalam Belanja Barang, pengeluaran untuk pemeliharaan rutin dianggarkan dalam Belanja Modal, atau bantuan untuk masyarakat dianggarkan dalam Belanja Modal. Untuk itu diharapkan adanya kesesuaian penyusunan anggaran, pelaksanaan anggaran dan pelaporan. Perolehan aset tetap yang akan digunakan dalam kegiatan pemerintahan dianggarkan dalam Belanja Modal.

Suatu belanja dapat dikategorikan sebagai Belanja Modal jika:

1. Pengeluaran tersebut mengakibatkan adanya perolehan aset tetap atau aset lainnya yang menambah aset pemerintah;
2. Pengeluaran tersebut melebihi batasan minimal kapitalisasi aset tetap atau aset lainnya yang telah ditetapkan oleh pemerintah; dan
3. Perolehan aset tetap tersebut diniatkan bukan untuk dijual atau diserahkan ke masyarakat atau pihak lainnya.

Dalam situasi yang ideal akan terdapat kesesuaian antara Belanja Modal sebagai akun anggaran dengan Aset Tetap sebagai akun finansial. Namun demikian, dalam hal terjadi kontradiksi antara akun anggaran dengan akun finansial, maka akuntansi akan menggunakan prinsip substansi mengungguli bentuk formal (substance over form).

#### F. Aset Tetap Renovasi

Aset Tetap Renovasi dapat dibedakan menjadi 2 (dua) jenis, yaitu:

1. Renovasi Aset Tetap bukan milik-dalam lingkup entitas pelaporan; Mencakup perbaikan aset tetap bukan milik suatu satuan kerja/SKPD yang memenuhi syarat kapitalisasi namun masih dalam satu entitas pelaporan, seperti: Renovasi aset tetap milik UPTD dan aset tetap milik SKPD lain. Pada satuan kerja yang melakukan renovasi tidak dicatat sebagai penambah nilai perolehan aset tetap terkait karena kepemilikan aset tetap tersebut ada pada pihak lain. Renovasi tersebut apabila telah selesai dilakukan dan belum diserahkan kepada pemilik akan dibukukan sebagai aset tetap lainnya-aset renovasi dan disajikan di neraca sebagai kelompok aset tetap. Pada akhir tahun anggaran, aset renovasi ini seyogyanya diserahkan pada pemilik. Jika dokumen sumber penyerahan tersebut telah diterbitkan, maka aset tetap renovasi tersebut dikeluarkan dari neraca dan SKPD pemilik akan mencatat dan menambahkannya sebagai aset tetap terkait. Mekanisme penyerahan mengikuti peraturan yang berlaku. Apabila sampai dengan tanggal pelaporan renovasi tersebut belum selesai dikerjakan, maka akan dicatat sebagai konstruksi dalam pengerjaan.
2. Renovasi Aset Tetap bukan milik-diluar lingkup entitas pelaporan. Mencakup perbaikan aset tetap bukan milik suatu satuan kerja atau SKPD, di luar entitas pelaporan yang memenuhi syarat kapitalisasi. Lingkup renovasi jenis ini meliputi:
  - a) Renovasi aset tetap milik pemerintah lainnya; dan
  - b) Renovasi aset tetap milik pihak lain, selain pemerintah (swasta, BUMD, yayasan, dan lain-lain).

Renovasi semacam ini, pengakuan dan pelaporannya serupa dengan renovasi aset bukan milik-dalam lingkup entitas pelaporan, yaitu pada satuan kerja yang melakukan renovasi tidak dicatat sebagai penambah nilai perolehan aset tetap terkait karena kepemilikan aset tersebut ada di pihak lain. Apabila renovasi aset tersebut telah selesai dilakukan sebelum tanggal pelaporan, maka transaksi renovasi akan dibukukan sebagai aset tetap lainnya-aset renovasi dan disajikan di neraca sebagai kelompok aset tetap. Apabila sampai dengan tanggal pelaporan renovasi tersebut belum selesai dikerjakan, maka akan dicatat sebagai KDP.



**BAB V**  
**PEDOMAN MANAJEMEN SUMBER DAYA MANUSIA**  
**SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK**

**I. PENDAHULUAN**

Undang – Undang No 23 Tahun 2014 tentang Pemerintahan Daerah mengamanatkan pemerintah daerah untuk mengemban tanggung jawab dalam melakukan penataan daerah dengan membangun tata kelola pemerintahan yang baik agar memiliki daya saing kinerja yang efektif serta efisien. Beberapa indikator yakni bersih, efektif, transparan dan akuntabel merupakan perimeter yang diharapkan untuk dipenuhi.

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik mengamanatkan bahwa pemerintah daerah harus menerapkan kebijakan mengenai teknologi dan informasi yang ada di daerah agar menyesuaikan dengan kebijakan pemerintah pusat.

Sistem Pemerintahan Berbasis Elektronik (SPBE) adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE. Adapun tujuan penyelenggaraan SPBE adalah mewujudkan tata kelola pemerintahan dan pelayanan publik yang bersih, efektif, efisien, akuntabel dan terpercaya, serta meningkatkan efisiensi dan keterpaduan penyelenggaraan pemerintahan berbasis elektronik.

Dalam rangka menjalankan Undang-undang serta Peraturan Presiden tersebut, Pemerintah Kabupaten Jombang akan mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya melalui penerapan sistem pemerintahan berbasis elektronik. Penerapan sistem pemerintahan berbasis elektronik di Kabupaten Jombang tersebut telah tertuang dalam Peraturan Bupati Jombang Nomor 15 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Jombang, sebagai pedoman bagi Perangkat Daerah dalam pelaksanaan dan pengembangan SPBE di Daerah, sehingga dapat berjalan dengan baik dan berkualitas sesuai dengan ketentuan peraturan perundang-undangan.

Manajemen SPBE adalah serangkaian proses untuk mencapai penerapan SPBE yang efektif, efisien dan berkesinambungan, serta layanan SPBE yang berkualitas. Manajemen SDM merupakan salah satu bagian dari 8 (delapan) bagian manajemen SPBE yang bertujuan untuk menjamin keberlangsungan dan peningkatan mutu layanan dalam SPBE. Manajemen SDM dilakukan melalui serangkaian proses perencanaan, pengembangan, pembinaan dan pendayagunaan sumber daya manusia dalam SPBE. Manajemen sumber daya manusia memastikan ketersediaan dan kompetensi sumber daya manusia untuk pelaksanaan Tata Kelola SPBE dan Manajemen SPBE.

Maksud penyusunan perencanaan pelaksanaan manajemen SDM SPBE ini adalah merumuskan perencanaan yang komprehensif mengenai kebutuhan dan kompetensi sumber daya manusia di bidang TIK SPBE di lingkup Pemerintah Kabupaten Jombang. Adapun tujuan dari penyusunan perencanaan pelaksanaan manajemen SDM SPBE ini adalah tersedianya dokumen perencanaan pelaksanaan manajemen SDM sebagai acuan dalam upaya pemenuhan ketersediaan dan kompetensi SDM SPBE di Kabupaten Jombang

Sasaran Penyusunan Perencanaan manajemen SDM adalah terpenuhinya kompetensi SDM TIK SPBE dalam rangka mewujudkan penerapan SPBE di Pemerintah Kabupaten Jombang. Adapun keluaran Penyusunan Perencanaan Pelaksanaan Manajemen SDM SPBE adalah gambaran ketersediaan, kebutuhan kompetensi di bidang TIK SPBE dan rencana pelaksanaan pemenuhan kompetensi SDM di bidang TIK SPBE di

Kabupaten Jombang.

## **II. DEFINISI**

1. Pegawai Aparatur Sipil Negara yang selanjutnya disebut Pegawai ASN adalah pegawai negeri sipil dan pegawai pemerintah dengan perjanjian kerja yang diangkat oleh pejabat pembina kepegawaian dan disertai tugas dalam suatu jabatan pemerintahan atau disertai tugas negara lainnya dan digaji berdasarkan peraturan perundang-undangan.
2. Pegawai Negeri Sipil yang selanjutnya disingkat PNS adalah warga negara Indonesia yang memenuhi syarat tertentu, diangkat sebagai Pegawai ASN secara tetap oleh pejabat pembina kepegawaian untuk menduduki jabatan pemerintahan.
3. Pegawai Pemerintah dengan Perjanjian Kerja yang selanjutnya disingkat PPPK adalah warga negara Indonesia yang memenuhi syarat tertentu, yang diangkat berdasarkan perjanjian kerja untuk jangka waktu tertentu dalam rangka melaksanakan tugas.
4. Pejabat Pembina Kepegawaian yang selanjutnya disingkat PPK adalah pejabat yang mempunyai kewenangan menetapkan pengangkatan, pemindahan, dan pemberhentian Pegawai ASN dan pembinaan manajemen ASN di instansi pemerintah sesuai dengan ketentuan peraturan perundang-undangan.
5. Pejabat yang Berwenang yang selanjutnya disingkat PyB adalah pejabat yang mempunyai kewenangan melaksanakan proses pengangkatan, pemindahan, dan pemberhentian Pegawai ASN sesuai dengan ketentuan peraturan perundang-undangan.
6. Kompetensi adalah pengetahuan, keterampilan, dan sikap/perilaku seorang Pegawai ASN yang dapat diamati, diukur, dan dikembangkan dalam melaksanakan tugas jabatannya.
7. Pengembangan Kompetensi Pegawai ASN adalah pengembangan kompetensi yang dilaksanakan bagi PNS dan PPPK.
8. Pengembangan Kompetensi PNS adalah upaya untuk pemenuhan kebutuhan kompetensi PNS dengan standar kompetensi jabatan dan rencana pengembangan karier.
9. Pengembangan Kompetensi PPPK adalah proses peningkatan pengetahuan PPPK untuk mendukung pelaksanaan tugas.
10. Standar Kompetensi Jabatan adalah deskripsi pengetahuan, keterampilan dan perilaku yang diperlukan seorang Pegawai ASN dalam melaksanakan tugas jabatan.
11. Perencanaan Pengembangan Kompetensi Pegawai ASN adalah kegiatan secara sistematis merencanakan pengembangan kompetensi Pegawai ASN dalam jangka waktu tertentu yang dilaksanakan oleh setiap instansi pemerintah.
12. Pelaksanaan Pengembangan Kompetensi Pegawai ASN adalah kegiatan pengembangan kompetensi Pegawai ASN yang dapat dilakukan melalui Pendidikan dan/atau pelatihan.
13. Evaluasi Pengembangan Kompetensi Pegawai ASN adalah kegiatan pemantauan dan penilaian Pelaksanaan Pengembangan Kompetensi Pegawai ASN yang dilakukan oleh PPK pada setiap instansi pemerintah pusat dan daerah.
14. Jam Pelajaran yang selanjutnya disingkat JP adalah 45 (empat puluh lima) menit.
15. Lembaga Administrasi Negara yang selanjutnya disingkat LAN adalah lembaga pemerintah nonkementerian yang diberi kewenangan melakukan pengkajian dan pendidikan dan pelatihan aparatur sipil negara.

## **III. KEBIJAKAN PENYELENGGARAAN**

### **A. Jenis Perencanaan Pengembangan Kompetensi Pegawai ASN**

Jenis Perencanaan Pengembangan Kompetensi Pegawai ASN terdiri

atas beberapa hal sebagai berikut:

1. Perencanaan Pengembangan Kompetensi PNS merupakan proses kegiatan merencanakan Pengembangan Kompetensi PNS dalam jangka waktu 5 (lima) tahunan dan tahunan pada setiap instansi pemerintah pusat dan daerah.
2. Perencanaan Pengembangan Kompetensi PPPK merupakan proses kegiatan merencanakan Pengembangan Kompetensi PPPK dalam jangka waktu tahunan pada setiap instansi pemerintah pusat dan daerah.

#### B. Tingkat Perencanaan Pengembangan Kompetensi Pegawai ASN

Tingkat Perencanaan Pengembangan Kompetensi Pegawai ASN mencakup beberapa hal antara lain:

1. Tingkat Perencanaan Pengembangan Kompetensi Pegawai ASN secara instansional  
Perencanaan Pengembangan Kompetensi Pegawai ASN tingkat instansi dilakukan oleh unit kerja yang mengelola penyelenggaraan urusan di bidang sumber daya manusia (SDM) dengan melakukan rekapitulasi dan validasi perencanaan pengembangan kompetensi individu.
2. Tingkat Perencanaan Pengembangan Kompetensi Pegawai ASN secara nasional
  - a) Perencanaan Pengembangan Kompetensi sebagaimana dimaksud dalam angka 1, disampaikan oleh PyB kepada LAN melalui sistem informasi Pengembangan Kompetensi ASN.
  - b) LAN menjadikan Perencanaan Pengembangan Kompetensi sebagaimana dimaksud pada huruf a sebagai bahan untuk menyusun rencana Pengembangan Kompetensi Pegawai ASN secara nasional.

#### C. Tahapan Perencanaan Pengembangan Kompetensi Pegawai ASN

Tahapan Perencanaan Pengembangan Kompetensi Pegawai ASN terdiri atas beberapa hal sebagai berikut:

1. Input  
Tahapan ini diperlukan dalam proses perencanaan pengembangan kompetensi ASN. Input yang diperlukan paling rendah meliputi beberapa hal sebagai berikut:
  - a) Dokumen perencanaan 5 (lima) tahunan kementerian/lembaga/daerah, menjadi bahan pertimbangan dalam merumuskan pemenuhan kebutuhan kompetensi ASN sesuai prioritas kebijakan instansi;
  - b) Profil Pegawai, yang mencakup jabatan, unit kerja, demografi (usia, pendidikan), riwayat pengembangan kompetensi yang pernah diikuti oleh pegawai. Bagi instansi yang sudah mengimplementasikan manajemen talenta atau telah melaksanakan pola karier, untuk mencantumkan posisi pegawai berdasarkan hasil pemetaan kinerja dan potensi;
  - c) Standar Kompetensi Jabatan, yang penyusunannya mengacu pada peraturan perundang-undangan yang berlaku;
  - d) Data Analisis Kesenjangan Kompetensi, merupakan data yang dihasilkan dari hasil analisis antara profil kompetensi pegawai dengan Standar Kompetensi Jabatan yang memuat tingkat kesenjangan pegawai pada kompetensi tertentu;
  - e) Data Analisis Kinerja ASN, bagi:
    - 1) PNS  
Data analisis kinerja ini merupakan data Kesenjangan Kinerja yang dihasilkan dengan membandingkan hasil penilaian kinerja PNS dengan target kinerja jabatan yang didudukinya.

Data analisis kinerja dapat diperoleh dari sistem penilaian kinerja instansi.

2) PPPK

Data analisis kinerja ini merupakan data yang dihasilkan dari penilaian capaian target kinerja PPPK yang tercantum dalam perjanjian kerja. Data analisis kinerja dapat diperoleh dari sistem penilaian kinerja instansi; dan

f) Anggaran, merupakan alokasi anggaran yang dibutuhkan dalam pelaksanaan Pengembangan Kompetensi Pegawai ASN.

2. Proses

Tahapan ini terdiri atas:

a) Inventarisasi usulan kebutuhan Pengembangan Kompetensi Pegawai ASN bagi:

1) PNS

Tahapan ini merupakan rangkaian kegiatan untuk mengidentifikasi pengembangan kompetensi yang dibutuhkan oleh setiap PNS dalam organisasi yang dilakukan dengan tahapan sebagai berikut:

(a) Atasan langsung melakukan proses dialog berdasarkan data analisis kesenjangan kompetensi dan data kesenjangan kinerja;

(b) Unit kerja jabatan pimpinan tinggi pratama melakukan rekapitulasi terhadap hasil yang disampaikan oleh Atasan langsung

(c) Hasil rekapitulasi diverifikasi oleh:

(1) Pejabat Pimpinan Tinggi Pratama dan Pejabat Pimpinan Tinggi Madya untuk instansi pusat; dan

(2) Pejabat Pimpinan Tinggi Pratama untuk instansi daerah; dan

(d) Hasil inventarisasi kebutuhan kompetensi yang sudah diverifikasi disampaikan kepada unit kerja yang mengelola penyelenggaraan urusan di bidang SDM.

2) PPPK

Tahapan ini merupakan rangkaian kegiatan untuk mengidentifikasi pengembangan kompetensi yang dibutuhkan oleh setiap PPPK dalam organisasi yang dilakukan dengan mekanisme sebagai berikut:

(a) Atasan langsung PPPK mengusulkan kebutuhan pengembangan kompetensi tiap PPPK di unit kerjanya berdasarkan data penilaian kinerja dan kebutuhan pengayaan pengetahuan PPPK dalam rangka mendukung pelaksanaan tugas organisasi; dan

(b) Usulan kebutuhan disampaikan kepada unit kerja yang mengelola penyelenggaraan urusan di bidang SDM untuk dilakukan analisis dan validasi.

b) Validasi usulan kebutuhan Pengembangan Kompetensi Pegawai ASN, bagi:

1) PNS

Unit kerja yang mengelola penyelenggaraan urusan di bidang SDM melakukan validasi kebutuhan Pengembangan Kompetensi PNS, dengan memperhatikan beberapa hal sebagai berikut :

(a) Data profil PNS;

(b) Data hasil analisis kesenjangan kompetensi;

(c) Data hasil analisis kesenjangan kinerja;

(d) Prioritas kebijakan dalam dokumen perencanaan 5 (lima) tahunan kementerian/lembaga/daerah;

- (e) Ketersediaan anggaran Pengembangan Kompetensi PNS; dan
- (f) Pemenuhan 20 (dua puluh) JP Pengembangan Kompetensi PNS per tahun.

Khusus untuk inventarisasi kebutuhan pengembangan PNS Jabatan Pimpinan Tinggi Madya dilakukan secara langsung oleh unit kerja yang mengelola penyelenggaraan urusan di bidang SDM dengan diverifikasi oleh PPK.

2) PPPK

Unit kerja yang mengelola penyelenggaraan urusan di bidang SDM melakukan validasi kebutuhan Pengembangan Kompetensi PPPK, dengan memperhatikan beberapa hal sebagai berikut :

- (a) Data profil PPPK;
- (b) Data hasil penilaian kinerja dan tingkat capaian kinerja PPPK;
- (c) Prioritas kebijakan dalam dokumen perencanaan 5 (lima) tahunan kementerian/lembaga/daerah;
- (d) Ketersediaan anggaran Pengembangan Kompetensi PPPK;
- (e) Pemenuhan JP Pengembangan Kompetensi PPPK pertahun sebagaimana diatur berdasarkan peraturan perundang-undangan; dan
- (f) Ketentuan mengenai penetapan jenis dan jalur pengembangan kompetensi PPPK sebagaimana diatur berdasarkan peraturan perundang-undangan.

c) Menyusun Rencana 5 (Lima) Tahunan Pengembangan Kompetensi PNS

Rencana 5 (Lima) Tahunan ini diperuntukan khusus bagi PNS yang mencakup data mengenai:

- 1) nama pegawai yang akan dikembangkan;
- 2) jenis kompetensi yang perlu dikembangkan;
- 3) jenis dan jalur pengembangan kompetensi; dan
- 4) tahun pelaksanaan.

Rencana Lima Tahunan ini dapat direviu atau disesuaikan kembali untuk disesuaikan dengan kondisi organisasi dan kebutuhan pegawai atau instansi.

d) Menyusun Rencana Tahunan Pengembangan Kompetensi ASN

Rencana Tahunan ini mencakup:

- 1) nama pegawai yang akan dikembangkan;
- 2) jenis kompetensi yang perlu dikembangkan;
- 3) jenis dan jalur pengembangan kompetensi;
- 4) penyelenggara pengembangan kompetensi;
- 5) jadwal dan waktu pelaksanaan;
- 6) anggaran yang dibutuhkan; dan
- 7) jumlah JP.

e) Rencana Pengembangan Kompetensi Pegawai ASN sebagaimana pada huruf c dan huruf d yang telah ditetapkan oleh PPK disampaikan kepada LAN melalui sistem informasi Pengembangan Kompetensi ASN sebagai bahan penyusunan rencana Pengembangan Kompetensi ASN Nasional.

f) Rencana Tahunan Pengembangan Kompetensi ASN sebagaimana dimaksud pada huruf d, disampaikan kepada LAN pada triwulan ketiga tahun anggaran sebelumnya.

D. Pelaksanaan Pengembangan Kompetensi Pegawai ASN

1. Penyelenggaraan Pengembangan Kompetensi Pegawai ASN, terdiri atas:

a) Pelaksanaan Pengembangan Kompetensi melalui jalur pendidikan

yang dilaksanakan sesuai dengan ketentuan yang berlaku.

b) Pelaksanaan Pengembangan Kompetensi melalui jalur pelatihan yang dilaksanakan secara:

1) Mandiri oleh internal

Instansi pemerintah dapat menyelenggarakan pengembangan kompetensi secara mandiri oleh lembaga pelatihan atau unit kerja/lembaga yang ditunjuk untuk mengembangkan kompetensi.

2) Bersama dengan instansi pemerintah yang terakreditasi

Instansi pemerintah dapat melakukan pengembangan kompetensi secara bersama dengan instansi pemerintah lain yang telah diakreditasi oleh LAN untuk melaksanakan pengembangan kompetensi tertentu.

3) Bersama dengan lembaga pengembangan kompetensi yang independen

Instansi pemerintah dapat melakukan pengembangan kompetensi secara bersama dengan lembaga pengembangan kompetensi independen yang telah terakreditasi.

2. Jenis dan Jalur Pengembangan Kompetensi Pegawai ASN

Jenis dan jalur Pengembangan Kompetensi Pegawai ASN terdiri atas:

a) Pendidikan

Jenis Pengembangan Kompetensi ini dilakukan melalui jalur pemberian tugas belajar pada jenjang pendidikan formal tertentu sesuai dengan ketentuan peraturan perundang-undangan.

Mekanisme yang perlu diperhatikan oleh Unit kerja yang mengelola penyelenggaraan urusan di bidang SDM dalam penentuan nama PNS yang akan ditetapkan sebagai peserta pendidikan melalui tugas belajar oleh PPK, harus sesuai dengan rencana pengembangan kompetensi yang telah ditetapkan.

b) Pelatihan

Jenis Pengembangan Kompetensi ini terdiri atas:

1) Pelatihan Klasikal

Jenis pelatihan ini merupakan proses pembelajaran tatap muka di dalam kelas dengan mengacu kurikulum dan dilaksanakan melalui jalur :

- (a) pelatihan kepemimpinan/struktural/manajerial;
- (b) pelatihan untuk tujuan tertentu di tingkat nasional;
- (c) pelatihan teknis;
- (d) pelatihan fungsional;
- (e) pelatihan terkait kompetensi sosial kultural;
- (f) seminar atau konferensi;
- (g) workshop atau lokakarya;
- (h) sarasehan;
- (i) kursus;
- (j) penataran;
- (k) bimbingan teknis;
- (l) sosialisasi; dan
- (m) jalur lain yang memenuhi ketentuan pelatihan klasikal.

2) Pelatihan Nonklasikal

Jenis pelatihan ini merupakan proses praktik kerja dan/atau pembelajaran di luar kelas dan dilaksanakan melalui jalur:

- (a) pertukaran PNS dengan pegawai swasta;
- (b) magang/praktik kerja;
- (c) benchmarking atau study visit;
- (d) pelatihan jarak jauh;
- (e) coaching;
- (f) mentoring;
- (g) detasering;

- (h) penugasan terkait program prioritas;
  - (i) e-learning;
  - (j) belajar mandiri/self development;
  - (k) team building; dan
  - (l) jalur lain yang memenuhi ketentuan pelatihan non klasikal.
3. Monitoring
- a) Seluruh hasil pelaksanaan pengembangan kompetensi yang telah dilakukan ASN di-input oleh unit kerja yang mengelola penyelenggaraan urusan di bidang SDM.
  - b) Unit kerja sebagaimana dimaksud pada huruf a menyampaikan hasil monitoring secara rutin per semester ke LAN melalui sistem informasi Pengembangan Kompetensi ASN.
- E. Evaluasi Pengembangan Kompetensi Pegawai ASN
1. Jenis Evaluasi
    - a) Evaluasi Administratif
      - 1) untuk melihat kesesuaian antara perencanaan dan pelaksanaan Pengembangan Kompetensi ASN.
      - 2) Periode  
Evaluasi administratif disampaikan kepada LAN melalui sistem informasi Pengembangan Kompetensi ASN paling lambat tanggal 31 Januari pada tahun berikutnya.
    - b) Evaluasi Substantif
      - 1) untuk melihat kesesuaian antara pemenuhan kebutuhan kompetensi dengan standar kompetensi jabatan dan pengembangan karir.
      - 2) Periode  
Evaluasi substantif disampaikan ke LAN melalui sistem informasi Pengembangan Kompetensi ASN, paling lambat tanggal 31 Maret pada tahun berikutnya.
  2. Pelaksana Evaluasi
    - a) PPK bertanggung jawab terhadap evaluasi Pengembangan Kompetensi Pegawai ASN.
    - b) Dalam melaksanakan evaluasi, PPK dapat menunjuk pejabat dan/atau membentuk tim sebagai pelaksana evaluasi Pengembangan Kompetensi Pegawai ASN.

#### **IV. STANDAR PENYELENGGARAAN**

##### **A. Strategi peningkatan kapasitas SDM SPBE**

Berdasarkan data ketersediaan dan profil ASN yang memiliki kualifikasi pendidikan komputer pada masing-masing Perangkat Daerah di Kabupaten Jombang dapat diketahui bahwa SDM yang memiliki pendidikan komputer masih sangat kurang. Dari jumlah 62 Perangkat Daerah hanya 21 Perangkat Daerah yang memiliki SDM komputer. Keberadaan SDM juga jumlah tidak merata untuk 21 Perangkat Daerah tersebut.

Peningkatan kapasitas SDM SPBE mencakup upaya untuk menetapkan standar kompetensi teknis SPBE, mengembangkan kompetensi teknis SDM SPBE, mengembangkan pola karir dan remunerasi SDM SPBE agar pembangunan, pengembangan, pengoperasian, dan pemberian layanan SPBE dapat berjalan dengan baik, berkesinambungan, dan memenuhi harapan/kebutuhan pengguna.

Kompetensi dan Pendidikan sebagai syarat minimal pengelolaan SPBE sudah terperinci secara spesifik. Namun demikian tidak berarti bahwa satu keahlian harus dimiliki oleh satu orang tertentu. Kompetensi tersebut dapat dimiliki oleh beberapa orang dan satu orang juga dapat

memiliki lebih dari satu kompetensi. Kebutuhan pengelola SPBE ini tersebut dapat disesuaikan dengan berapa bidang keahlian yang maksimal dapat dikuasai dengan baik oleh seorang ahli informatika atau pranata komputer tersebut. Adapun strategi untuk mencapai peningkatan kapasitas SDM SPBE adalah:

1. mengembangkan jabatan fungsional Pegawai Negeri Sipil (PNS) yang terkait dengan SPBE; dan
2. membangun kemitraan dengan pihak non pemerintah dalam peningkatan kompetensi teknis ASN, penyediaan tenaga ahli, riset, serta pembangunan dan pengembangan SPBE.

#### B. Rencana pelaksanaan manajemen SDM

Rencana pelaksanaan manajemen SDM SPBE melalui pemenuhan kompetensi ASN sebagai pengelola SPBE di masing-masing Perangkat Daerah Tahun 2022 sebagai berikut :

No	RENCANA KEGIATAN	TUJUAN	OUTCOME	JUMLAH	KET
1.	Rekrutmen ASN TIK melalui Formasi CASN Jabatan Pranata Komputer	Memenuhi SDM TIK SPBE Perangkat Daerah	Jabatan Fungsional Pranata Komputer	Sesuai kebutuhan berdasar Anjab	Jangka panjang  Dilaksanakan melalui pengadaan formasi CASN
2.	Pengangkatan PNS dalam Jabatan Fungsional melalui penyesuaian Inpassing	Memenuhi SDM TIK SPBE Perangkat Daerah	Jabatan Fungsional Pranata Komputer	Sesuai jumlah PNS yang telah dan/atau masih menjalankan tugas di bidang TIK	Jangka panjang  Dilaksanakan melalui pengangkatan Jabatan fungsional penyesuaian inpassing
3.	Diklat Komputer - Pengembangan Sistem Informasi Berbasis WEB	Mengembangkan kompetensi dan kemampuan ASN pengelola SPBE Perangkat Daerah di bidang jaringan/ sistem informasi berbasis WEB	Meningkatnya kompetensi dan kemampuan ASN pengelola SPBE Perangkat Daerah di bidang jaringan /sistem informasi berbasis WEB	124 orang terdiri dari 40 mengikuti secara klasikal dan 84 secara virtual /online	Jangka pendek  Dilaksanakan secara klasikal dan secara virtual/online  Tribulan I



4.	Workshop Penguatan Kompetensi SDM TIK SPBE	Memberikan pemahaman dan bekal kompetensi bagi SDM pengelola SPBE di bidang proses bisnis pemerintahan, aplikasi SPBE. Infrastruktur SPBE, data dan informasi, keamanan SPBE, dan Arsitektur SPBE	Pengelola SPBE Perangkat Daerah memahami terkait proses bisnis pemerintahan, aplikasi SPBE. Infrastruktur SPBE, data dan informasi, keamanan SPBE, dan Arsitektur SPBE	124 orang (masing-masing perangkat daerah minimal 2 orang)	Jangka pendek  Dilaksanakan secara virtual/online  Tribulan II
5.	Bimbingan Teknis SPBE	Memberikan kompetensi ASN pengelola SPBE	Pengelola SPBE Perangkat Daerah memenuhi standar kompetensi teknis SPBE	62 orang	Jangka pendek  Dilaksanakan secara klasikal  Tribulan IV (PAK)
6.	Bimtek Pemanfaatan Aplikasi Srikandi				Jangka pendek  Dilaksanakan secara klasikal  Tribulan IV (PAK)

**BAB VI**  
**PEDOMAN MANAJEMEN PENGETAHUAN**  
**SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK**

**I. PENDAHULUAN**

Pengetahuan atau knowledge merupakan informasi yang dapat digunakan untuk membuat keputusan atau mengambil tindakan yang diperlukan. Dengan demikian pengetahuan di dalam organisasi sangatlah penting karena menentukan kualitas tindakan dan keputusan yang diambil, yang dapat mempengaruhi kinerja, daya saing, bahkan keberlangsungan dari organisasi. Agar terhindar dari kerugian yang dapat dialami oleh organisasi, karena sulitnya pengambilan keputusan atau pelaksanaan tindakan sebagai akibat dari tidak tersedianya pengetahuan yang diperlukan, maka pengetahuan di dalam organisasi haruslah dikelola dengan baik.

Peran pegawai dalam konteks pengambilan keputusan berbasis pengetahuan sangatlah penting, mengingat pengetahuan organisasi dapat berasal dari individu maupun sekelompok pegawai. Pegawai merupakan modal yang menjadi salah satu komponen utama dari intangible asset serta strategic partner bagi organisasi. Di lain pihak, setiap pegawai cepat atau lambat pasti akan meninggalkan organisasi, atau bermutasi ke unit kerja lain. Oleh karena itu, sangatlah penting untuk tetap menjaga agar pengetahuan yang dimiliki tetap menjadi aset organisasi, untuk dapat dimanfaatkan selanjutnya oleh pegawai lain atau oleh organisasi tersebut di masa datang.

Instansi pemerintahan sebagaimana organisasi lainnya dituntut untuk senantiasa meningkatkan kinerjanya. Dengan perkembangan teknologi informasi dan komunikasi (TIK) saat ini, pemanfaatan TIK dalam pemerintahan melalui Sistem Pemerintahan Berbasis Elektronik (SPBE) pun terus meningkat. SPBE diharapkan dapat memberi peluang untuk mendorong dan mewujudkan penyelenggaraan pemerintahan yang terbuka, partisipatif, inovatif, dan akuntabel; meningkatkan kolaborasi antar instansi pemerintah dalam melaksanakan urusan dan tugas pemerintahan untuk mencapai tujuan bersama; meningkatkan kualitas dan jangkauan pelayanan publik kepada masyarakat luas; dan menekan tingkat penyalahgunaan kewenangan dalam bentuk kolusi, korupsi, dan nepotisme. Mengingat kompleksitas dari SPBE, untuk meningkatkan keterpaduan dan efisiensi SPBE yang digunakan oleh Pemerintah Kabupaten Jombang, diperlukan tata kelola dan manajemen SPBE.

Manajemen Pengetahuan dalam SPBE diharapkan dapat mengurangi duplikasi upaya dalam mendapatkan suatu pengetahuan yang diperlukan untuk mengambil keputusan, mengurangi biaya dan waktu operasional layanan SPBE, dan meningkatkan kompetensi operator SPBE. Selain itu dengan manajemen pengetahuan yang baik, diharapkan pegawai dan organisasi pemerintahan dapat diberdayakan, yang pada akhirnya dapat meningkatkan kinerja dan kualitas layanan SPBE.

Tujuan dari Manajemen Pengetahuan SPBE adalah untuk meningkatkan kualitas layanan SPBE; dan meningkatnya kualitas pengambilan keputusan dalam SPBE melalui penerapan Manajemen Pengetahuan (mendukung proses pengambilan keputusan dalam SPBE). Adapun manfaat yang diharapkan dari penerapan Manajemen Pengetahuan SPBE di lingkungan Pemerintah Kabupaten Jombang adalah meningkatnya kinerja individu dan instansi pemerintahan, meningkatnya efisiensi dari pemanfaatan sumber daya pengetahuan di instansi dan meningkatnya ketahanan serta keberlanjutan proses bisnis dalam Sistem Pemerintahan Berbasis Elektronik.

## II. DEFINISI

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. Pengguna SPBE adalah Instansi Pusat, Pemerintah Daerah, pegawai Aparatur Sipil Negara, perorangan, masyarakat, pelaku usaha, dan pihak lain yang memanfaatkan layanan SPBE..
3. Pengetahuan atau knowledge adalah pemahaman yang dimiliki oleh seseorang mengenai sesuatu hal, yang didapat dari pengalaman (experience) dan atau proses pembelajaran (education). Pemahaman tersebut selanjutnya dapat digunakan sebagai dasar dalam membuat keputusan atau melakukan tindakan yang dibutuhkan.
4. Manajemen pengetahuan adalah upaya terstruktur dan sistematis dalam mengembangkan dan menggunakan pengetahuan yang dimiliki untuk membantu proses pengambilan keputusan bagi peningkatan kinerja organisasi. Aktivitas dalam manajemen pengetahuan meliputi upaya perolehan, penyimpanan, pengolahan dan pengambilan kembali, penggunaan dan penyebaran, serta evaluasi dan penyempurnaan terhadap pengetahuan sebagai aset intelektual organisasi.
5. Manajemen Pengetahuan SPBE adalah serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam SPBE.

## III. KEBIJAKAN PENYELENGGARAAN

### A. Prinsip Manajemen Pengetahuan SPBE

Prinsip utama dalam penerapan Manajemen Pengetahuan SPBE di lingkungan Pemerintah Kabupaten Jombang adalah:

1. Berorientasi pada penerapan SPBE yang sesuai dengan visi dan misi instansi pemerintahan;
2. Merupakan bagian dari proses pengambilan keputusan dengan memanfaatkan pengetahuan terbaik yang dikelola;
3. Memperhatikan faktor manusia, proses bisnis, teknologi, dan budaya organisasi;
4. Berorientasi pada proses pengumpulan, pengelolaan dan bagi pakai pengetahuan dalam SPBE;
5. Bersifat transparan, inklusif, sistematis, terstruktur, dan tepat waktu;
6. Mengutamakan efektivitas, keterpaduan, kesinambungan, efisiensi, akuntabilitas, interoperabilitas dan keamanan;
7. Bersifat dinamis, berulang atau iteratif, tanggap akan perubahan dan merupakan upaya perbaikan secara terus menerus.

### B. Kerangka Kerja Manajemen Pengetahuan SPBE

Kerangka kerja Manajemen Pengetahuan bertujuan untuk membantu Pemerintah Kabupaten Jombang dalam mengintegrasikan Manajemen Pengetahuan SPBE dalam kegiatan dan pelaksanaan tugas dan fungsinya, yang selanjutnya dapat dikembangkan dan disesuaikan dengan karakteristik Pemerintah Kabupaten Jombang.

Adapun komponen dasar kerangka kerja Manajemen Pengetahuan SPBE dalam rangka mewujudkan pengelolaan pengetahuan SPBE, terdiri dari 3 komponen utama yaitu:

1. Pembangunan Budaya Berbagi dan Meningkatkan Pengetahuan SPBE

Pembangunan budaya yang mendukung pencapaian tujuan manajemen pengetahuan SPBE harus dibangun dan dikembangkan dengan menyesuaikan dengan nilai-nilai budaya di Pemerintah Kabupaten Jombang.

Budaya sadar berbagi menjadi hal utama dalam pengelolaan pengetahuan SPBE di Pemerintah Kabupaten Jombang, mengingat pengetahuan yang dimiliki oleh individu atau sekelompok individu harus dapat dimanfaatkan bersama untuk kepentingan organisasi.

Budaya meningkatkan pengetahuan SPBE perlu dibangun untuk mendorong pola pikir yang berorientasi pada pemecahan masalah, pembangunan kompetensi individu dan peningkatan kinerja organisasi yang dibutuhkan oleh instansi pemerintah.

Untuk itu membangun suatu lingkungan yang kondusif untuk mendorong terciptanya budaya berbagi dan meningkatkan pengetahuan SPBE di Pemerintah Kabupaten Jombang, diperlukan kepemimpinan digital yang memiliki komitmen dalam mengelola pengetahuan, mampu memberi arahan kebijakan yang jelas dan mudah dipahami, serta memberi dukungan secara konsisten dalam memanfaatkan teknologi informasi untuk meningkatkan pengetahuan organisasi terkait SPBE, membangun trust dan mendorong pola pikir serta budaya kerja yang kolaboratif dan inovatif.

Kebijakan mengenai prinsip, proses, dan penugasan secara formal sangat penting untuk memastikan keberhasilan manajemen pengetahuan SPBE di instansi pemerintah. Selain itu, untuk mendorong penerapan manajemen pengetahuan SPBE, perlu dibangun sistem penghargaan terhadap kontribusi ASN dalam pembangunan basis pengetahuan SPBE, baik dalam berbagi pengetahuan maupun berpartisipasi dalam memecahkan masalah dan menciptakan pengetahuan-pengetahuan baru SPBE.

## 2. Penyelenggaraan Proses Bisnis Manajemen Pengetahuan SPBE

Proses Bisnis Manajemen Pengetahuan SPBE dapat diterapkan dengan berpedoman pada siklus generik manajemen pada umumnya, yang mencakup perencanaan, pelaksanaan, pemantauan evaluasi dan perbaikan, dan secara khusus memenuhi siklus manajemen pengetahuan (knowledge management life cycle).

Sesuai Peraturan Presiden Nomor 95 tahun 2018 tentang SPBE, proses Manajemen Pengetahuan SPBE terdiri dari proses Pengumpulan, Pengolahan, Penyimpanan, Penggunaan, dan Alih Pengetahuan dan Teknologi.

Proses Manajemen Pengetahuan SPBE harus menjadi bagian yang terpadu dengan proses manajemen secara keseluruhan, menyatu dalam budaya, dan disesuaikan dengan proses bisnis organisasi di lingkup Pemerintah Kabupaten Jombang.

Penggunaan teknologi dan sistem informasi manajemen pengetahuan SPBE yang terpusat dan terintegrasi menjadi sarana penting dalam mendukung terselenggarakannya proses pengelolaan pengetahuan SPBE di lingkungan Pemerintah Kabupaten Jombang secara efektif dan efisien.

## 3. Pembentukan Struktur Pengelola Manajemen Pengetahuan SPBE

Struktur Manajemen Pengetahuan SPBE di lingkungan Pemerintah Kabupaten Jombang harus dibentuk dan ditetapkan dalam rangka memastikan penugasan yang jelas dalam pelaksanaan manajemen pengetahuan SPBE sesuai siklus proses manajemen pada umumnya dari perencanaan, pelaksanaan, pemantauan pengendalian, sampai dengan tindakan perbaikan secara berkelanjutan.

Untuk keterpaduan, struktur pengelola manajemen pengetahuan SPBE harus menjadi bagian yang integral dalam tim koordinasi SPBE di Pemerintah Kabupaten Jombang.

## C. Ekosistem Manajemen Pengetahuan SPBE

Ekosistem Manajemen Pengetahuan SPBE merupakan suatu

tatanan utuh yang memungkinkan tumbuh dan berkembangnya pengetahuan SPBE yang berguna bagi berbagai pihak yang berkepentingan. Ekosistem terdiri dari berbagai komponen atau sub-sistem yang saling berinteraksi satu sama lain, dan dengan lingkungan sekitarnya.

Komponen pelaku dalam ekosistem manajemen pengetahuan SPBE, secara garis besar dapat dikelompokkan sebagai berikut.

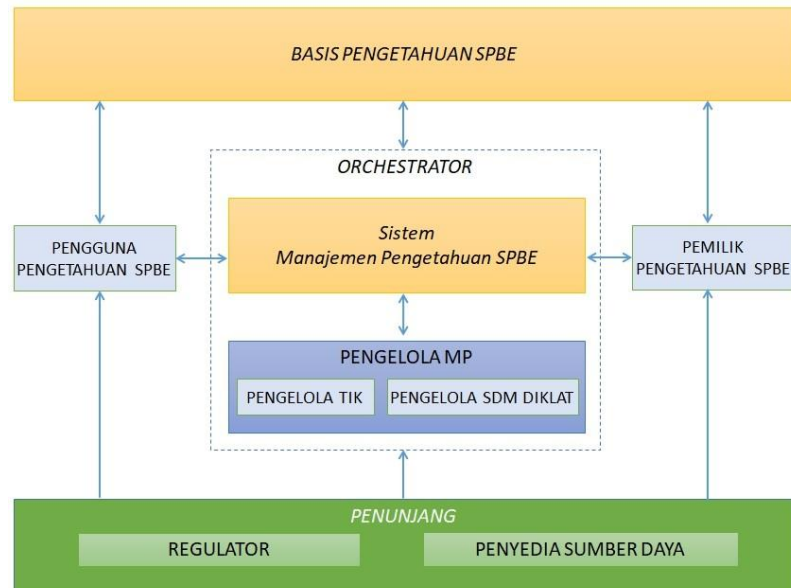
1. Pelaksana, yang terdiri dari
  - a) Pemilik pengetahuan SPBE, yang dapat berupa individu maupun organisasi.
  - b) Pengguna pengetahuan SPBE, yang dapat berasal dari internal organisasi, maupun eksternal organisasi.
  - c) Pengelola proses manajemen pengetahuan SPBE, adalah pengelola di tingkat Pemerintah Kabupaten Jombang. Pengelola proses manajemen pengetahuan SPBE, selain membangun basis pengetahuan SPBE, juga bertugas sebagai orchestrator yang mendorong interaksi dan kolaborasi, untuk menjembatani kebutuhan pengetahuan antara pemilik dan pengguna pengetahuan.
  - d) Penyedia teknologi untuk mendukung penerapan manajemen pengetahuan, yang antara lain terdiri dari
    - (1) Pengelola Knowledge base atau basis pengetahuan SPBE, yang menyediakan dan memelihara basis pengetahuan SPBE untuk dapat diakses dan digunakan oleh penggunanya, dan/atau
    - (2) Pengelola alat bantu aplikasi manajemen pengetahuan SPBE, antara lain yang bertugas mengelola dan menyediakan alat bantu untuk mendukung proses-proses manajemen pengetahuan, seperti aplikasi untuk mencari pengetahuan SPBE yang dibutuhkan, berbagi pengetahuan SPBE, penciptaan pengetahuan baru SPBE, dan sebagainya.
  - e) Pengelola kompetensi sumber daya manusia, yang berkepentingan dalam melakukan pengembangan kompetensi individu khususnya untuk pendidikan dan pelatihan dalam Instansi Pemerintah.

Suatu instansi pemerintah, unit kerja maupun individu tertentu, dapat berperan sebagai pemilik maupun pengguna pengetahuan SPBE, tergantung pada konteks dari pengetahuan SPBE terkait.

2. Pendukung, yang terdiri dari
  - a) Pengelola kebijakan (regulator), dalam hal ini,
    - (1) Penentu kebijakan dan peraturan terkait penerapan manajemen pengetahuan SPBE; serta
    - (2) Pengawas, yang mengawasi jalannya aktivitas atau proses manajemen pengetahuan agar sesuai dengan kebijakan yang ditetapkan.
  - b) Penyedia sumber daya, termasuk dalam hal ini, sumber daya anggaran, sumber daya fasilitas, serta sumber daya organisasi lainnya di Instansi Pemerintah.

Komponen pelaku tersebut di atas berinteraksi dalam suatu ekosistem Manajemen Pengetahuan SPBE, yang ditunjang antara lain dengan nilai-nilai, prinsip, kebijakan, struktur organisasi, proses, sumber daya, sarana dan prasarana yang mendukung fungsi dan tumbuh-kembangnya ekosistem menjadi semakin baik dan bermanfaat.

Secara garis besar ekosistem Manajemen Pengetahuan SPBE dapat digambarkan sebagai berikut



#### D. Proses Manajemen Pengetahuan Spbe

Proses-proses dalam siklus manajemen pengetahuan sesuai Peraturan Presiden Nomor 95 tahun 2018 tentang SPBE dapat dijabarkan sebagai berikut.

##### 1. Proses Pengumpulan

Pengetahuan terkait SPBE yang biasanya tersebar di instansi pemerintahan, perlu dikumpulkan, untuk selanjutnya dapat disimpan dan dirawat dengan baik. Proses pengumpulan dalam manajemen pengetahuan SPBE perlu dilakukan secara terencana sesuai kebutuhan SPBE.

##### 2. Proses Pengolahan

Pengetahuan SPBE yang telah dikumpulkan perlu diolah, disusun dan diatur dengan baik, untuk memudahkan perawatan serta penggunaannya.

##### 3. Proses Penyimpanan

Pengetahuan SPBE perlu disimpan dalam suatu tempat penyimpanan, yang memungkinkan pemeliharaan pengetahuan tersebut dalam berbagai bentuk representasi pengetahuan.

##### 4. Proses Penggunaan

Pengetahuan SPBE yang telah disimpan, harus senantiasa tersedia dan dapat ditemui, diakses serta digunakan kembali oleh berbagai pihak sesuai tujuan dan kebutuhannya.

##### 5. Proses Alih Pengetahuan dan Teknologi

Proses alih pengetahuan dan teknologi terkait SPBE bertujuan untuk memastikan bahwa pengetahuan SPBE dapat dikuasai oleh pihak-pihak yang membutuhkannya dalam rangka pencapaian tujuan SPBE

#### IV. STANDAR PENYELENGGARAAN

Dalam pelaksanaan penerapan manajemen pengetahuan SPBE di Pemerintah Kabupaten Jombang perlu disiapkan strategi serta tahapan yang perlu dilakukan agar manajemen pengetahuan SPBE dapat berjalan dengan baik. Strategi atau tahapan tersebut meliputi pembentukan organisasi, proses perencanaan, proses pelaksanaan, serta pemantauan dan evaluasi.

##### A. Penyiapan Pengelolaan

Manajemen Pengetahuan SPBE perlu diterapkan di semua tingkat di lingkungan Pemerintah Kabupaten Jombang. Dalam menerapkan Manajemen Pengetahuan SPBE perlu penetapan bentuk organisasi yang bertanggung-jawab serta berwenang dalam pelaksanaan manajemen

pengetahuan SPBE di lingkungan instansi pemerintah, yang meliputi pembentukan struktur pelaksana, penyiapan sumber daya, serta penetapan kebijakan internal terkait penerapan Manajemen Pengetahuan SPBE.

#### 1. Struktur Manajemen Pengetahuan SPBE.

Struktur Manajemen Pengetahuan SPBE di Pemerintah Kabupaten Jombang, secara garis besar terdiri dari 2 (dua) komponen utama yaitu:

##### a) Komite Pengarah Manajemen Pengetahuan SPBE;

Komite Pengarah terdiri dari pimpinan yang bertugas dan bertanggung jawab untuk:

- 1) Menetapkan kebijakan penerapan Manajemen Pengetahuan SPBE;
- 2) Memberikan arahan dalam penerapan Manajemen Pengetahuan SPBE;
- 3) Mengawasi pelaksanaan Manajemen Pengetahuan SPBE di lingkungan Pemerintah Kabupaten Jombang.

Komite Pengarah Manajemen Pengetahuan, sebaiknya terintegrasi dalam Koordinator SPBE di tingkat instansi, dan berperan aktif dalam memberikan arahan dan kebijakan terkait manajemen pengetahuan SPBE, seperti penentuan konteks pengelolaan pengetahuan SPBE di lingkungannya, terlibat langsung dalam perencanaan dan pengendalian manajemen pengetahuan SPBE, maupun terlibat aktif dalam mendorong budaya kerja yang kondusif dalam membangun dan meningkatkan pengetahuan SPBE

##### b) Pelaksana Manajemen Pengetahuan SPBE.

Pelaksana Manajemen Pengetahuan SPBE bertugas dan bertanggung-jawab dalam:

- 1) Melakukan koordinasi dalam perencanaan dan evaluasi Manajemen Pengetahuan SPBE, dengan
  - (a) Menyiapkan instrumen kebijakan yang dibutuhkan dalam pelaksanaan manajemen pengetahuan, antara lain,
    - (1) Pedoman pelaksanaan Manajemen Pengetahuan SPBE
    - (2) Rencana kerja Manajemen Pengetahuan SPBE,
    - (3) Prosedur kerja yang dibutuhkan dalam pelaksanaan Manajemen Pengetahuan SPBE;
  - (b) Melakukan koordinasi dalam melakukan pengukuran, pemantauan dan evaluasi manajemen pengetahuan;
  - (c) Melakukan koordinasi dalam pelatihan yang diperlukan dalam implementasi manajemen pengetahuan SPBE.
- 2) Melakukan koordinasi dalam identifikasi, pengumpulan, pengolahan, penggunaan serta proses alih pengetahuan dan teknologi SPBE dalam instansi, antara lain dengan
  - (a) Melakukan analisis kesesuaian konten pengetahuan yang dikumpulkan;
  - (b) Mendorong interaksi dan komunikasi antara pemilik dan pengguna pengetahuan, baik di dalam instansi maupun antar instansi;
  - (c) Membentuk Komunitas Praktisi SPBE.
- 3) Melakukan koordinasi dalam penyediaan fasilitas teknologi untuk Manajemen Pengetahuan SPBE, dengan
  - (a) Memastikan tersedianya layanan aplikasi sistem manajemen pengetahuan SPBE untuk instansi;
  - (b) Melakukan pengelolaan teknis terhadap tools / alat bantu sistem manajemen pengetahuan;
  - (c) Berkoordinasi dengan pengelola teknis Sistem Manajemen Pengetahuan SPBE di tingkat Pusat.

Struktur Manajemen Pengetahuan SPBE dapat berupa kelompok kerja yang menjalankan tugas tambahan terkait penyelenggaraan SPBE di instansi, namun hendaknya pelaksanaan Manajemen Pengetahuan SPBE menjadi bagian yang melekat pada tugas dan fungsi suatu unit kerja tertentu dan/atau beberapa unit kerja terkait di lingkup Pemerintah Kabupaten Jombang. Unit kerja pelaksana Manajemen Pengetahuan SPBE dapat berbeda satu sama lain, bergantung pada karakteristik di lingkup Pemerintah Kabupaten Jombang.

Dalam membangun basis pengetahuan SPBE, pelaksana dapat mendorong interaksi dan komunikasi antara pemilik dan pengguna pengetahuan SPBE melalui pembentukan berbagai kelompok Komunitas Praktisi SPBE (Community of Practices) sesuai ruang lingkup pengetahuan SPBE yang dibangun.

Masing-masing Komunitas Praktisi SPBE yang dibentuk, memiliki karakteristik sebagai berikut,

- a) Komunitas Praktisi SPBE merupakan suatu kelompok individu yang memiliki minat, kebutuhan serta penugasan untuk memberikan kontribusi dalam mengembangkan pengetahuan di suatu lingkup atau bidang SPBE tertentu.
- b) Komunitas Praktisi SPBE saling berbagi pengetahuan dan berdiskusi dalam suatu Forum yang membahas berbagai topik tertentu sesuai lingkup atau bidangnya.
- c) Komunitas Praktisi SPBE memiliki pengelola komunitas dan anggota komunitas sebagai partisipan, dan didukung oleh pakar atau ahli di bidang tertentu.
- d) Komunitas Praktisi SPBE memiliki tujuan dan rencana aktivitas dengan target yang terukur.

## 2. Penyiapan Sumber Daya.

Sumber daya merupakan faktor penting agar suatu organisasi dapat menjalankan fungsinya secara teratur dan benar sesuai dengan peraturan yang telah ditetapkan. Dalam hal sumber daya, organisasi harus menentukan dan menyediakan sumber daya seperti sumber daya manusia (SDM), sarana prasarana teknologi, serta anggaran yang diperlukan untuk mendukung pembentukan, implementasi, pemeliharaan, pengukuran, pelaporan dan peningkatan berkelanjutan dari sistem manajemen pengetahuan.

Tugas pelaksana Manajemen Pengetahuan SPBE di lingkup Pemerintah Kabupaten Jombang untuk menyiapkan rencana kebutuhan dan alokasi sumber daya dalam mendukung pelaksanaan Manajemen Pengetahuan di Kabupaten Jombang. Bupati bertugas mengarahkan dan memfasilitasi ketersediaan kebutuhan sumber daya yang dibutuhkan, untuk keberhasilan pencapaian Manajemen Pengetahuan SPBE sesuai dengan prioritas di Kabupaten Jombang.

Ketersediaan SDM dalam mendukung proses pelaksanaan Manajemen Pengetahuan adalah hal yang sangat penting, dengan demikian Pemerintah Kabupaten Jombang perlu mengidentifikasi kompetensi dan keterampilan yang dibutuhkan dalam mengimplementasikan Manajemen Pengetahuan SPBE di Kabupaten Jombang, termasuk kebutuhan sosialisasi, pelatihan, sampai dengan fasilitasi forum diskusi dalam rangka implementasi Manajemen Pengetahuan SPBE di instansi. Kebutuhan sumber daya manusia dalam implementasi Manajemen Pengetahuan, antara lain berupa

- a) Chief Knowledge Officer (CKO), adalah individu yang memiliki visi serta digital leadership yang diperlukan dalam memberikan arahan strategis dan mendorong inisiatif pelaksanaan Manajemen Pengetahuan SPBE di Kabupaten Jombang. CKO dapat



diperankan oleh Koordinator SPBE atau minimal Ketua Komite Pengarah Manajemen Pengetahuan SPBE di Instansi Pemerintah.

- b) Knowledge Managers, adalah individu-individu yang memiliki kemampuan dan pemahaman tentang strategi implementasi Manajemen Pengetahuan, yang diperlukan untuk dapat merintis, menginisiasi, dan mengawasi berjalannya kegiatan Manajemen Pengetahuan SPBE di Kabupaten Jombang.
- c) Knowledge Analyst, adalah individu-individu yang memiliki kemampuan antara lain dalam,
  - 1) menganalisa kebutuhan dan mengetahui lokasi pengetahuan,
  - 2) melakukan kodifikasi pengetahuan,
  - 3) mengelola bentuk dan representasi pengetahuan, serta menjaga kemutakhirannya.

Knowledge Analyst merupakan bagian dari Pelaksana Manajemen Pengetahuan di Instansi Pemerintah.

- d) Knowledge Systems Engineer, adalah individu-individu yang memiliki kemampuan dalam menyediakan dan mengelola solusi aplikasi pendukung penerapan Manajemen Pengetahuan SPBE. Knowledge Systems Engineer merupakan bagian dari Pelaksana Manajemen Pengetahuan di Instansi Pemerintah.
- e) Knowledge Champions, adalah individu-individu yang memiliki wawasan yang lebih dan sebagai teladan untuk mendorong keterlibatan seluruh Knowledge Workers, dalam membangun basis pengetahuan dan bagi pakai pengetahuan SPBE di Instansi Pemerintah. Knowledge Champions merupakan bagian dari Pelaksana Manajemen Pengetahuan di Instansi Pemerintah, dan secara khusus menjadi penggerak komunitas praktisi di bidang tertentu.

Dalam rangka pengembangan kompetensi tersebut, beberapa pelatihan yang dibutuhkan antara lain terkait pemahaman manajemen pengetahuan (knowledge management awareness), sampai dengan pelatihan teknik dan alat bantu yang dibutuhkan dalam Manajemen Pengetahuan SPBE. Ketersediaan sarana dan prasarana teknologi dibutuhkan dalam mendukung proses Manajemen Pengetahuan SPBE harus memenuhi prinsip-prinsip SPBE antara lain mengutamakan penggunaan kode sumber terbuka (Open Source Software) dan interoperabilitas antar sistem. Ketersediaan anggaran yang dibutuhkan dalam implementasi Manajemen Pengetahuan SPBE di instansi sangatlah penting, dan perlu dikelola sesuai peraturan yang berlaku dengan mengutamakan efektivitas, keterpaduan dan efisiensi.

### 3. Penetapan Kebijakan Internal.

Kebijakan internal merupakan mekanisme supaya organisasi Manajemen Pengetahuan dapat memperoleh alokasi sumber daya yang dibutuhkan dan dapat berjalan sesuai dengan tujuannya, sehingga pengetahuan SPBE yang diperlukan oleh institusi dapat tersedia secara tepat sasaran pada waktu yang dibutuhkan. Kebijakan internal untuk Manajemen Pengetahuan SPBE pada tiap institusi dapat berbeda karena bergantung pada peraturan dan kebijakan internal yang telah ditetapkan institusi tersebut.

Kebijakan internal yang dibutuhkan adalah dan tidak terbatas pada hal-hal berikut ini,

- a) Kebijakan terkait pengembangan dan pemeliharaan Pengetahuan terkait SPBE,
- b) Penetapan organisasi pelaksana Manajemen Pengetahuan SPBE, misalnya dalam bentuk peraturan, keputusan atau sejenisnya,

- c) Penetapan personil pelaksana Manajemen Pengetahuan SPBE, misalnya dalam bentuk surat penugasan atau sejenisnya,
- d) Pedoman pelaksanaan Manajemen Pengetahuan SPBE, misalnya dalam bentuk dokumen acuan kegiatan, tata cara pelaksanaan, prosedur kerja, atau sejenisnya, yang antara lain memuat,
  - 1) arah kebijakan internal,
  - 2) tujuan penerapan,
  - 3) pihak-pihak yang berkepentingan,
  - 4) strategi pelaksanaan, dan
  - 5) sumber daya yang dibutuhkan dalam penerapan Manajemen Pengetahuan SPBE di Instansi Pemerintah.

## B. Proses Perencanaan

Perencanaan Manajemen Pengetahuan SPBE merupakan bagian dalam perencanaan SPBE di lingkungan Pemerintah Kabupaten Jombang, yang meliputi antara lain penentuan ruang lingkup dan identifikasi pengetahuan SPBE yang dikelola, yang menjadi dasar dalam penyusunan rencana strategis, peta rencana, serta rencana kegiatan dalam melaksanakan Manajemen Pengetahuan SPBE.

### 1. Penentuan Ruang Lingkup Manajemen Pengetahuan SPBE

Ruang lingkup pengetahuan SPBE yang perlu dikelola, pada hakikatnya meliputi seluruh aspek dalam SPBE. Namun dalam penerapannya, dapat dilakukan secara bertahap. Sebagai contoh, ruang lingkup Manajemen Pengetahuan SPBE dapat dikelompokkan sesuai muatan dalam peta rencana Sistem Pemerintahan Berbasis Elektronik, antara lain tata kelola SPBE, manajemen SPBE, layanan SPBE, infrastruktur, aplikasi, keamanan informasi dan audit TIK. Ruang lingkup Manajemen Pengetahuan SPBE ini selanjutnya dapat dievaluasi sesuai perkembangan SPBE pada umumnya dan penerapan Manajemen Pengetahuan SPBE pada khususnya.

### 2. Identifikasi Kebutuhan Pengetahuan SPBE

Identifikasi pengetahuan SPBE merupakan hal penting yang perlu dilakukan dalam tahap awal perencanaan Manajemen Pengetahuan SPBE di Pemerintah Kabupaten Jombang. Dalam tahap ini, dilakukan identifikasi pengetahuan-pengetahuan apa saja yang telah dimiliki, ataupun yang belum dimiliki, dan yang diperlukan oleh institusi untuk menunjang pemanfaatan dan pencapaian tujuan SPBE.

Pengetahuan tentang SPBE yang dibutuhkan oleh Pemerintah Kabupaten Jombang dapat berbentuk tacit atau pengetahuan yang masih berada dalam pemikiran seseorang yang didapat dari pemahaman atau pengalaman terkait SPBE; maupun telah berbentuk explicit yang telah direkam atau didokumentasikan ke dalam suatu bentuk yang dapat diakses dan dipahami oleh orang lain.

Dengan melakukan identifikasi kebutuhan pengetahuan SPBE, diharapkan dapat ditelusuri dan diketahui lokus praktek, entitas atau unit kerja, serta individu yang membutuhkan, mampu menciptakan atau memiliki pengetahuan SPBE yang perlu dikelola. Individu pemilik pengetahuan dapat berupa para ahli atau pakar praktisi dalam organisasi. Hal penting dalam melakukan identifikasi pengetahuan adalah menentukan pengetahuan SPBE yang bersifat kritical atau sangat dibutuhkan oleh instansi, dan melakukan prioritas dalam upaya pengelolaannya.

## C. Proses Pelaksanaan

Dalam pelaksanaan implementasi manajemen pengetahuan SPBE

terdapat langkah-langkah sebagai berikut :

### 1. Proses Pengumpulan

Pengetahuan terkait SPBE baik yang bersifat konseptual, operasional/prosedural sampai dengan permasalahan SPBE, perlu dikumpulkan untuk kemudian disimpan, dikelola dan dirawat dalam bentuk atau media yang memberikan kemudahan dalam pencarian, penyebaran dan penggunaannya kembali. Proses pengumpulan pengetahuan baru terkait SPBE dapat dilakukan di seluruh lini proses bisnis di instansi pemerintahan, untuk kemudian diletakkan dalam suatu repository atau tempat penyimpanan yang disebut basis pengetahuan (knowledge base) SPBE dalam bentuk terpusat.

Proses pengumpulan pengetahuan SPBE dapat dilaksanakan dalam berbagai cara, antara lain sebagai berikut.

#### a) Proses pengumpulan pengetahuan secara formal

Proses ini dapat berupa proses atau prosedur kerja sehari-hari yang terintegrasi dalam proses pencatatan atau dokumentasi, misalnya yang terkait pengoperasian, pelayanan sampai dengan pengembangan SPBE. Sebagai contoh, pencatatan penanganan insiden atau permasalahan sistem oleh petugas pelayanan SPBE, dokumentasi pengembangan sistem, atau dokumentasi hasil rapat yang menghasilkan keputusan pemecahan masalah. Proses pengumpulan jenis ini sangat bergantung dari kematangan proses terkait di dalam organisasi;

#### b) Proses pengumpulan pengetahuan yang terjadi secara informal

Proses ini biasanya bersifat sukarela, melalui diskusi, konsultasi atau tanya jawab permasalahan dengan praktisi atau pakar terkait. Hal ini dapat difasilitasi oleh sistem manajemen pengetahuan, misalnya melalui fasilitas Forum Diskusi SPBE untuk mendorong pengumpulan serta penciptaan pengetahuan SPBE yang dibutuhkan. Proses pengumpulan pengetahuan SPBE dapat merupakan tahap lanjut dari proses pengelolaan data dan informasi di instansi pemerintah, oleh sebab itu proses pengumpulan pengetahuan sebaiknya difasilitasi sejak awal.

Pengumpulan pengetahuan dapat distimulasi sejak pengetahuan masih berbentuk intangible, antara lain dengan cara berdiskusi dengan berbagai pihak yang memiliki pengetahuan tertentu. Selama proses diskusi, informasi yang dipertukarkan diharapkan dapat menstimulir penciptaan pengetahuan baru terkait topik diskusi.

Pengetahuan SPBE harus diubah dari bentuk intangible, tacit atau masih berupa data, informasi atau pemahaman yang tidak terstruktur atau belum didefinisikan dalam bahasa formal; menjadi pengetahuan yang berbentuk tangible dan explicit. Dengan kata lain pengetahuan yang dikumpulkan harus dicatat, diartikulasi, dan direpresentasikan dengan baik, agar dapat diserap dan digunakan kembali.

### 2. Proses Pengolahan

Pengolahan pengetahuan, dapat pula dilakukan terhadap pengetahuan lama yang telah ada, yang diolah, dimodifikasi atau dibentuk menjadi pengetahuan baru. Representasi pengetahuan SPBE yang baik sangat penting agar dapat dipahami oleh orang lain, serta dapat menjamin pemanfaatan kembali pengetahuan tersebut dalam mendukung pengambilan keputusan dan melakukan tindakan dalam SPBE.

Pengetahuan eksplisit SPBE yang dikumpulkan dalam basis pengetahuan (knowledge base), perlu dikodifikasi, disusun (organize), serta dilengkapi dengan metadata pengetahuan, untuk memudahkan

pencarian dan penggunaannya kembali. Dengan perkembangan teknologi saat ini hal tersebut dapat dilakukan dengan dukungan alat bantu sistem informasi manajemen pengetahuan untuk memudahkan pengolahan pengetahuan SPBE. Pengolahan pengetahuan SPBE dalam instansi pemerintah dapat dilakukan oleh pihak-pihak yang ditunjuk, sesuai dengan bidang kepakaran atau tugas pokok dan fungsi SPBE terkait yang diembannya.

### 3. Proses Penyimpanan

Pengetahuan SPBE memerlukan suatu tempat penyimpanan (knowledge base repository). Tempat dan struktur penyimpanan pengetahuan SPBE tersebut perlu didesain sedemikian rupa sehingga memenuhi kebutuhan, baik dari sisi kapasitas, fungsionalitas penyimpanan, maupun dari kebutuhan ketepatan dan kecepatan (performansi) saat pencarian dan pengaksesan pengetahuan di tempat penyimpanan pengetahuan.

Perkembangan teknologi saat ini memungkinkan penyimpanan media pengetahuan secara elektronik yang tidak terbatas pada bentuk tulisan (text), tetapi juga bentuk gambar dan suara, bentuk statis maupun dinamis (video animasi), yang dapat digunakan untuk merepresentasikan informasi dan pengetahuan yang telah dikumpulkan. Penyimpanan pengetahuan instansi sebaiknya dilakukan secara terpusat pada Pusat Data Nasional dengan memanfaatkan teknologi komputasi awan (cloud), sehingga memudahkan dalam menyediakan layanan secara berbagi pakai.

### 4. Proses Penggunaan

Pengetahuan SPBE dapat digunakan untuk mendukung efektifitas dan efisiensi dalam penyediaan dan penggunaan layanan SPBE, maupun untuk mendukung pengambilan keputusan terkait SPBE. Untuk itu pengetahuan SPBE harus senantiasa tersedia untuk digunakan, baik untuk pembelajaran, penanganan masalah, sampai dengan berinovasi dalam pengoperasian sistem, perawatan, evaluasi, perencanaan serta pengembangan sistem atau layanan baru SPBE.

Pengetahuan SPBE yang telah ada pun dapat digunakan kembali, dilengkapi, diperbaiki atau dikombinasikan dengan pengetahuan SPBE lainnya untuk menjadi pengetahuan baru. Pengukuran efektifitas penggunaan pengetahuan perlu dilakukan, dan menjadi masukan dalam pemantauan dan evaluasi penerapan manajemen pengetahuan yang dilaksanakan di Pemerintah Kabupaten Jombang

### 5. Proses Alih Pengetahuan dan Teknologi

Proses alih pengetahuan dan teknologi, atau transfer technology terkait SPBE adalah proses pemindahan pengetahuan dan tatacara (know-how) terkait SPBE dari satu atau sekelompok individu ke individu lainnya. Proses transfer teknologi SPBE tersebut bertujuan untuk memastikan pengetahuan dan teknologi tersebut dapat diserap atau dipahami oleh penerima nya, sedemikian rupa sehingga pengetahuan tersebut dapat digunakan untuk mengambil keputusan atau melakukan aksi.

Proses internalisasi pengetahuan SPBE oleh individu, atau dengan kata lain merupakan upaya mempelajari pengetahuan tentang SPBE yang telah bersifat eksplisit untuk dipahami dan digunakan untuk melakukan tindakan atau membuat keputusan. Untuk mendorong proses internalisasi ini berbagai cara atau alat dapat digunakan untuk mendukung alih pengetahuan, dari representasi atau media pembelajaran pengetahuan yang deskriptif dan mudah dimengerti, sampai dengan fasilitas tanya jawab, diskusi atau forum berbagi pengetahuan dengan individu lain dan para pakar atau ahli (subject matter expert) di bidang SPBE.

#### D. Proses Pemantauan dan Evaluasi

Pengendalian proses Manajemen Pengetahuan SPBE dilakukan dengan memperhatikan pelaksanaan prinsip-prinsip Manajemen Pengetahuan SPBE, pemenuhan dan peningkatan kapabilitas serta kematangan proses Manajemen Pengetahuan, serta efektifitas dalam implementasi Manajemen Pengetahuan dalam mencapai tujuan SPBE. Proses pengawasan Manajemen Pengetahuan SPBE dilaksanakan secara terintegrasi dengan proses pemantauan dan evaluasi SPBE serta audit TIK SPBE sesuai peraturan yang berlaku.

##### 1. Kematangan Penerapan Manajemen Pengetahuan SPBE

Kematangan penerapan Manajemen Pengetahuan SPBE, sesuai PermenPANRB nomor 59 tahun 2020 tentang Pemantauan dan Evaluasi SPBE dapat diukur dan bergantung pada aspek-aspek tata kelola seperti budaya, kepemimpinan dan kebijakan internal yang jelas dan kondusif, struktur pengelolaan yang optimal, penyelenggaraan proses Manajemen Pengetahuan yang efektif, efisien dan berkesinambungan, serta dukungan teknologi dan sumber daya yang memadai. Pengukuran tingkat kematangan Manajemen Pengetahuan sangatlah penting dan menjadi acuan untuk mendukung perencanaan dan perbaikan ke depan.

##### 2. Pengukuran Efektivitas Implementasi

Melakukan pengukuran efektivitas implementasi Manajemen Pengetahuan SPBE bukanlah hal yang mudah. Untuk mendapatkan korelasi langsung antara pelaksanaan proses Manajemen Pengetahuan SPBE, kualitas basis pengetahuan yang terbangun dan termanfaatkan, serta peningkatan kualitas layanan SPBE dan kualitas pengambilan keputusan dalam SPBE merupakan suatu tantangan tersendiri bagi pengelola Manajemen Pengetahuan SPBE. Beberapa pendekatan sederhana dalam melakukan pengukuran efektivitas implementasi Manajemen Pengetahuan SPBE adalah melalui pengukuran kuantitatif sebagai indikator aktivitas proses sebagai berikut.

##### a) Aktivitas pencarian pengetahuan SPBE

Pengukuran aktivitas pencarian pengetahuan SPBE yang dapat memberi gambaran tentang kebutuhan pengetahuan SPBE oleh pengguna, antara lain sebagai berikut.

- 1) Jumlah permintaan pencarian pengetahuan SPBE, berdasarkan lingkup, lokasi, unit kerja, maupun waktu.
- 2) Pengetahuan SPBE yang paling banyak dicari atau diminta oleh pengguna berdasarkan lokasi, unit kerja, maupun waktu.

##### b) Aktivitas penciptaan pengetahuan

Pengukuran aktifitas penciptaan pengetahuan (eksplisit) untuk dibagi- pakai yang dapat memberikan gambaran tentang pengembangan basis pengetahuan SPBE di suatu instansi, antara lain sebagai berikut.

- 1) Jumlah dan pertumbuhan artikel atau representasi pengetahuan SPBE baru yang terkumpul berdasarkan lokasi, unit kerja, maupun waktu.
- 2) Jumlah artikel atau representasi pengetahuan SPBE dari pakar atau ahli bidang tertentu, termasuk pegawai yang mendekati masa pensiun.

##### c) Aktivitas berdiskusi dan berbagi pengalaman

Pengukuran aktivitas berdiskusi dan berbagi pengalaman yang dapat memberikan gambaran tentang efektifitas proses penciptaan pengetahuan yang dibutuhkan secara kolektif, antara

lain sebagai berikut.

- 1) Jumlah pertanyaan atau permasalahan SPBE yang disampaikan dalam diskusi
- 2) Jumlah jawaban, respon atau komentar atas pertanyaan atau permasalahan SPBE yang dibahas dalam diskusi
- 3) Jumlah individu yang mengajukan pertanyaan terkait SPBE
- 4) Jumlah individu yang memberikan jawaban, respon atau komentar terhadap pertanyaan terkait SPBE.

Pengukuran efektivitas implementasi Manajemen Pengetahuan SPBE dapat dikembangkan selanjutnya, sesuai kebutuhan, kapasitas, kondisi penerapan, maupun tingkat kematangan penerapan Manajemen Pengetahuan di Pemerintah Kabupaten Jombang.

**BAB VII**  
**PEDOMAN MANAJEMEN PERUBAHAN**  
**SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK**

**I. PENDAHULUAN**

Manajemen Perubahan mendokumentasikan tata cara untuk melakukan perubahan-perubahan yang berkaitan dengan Masterplan Layanan SPBE. Tujuan adanya manajemen perubahan adalah Memastikan Layanan SPBE tersebut dapat memenuhi target yang telah dicanangkan. Perubahan-perubahan yang terjadi selama proses perubahan layanan SPBE Kabupaten Jombang dicatat sehingga dapat dikelola dan didokumentasikan dengan baik.

**II. DEFINISI**

1. Manajemen Perubahan SPBE adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur, dan budaya untuk menentukan tindakan terbaik terkait pencatatan perubahan layanan SPBE.
2. Perubahan Layanan SPBE adalah terjadinya perubahan layanan dalam suatu peristiwa yang akan mempengaruhi keberhasilan terhadap pencapaian tujuan penerapan SPBE.

**III. KEBIJAKAN PENYELENGGARAAN**

**A. Peran dan Tanggung Jawab**

Setiap entitas memiliki peran dan tanggung jawab pada tiap proses manajemen perubahan. Adapun kategori peran dan tanggung jawab tersebut adalah sebagai berikut.

1. Responsible (R)  
Entitas ini memiliki tanggung jawab untuk melaksanakan proses. Entitas ini wajib melaporkan pekerjaannya kepada entitas yang memiliki peran dan tanggung jawab dengan kategori Accountable.
2. Accountable (A)  
Entitas ini bertanggung jawab secara penuh terhadap proses yang sedang berlangsung dan memiliki wewenang untuk menyetujui hasil dari proses tersebut. Entitas ini dapat mengontrol keberjalanan proses melalui entitas lain yang memiliki peran dan tanggung jawab dengan kategori Responsible (R).
3. Supportive (S)  
Entitas yang dapat memberikan bantuan berupa sumber daya selama masa berlangsung manajemen perubahan.
4. Consulted (C)  
Entitas yang dapat memberikan informasi atau memberikan kapabilitas yang dibutuhkan untuk menyelesaikan suatu proses.
5. Informed (I)  
Entitas yang perlu diberikan informasi mengenai hasil dari suatu proses. Adapun bagaimana proses tersebut dilaksanakan tidak harus dikonsultasikan dengan entitas ini.

**B. Faktor Pendorong Perubahan**

Faktor-faktor yang dapat mendorong terjadinya perubahan dapat digolongkan ke dalam dua kelompok sebagai berikut.

**1. Faktor Teknologi**

Pendorong Teknologi tidak hanya dihasilkan oleh perubahan teknologi yang digunakan, tetapi juga segala aspek yang dapat mengimplikasikan kebutuhan untuk melakukan perubahan terhadap teknologi tersebut. Beberapa contoh Pendorong Teknologi antara lain adanya inovasi teknologi baru, pengurangan biaya manajemen aset teknologi informasi dan komunikasi, dan penarikan

penggunaan teknologi tertentu.

## 2. Faktor Bisnis

Pendorong bisnis berkaitan dengan tujuan-tujuan bisnis yang dimiliki oleh Pemerintah Kabupaten Jombang. Contoh-contoh pendorong bisnis antara lain perubahan kebijakan, pengembangan proses pelayanan umum, dan inovasi di bidang pelayanan umum.

## C. Prinsip Manajemen Perubahan

Manajemen perubahan terdapat tiga pendekatan yang perlu ditempuh di mana antara satu dengan lainnya perlu diintegrasikan. Ketiga pendekatan tersebut antara lain.

### 1. Strategis (Top-down)

Perubahan yang diarahkan oleh pejabat publik yang bertujuan untuk meningkatkan kualitas layanan SPBE baru, ataupun untuk menyelaraskan dengan perubahan arahan pimpinan, pemerintah pusat/provinsi, atau implementasi aturan/perundangan baru.

### 2. Bottom-up

Perubahan di tingkat OPD yang bertujuan untuk memperbaiki atau meningkatkan kualitas layanan SPBE yang berkaitan dengan infrastruktur dan aplikasi.

### 3. Evaluatif

Perubahan yang dihasilkan dari evaluasi terhadap realisasi layanan SPBE.

## IV. STANDAR PENYELENGGARAAN

### A. Proses Manajemen Perubahan

Secara umum, proses manajemen perubahan dapat dilihat pada di atas. Manajemen perubahan diawali dengan pendokumentasian usulan perubahan. Usulan tersebut kemudian dievaluasi untuk menjadi bahan pertimbangan keputusan pelaksanaan perubahan. Berdasarkan hasil evaluasi, dapat didefinisikan kebutuhan-kebutuhan perubahan yang ada. Setelah kebutuhan-kebutuhan perubahan terdefinisi, perlu dilakukan proses tata kelola di mana perubahan tersebut harus dikoordinasikan atau disetujui oleh pihak-pihak tertentu. Setelah usulan dan kebutuhan-kebutuhan perubahan disetujui, perubahan tersebut diimplementasikan dan harus didokumentasikan.

### B. Dokumentasi Usulan Perubahan

Bersamaan dengan proses realisasi layanan SPBE, akan ada informasi-informasi baru yang dapat mempengaruhi layanan SPBE itu sendiri. Informasi tersebut dapat berupa informasi mengenai teknologi, perubahan kebijakan, maupun lesson learned dari proses realisasi. Informasi-informasi tersebut dapat membuat beberapa bagian layanan SPBE menjadi tidak lagi relevan atau tidak lagi cukup untuk mewujudkan target yang dicanangkan sehingga diperlukan perubahan pada Masterplan tersebut.

Perubahan-perubahan yang diusulkan beserta pendorong perubahan tersebut perlu didokumentasikan. Adapun dokumentasi Usulan Perubahan tersebut mencakup hal-hal berikut.

#### 1. Deskripsi usulan perubahan

Usulan Perubahan harus menjelaskan bagian-bagian apa dalam Masterplan yang akan diubah beserta jenis serta bentuk perubahan yang diusulkan.

#### 2. Rasionalisasi usulan perubahan

Usulan Perubahan perlu menjabarkan faktor-faktor yang menjadi pendorong diusulkannya perubahan. Faktor-faktor tersebut dapat terdiri atas satu atau beberapa kelompok faktor yang telah disebutkan pada bagian sebelumnya.



3. Penilaian dampak yang dihasilkan dari usulan perubahan  
Usulan Perubahan perlu menyertakan penilaian terhadap dampak yang dihasilkan dari perubahan yang diusulkan. Dampak yang perlu dipertimbangkan antara lain dampak terhadap kebutuhan-kebutuhan tertentu yang berkaitan, dampak terhadap prioritas stakeholder, dan dampak terhadap proses realisasi.

#### C. Analisis Usulan Perubahan

Usulan Perubahan yang diajukan diklasifikasikan ke dalam kriteria prioritas berikut.

1. Darurat  
Usulan Perubahan yang mendesak berkaitan dengan penyesuaian Layanan SPBE dengan kapabilitas sumber daya aktual.
2. Tinggi  
Usulan Perubahan berkaitan dengan perubahan kebijakan, peraturan, ataupun perundangan yang mempengaruhi lingkungan pemerintahan Kabupaten Jombang.
3. Menengah  
Usulan Perubahan berkaitan dengan informasi-informasi baru yang didapatkan selama proses realisasi Layanan SPBE. Informasi-informasi tersebut dapat menjadi lesson learned yang dapat membantu pemerintah meningkatkan pelayanannya.
4. Rendah  
Usulan Perubahan berkaitan dengan perubahan layanan SPBE yang memengaruhi kinerja aplikasi dan infrastruktur yang digunakan dalam pemerintahan Kabupaten Jombang.

Selain itu, perlu dilakukan analisis kesenjangan untuk membandingkan kondisi ideal yang ingin dicapai oleh perubahan yang diusulkan dengan kondisi aktual Master Plan TIK. Perbandingan dua kondisi tersebut akan menjadi bahan dalam pendefinisian kebutuhan perubahan pada proses selanjutnya.

#### D. Pendefinisian Kebutuhan Perubahan

Pada proses ini didefinisikan kebutuhan-kebutuhan untuk merealisasikan perubahan. Kebutuhan-kebutuhan tersebut didasarkan pada analisis kesenjangan yang telah dilakukan pada proses sebelumnya. Adapun kebutuhan perubahan yang didefinisikan harus mengikuti karakteristik sebagai berikut.

1. Dapat dilacak (Traceable)  
Kebutuhan harus dapat dilacak ke suatu sumber tertentu yang mana pada hal ini adalah hasil analisis kesenjangan serta dokumen-dokumen lain yang terkait seperti dokumen kebijakan dan perundangan.
2. Tidak Ambigu  
Kebutuhan harus dinyatakan dengan jelas untuk mencegah terjadinya multi-interpretasi di antara para stakeholder.
3. Konsisten  
Kebutuhan-kebutuhan yang didefinisikan harus dipastikan untuk tidak bertentangan satu sama lain.

#### E. Pelaksanaan Proses Tata Kelola

Setelah Usulan Perubahan telah dianalisis dan telah didefinisikan kebutuhannya, maka kedua hal tersebut perlu disetujui oleh entitas-entitas yang berwenang sesuai dengan tata kelola dan organisasi yang diterapkan. Langkah awal dari proses ini adalah mempertemukan Bupati, Tim Koordinasi SPBE, dan Pokja Penerapan SPBE untuk membahas perubahan-perubahan yang telah diusulkan. Perubahan-perubahan yang diusulkan juga perlu disetujui oleh Bupati untuk

kemudian dijalankan

#### F. Implementasi Perubahan

Setelah usulan perubahan disetujui, usulan perubahan dapat mulai diimplementasikan. Pada proses ini perlu dipastikan bahwa setiap perubahan yang diimplementasikan harus didokumentasikan. Setelah perubahan diimplementasikan, perlu dilakukan pengukuran Faktor Kunci Keberhasilan untuk mengevaluasi tingkat keberhasilan dari perubahan yang dilakukan.

## **BAB VIII**

### **PEDOMAN MANAJEMEN LAYANAN**

### **SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK**

#### **I. PENDAHULUAN**

Rencana Induk Sistem Pemerintahan Berbasis Elektronik sebagai salah satu misi pembangunan nasional sesuai dengan amanat Undang-Undang Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang (RPJP) Nasional 2005 - 2025 adalah mewujudkan bangsa yang berdaya saing. Misi ini dapat dilakukan melalui pembangunan aparatur negara yang mencakup kelembagaan, ketatalaksanaan, pelayanan publik dan sumber daya manusia (SDM) aparatur. Berdasarkan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, aplikasi pemerintahan berbasis elektronik merupakan satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas dan fungsi Layanan SPBE. Bahwa untuk mendukung penyelenggaraan Sistem Pemerintahan Berbasis Elektronik sebagaimana diatur dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik dan Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik, perlu menetapkan panduan Penyelenggaraan Teknologi Informasi dan Komunikasi.

Tujuan dari pembangunan aparatur negara adalah mewujudkan tata kelola pemerintahan yang baik, peningkatan kualitas penyelenggaraan administrasi pemerintahan dan peningkatan partisipasi masyarakat dalam penyelenggaraan pembangunan. Kesiapan aparatur negara diperlukan untuk mengantisipasi proses globalisasi dan demokratisasi agar pemerintah melakukan perubahan mendasar pada sistem dan mekanisme pemerintahan, penyusunan kebijakan dan program pembangunan yang membuka ruang partisipasi masyarakat, dan pelayanan publik yang memenuhi aspek transparansi, akuntabilitas dan kinerja tinggi

#### **II. DEFINISI**

1. Aplikasi pemerintahan berbasis elektronik adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas dan fungsi layanan SPBE.
2. Aplikasi umum adalah aplikasi SPBE yang sama, standar, dan digunakan secara bagi pakai oleh instansi pusat dan/atau pemerintah daerah.
3. Aplikasi khusus adalah aplikasi SPBE yang dibangun, dikembangkan, digunakan dan dikelola oleh pemerintah daerah untuk memenuhi kebutuhan khusus yang bukan kebutuhan pemerintah daerah lain.
4. Siklus pengembangan aplikasi (system development life cycle/SDLC) adalah siklus pengembangan aplikasi terdiri dari proses analisis kebutuhan, proses perancangan, proses pengembangan, proses pengujian, proses implementasi dan proses tinjauan pasca implementasi aplikasi yang dapat dilaksanakan oleh internal, pihak ketiga atau melalui joint application development (JAD).

#### **III. KEBIJAKAN PENYELENGGARAAN**

##### **A. Pembangunan dan Pengembangan Aplikasi Layanan**

Pemerintah Daerah menggunakan aplikasi pemerintahan berbasis elektronik dalam rangka memberikan layanan pemerintahan berbasis elektronik sesuai dengan ketentuan peraturan perundang-undangan. Aplikasi pemerintahan berbasis elektronik yang dibangun dan dikembangkan oleh Pemerintah Daerah menjadi milik negara. Pembangunan dan pengembangan aplikasi pemerintahan berbasis elektronik mengutamakan penggunaan kode sumber terbuka (open

source). Dalam hal menggunakan kode sumber tertutup, Pemerintah Daerah harus mendapatkan rekomendasi dari Menteri.

Pemerintah Daerah menetapkan proses bisnis layanan pemerintah berbasis elektronik sesuai dengan Arsitektur SPBE Pemerintah Daerah. Proses bisnis sebagaimana dimaksud bertujuan untuk memberikan pedoman dalam penggunaan Dokumen Elektronik dan Informasi Elektronik serta penerapan aplikasi pemerintahan berbasis elektronik sesuai dengan standar keamanan informasi dan layanan pemerintah berbasis elektronik di daerah sesuai dengan ketentuan peraturan perundang-undangan. Pemerintah Daerah dapat mengembangkan aplikasi khusus yang didasarkan pada Rencana Induk SPBE, Arsitektur SPBE, dan kebutuhan khusus pada perangkat daerah masing-masing. Pembangunan dan pengembangan aplikasi dilakukan oleh:

1. Dinas Komunikasi dan Informatika; atau
2. Perangkat daerah pemilik proses bisnis

#### B. Siklus Pembangunan Aplikasi Layanan

Pembangunan dan pengembangan aplikasi pemerintahan berbasis elektronik dilaksanakan berdasarkan siklus pembangunan aplikasi (system development life cycle), yang terdiri dari tahapan:

1. Perencanaan pembangunan dan pengembangan aplikasi;
2. Proses perumusan analisis kebutuhan aplikasi;
3. Proses perancangan teknis;
4. Proses pembuatan kode program;
5. Proses pengujian aplikasi;
6. Proses implementasi aplikasi.

#### C. Kelengkapan Pendukung Aplikasi Layanan

Seluruh proses pembangunan dan pengembangan aplikasi harus dikonsultasikan dengan Dinas Komunikasi dan Informatika. Dinas Komunikasi dan Informatika memastikan bahwa proses pembangunan dan pengembangan aplikasi telah sesuai dengan kebijakan dan standar pengembangan aplikasi pembangunan dan pengembangan aplikasi. Pembangunan dan pengembangan aplikasi harus menyertakan kode sumber (source code) dan aplikasi disertai dokumen elektronik untuk disimpan dalam pusat aplikasi (repositori) paling sedikit:

1. detail teknis database (detail of database engineering design);
2. desain teknis pengembangan aplikasi;
3. manual bagi administrator;
4. manual bagi pengguna;
5. manual instalasi; dan
6. manual penanganan masalah (trouble shooting).

Dinas Komunikasi dan Informatika bertanggung jawab terhadap pengembangan dan penyelenggaraan pusat aplikasi (repositori) yang berisi sekumpulan paket aplikasi atau program dari suatu sistem elektronik yang digunakan untuk menunjang kinerja dari suatu aplikasi program. Aplikasi yang dikembangkan oleh perangkat daerah harus ditempatkan di pusat data Pemerintah Daerah yang dikelola oleh Dinas Komunikasi dan Informatika. Dinas Komunikasi dan Informatika melakukan inventarisasi aplikasi yang belum memenuhi aspek-aspek. Dinas Komunikasi dan Informatika melakukan rewiu dan evaluasi aplikasi secara berkala.

### IV. STANDAR PENYELENGGARAAN

#### A. Pelaksanaan Pembangunan dan Pengembangan Aplikasi

Tahap pelaksanaan pembangunan dan pengembangan aplikasi terdiri atas:

1. Proses perumusan analisis kebutuhan aplikasi, menghasilkan

dokumen Spesifikasi Kebutuhan Perangkat Lunak (SKPL) / Software Requirements Specification (SRS);

2. Proses perancangan teknis, menghasilkan dokumen Deskripsi Perancangan Perangkat Lunak (DPPL) / Software Design Description (SDD);
3. Proses pembuatan kode program (coding), menghasilkan kode sumber (source code);
4. Proses pengujian aplikasi;
5. Proses penerapan aplikasi;
6. Proses peninjauan ulang pasca implementasi.

#### B. Perumusan Analisis Kebutuhan Aplikasi

Proses perumusan analisis kebutuhan aplikasi, meliputi kegiatan pengumpulan, analisis, penyusunan, dan pendokumentasian Spesifikasi Kebutuhan Perangkat Lunak (SKPL), yang memuat:

1. Gambaran umum, identifikasi permasalahan, maksud dan tujuan pengembangan aplikasi;
2. Deskripsi kebutuhan aplikasi yang diinginkan, fungsi, identifikasi kelompok pengguna, lingkungan operasi, serta batasan ruang lingkup;
3. Deskripsi kebutuhan antarmuka (interface) aplikasi yang diinginkan;
4. Deskripsi kebutuhan fungsional berdasarkan proses bisnis.

#### C. Perancangan Teknis

Proses perancangan teknis, meliputi kegiatan penyusunan dan pendokumentasian Deskripsi Perancangan Perangkat Lunak (DPPL), yang memuat:

1. Arsitektur sistem aplikasi
2. Rancangan kebutuhan sistem aplikasi, basis data serta infrastruktur pendukung
3. Rancangan sistem manajemen database, termasuk skema fisik, skema konseptual, diagram relasi entitas (ERD), serta deskripsi data dictionary pada masing-masing entitas
4. Rancangan antarmuka (interface) aplikasi, termasuk tampilan masukan (input), tampilan navigasi, tampilan keluaran (output), serta tampilan cetakan
5. Desain rinci aplikasi
6. Deskripsi integritas sistem

#### D. Pembuatan Kode Program

Proses pembuatan kode program, meliputi kegiatan pelaksanaan pengkodean (coding) aplikasi dan basis data sesuai dengan Deskripsi Perancangan Perangkat Lunak (DPPL) yang telah disetujui, serta pendokumentasian kode program disertai dengan penjelasannya. Pembuatan kode program (source code) yang sesuai dengan Kebijakan dan Standar Keamanan Aplikasi pada Pemerintah Daerah

#### E. Pengujian Aplikasi

Proses pengujian aplikasi, meliputi kegiatan penyusunan rencana dan pelaksanaan setiap jenis pengujian, yang terdiri dari:

1. Pengujian unit (unit testing);
2. Pengujian sistem (system testing);
3. Pengujian integrasi (integration testing); dan
4. Pengujian penerimaan pengguna (user acceptance test/UAT).

#### F. Implementasi Aplikasi

Proses implementasi aplikasi, meliputi kegiatan:

1. Penyusunan rencana implementasi aplikasi di lingkungan

operasional yang mencakup kebutuhan sumber daya, urutan langkah implementasi dari komponen aplikasi, pemindahan perangkat lunak dari/atau perangkat keras dari lingkungan pengujian ke lingkungan operasional, fall-back plan dan/atau backup plan untuk mengantisipasi kegagalan dalam implementasi aplikasi, serta jadwal pelatihan.

2. Penyusunan panduan penggunaan aplikasi, panduan instalasi aplikasi, dan materi pelatihan aplikasi.
3. Serah terima aplikasi berikut dokumentasinya kepada pemilik proses bisnis.
4. Pelaksanaan pelatihan dan transfer pengetahuan.
5. Penetapan payung hukum dan petunjuk teknis yang selaras dengan proses bisnis.

#### G. Tinjauan Pasca Implementasi Aplikasi

Proses tinjauan pasca implementasi aplikasi meliputi kegiatan pelaksanaan evaluasi yang dijadikan bahan pembelajaran untuk pengembangan aplikasi selanjutnya serta penyusunan hasil tinjauan pasca implementasi aplikasi ke dalam dokumen tinjauan pasca implementasi aplikasi.

#### H. Prosedur Baku Pelaksanaan Kegiatan

Prosedur Baku pelaksanaan kegiatan pembangunan dan pengembangan aplikasi terdiri dari 5 (lima) SOP, yaitu:

1. SOP Perencanaan Pembangunan Aplikasi
  - a) Kepala OPD pemohon menyampaikan surat permohonan pengembangan aplikasi kepada Kepala Dinas Kominfo, dilengkapi dengan formulir permohonan
  - b) Kepala Dinas Kominfo mendisposisi permohonan kepada Kabid
  - c) Kabid memeriksa kelengkapan permohonan, dan selanjutnya mendisposisi permohonan kepada Kasi.
  - d) Kasi menyusun rencana kerja, dan membentuk Tim Pengembangan Aplikasi (terdiri dari: Front-end Developer, Back-end Developer, Database Administrator) beserta uraian tugas dan estimasi waktu penyelesaian.
  - e) Kasi menyampaikan rencana kerja kepada Tim Pengembangan Aplikasi.
  - f) Kasi mencatat permohonan ke dalam log permohonan pengembangan aplikasi.
  - g) Kasi membuat draft surat tanggapan atas permohonan pengembangan aplikasi kepada Kepala OPD pemohon, dan diparaf oleh Kabid.
  - h) Kabid meneruskan draft surat tanggapan ke Kepala Dinas.
  - i) Kepala Dinas menandatangani surat tanggapan kepada Kepala OPD pemohon.
2. SOP Penyusunan Analisis Kebutuhan Aplikasi
  - a) Tim Pengembangan Aplikasi menyelenggarakan rapat teknis bersama pemohon untuk membahas analisis pengembangan aplikasi.
  - b) Tim Pengembangan Aplikasi meminta keterangan kepada pemohon mengenai deskripsi aplikasi, proses bisnis, user, kebutuhan antarmuka, kebutuhan fungsional, kebutuhan model proses, dan kebutuhan model data.
  - c) Tim Pengembangan Aplikasi mencatat hasil identifikasi kebutuhan dalam BAP.
  - d) Tim Pengembangan Aplikasi melakukan analisis dan melaporkan dalam bentuk dokumen "Spesifikasi Kebutuhan Perangkat Lunak" (SKPL) / Software Requirement Specification (SRS).
  - e) Tim Pengembangan Aplikasi menyelenggarakan rapat teknis

- bersama pemohon untuk membahas dokumen SKPL, dan dituangkan dalam Berita Acara.
- f) Apabila semua kebutuhan telah disepakati, maka dilanjutkan ke tahapan berikutnya.
3. SOP Penyusunan Perancangan Teknis Aplikasi
- a) Tim Pengembangan Aplikasi menyusun dokumen “Deskripsi Perancangan Perangkat Lunak” (DPPL) / Software Description Design (SDD), yang berisi deskripsi mengenai: deskripsi aplikasi, arsitektur aplikasi, sistem manajemen database, antarmuka, serta integritas sistem.
  - b) Tim Pengembangan Aplikasi menyelenggarakan rapat teknis bersama pemohon untuk membahas dokumen DPPL, dan dituangkan dalam Berita Acara
  - c) Apabila semua kebutuhan telah disepakati, maka dilanjutkan ke tahapan berikutnya
4. SOP Pembuatan Kode Aplikasi
- a) Tim Pengembangan Aplikasi membuat folder repositori rancangan aplikasi untuk penempatan source code.
  - b) Tim Pengembangan Aplikasi melakukan pengkodean (coding) aplikasi berdasarkan dokumen DPPL.
  - c) Tim Pengembangan Aplikasi melakukan pengujian terhadap aplikasi, dan melaporkan dalam dokumen pengujian aplikasi.
  - d) Tim Pengembangan Aplikasi memperbaiki kesalahan yang terjadi.
  - e) Tim Pengembangan Aplikasi membuat manual penggunaan aplikasi.
  - f) Tim Pengembangan Aplikasi melaporkan hasil pengembangan aplikasi kepada Kasi.
  - g) Kasi membuat draft surat hasil pengembangan aplikasi dan surat rekomendasi kepada Kepala OPD pemohon, dan diparaf oleh Kabid.
  - h) Kabid meneruskan draft surat hasil pengembangan aplikasi ke Kepala Dinas pemohon.
  - i) Kepala Dinas menandatangani surat hasil pengembangan aplikasi kepada Kepala OPD pemohon.
5. SOP Inventarisasi Aplikasi
- a) Kepala OPD pemohon menyampaikan surat permohonan inventarisasi aplikasi kepada Kepala Dinas Kominfo, dilengkapi dengan formulir permohonan
  - b) Kepala Dinas Kominfo mendisposisi permohonan kepada Kabid
  - c) Kabid memeriksa kelengkapan permohonan, dan selanjutnya mendisposisi permohonan kepada Kasi
  - d) Tim Pengembangan Aplikasi menyelenggarakan rapat teknis bersama Tim Teknis OPD untuk melakukan inventarisasi dengan melampirkan:
    - (1) Source code aplikasi;
    - (2) Dokumentasi Analisis SKPL;
    - (3) Dokumentasi Analisis DPPL;
    - (4) Dokumentasi Analisis Pengujian Aplikasi;
    - (5) Petunjuk Instalasi;
    - (6) Petunjuk Penggunaan.
  - e) Tim Teknis OPD mempresentasikan aplikasi.
  - f) Tim Pengembangan Aplikasi melakukan analisis terhadap:
    - (1) Kebutuhan, ruang lingkup, dan cakupan aplikasi
    - (2) Aplikasi sejenis yang sudah ada di Pemerintah Daerah
    - (3) Ketersediaan aplikasi lain yang berhubungan dan perlu diintegrasikan
    - (4) Kebutuhan dan ketersediaan infrastruktur (server, jaringan,

- PC, pengguna), SDM, dan anggaran
- g) Tim Pengembangan Aplikasi melakukan instalasi dan pengujian aplikasi di server Kominfo, serta membandingkan dengan hasil presentasi sebelumnya.
  - h) Tim Pengembangan Aplikasi memberikan tanggapan terhadap aplikasi.
  - i) Tim Pengembangan Aplikasi menambahkan aplikasi ke dalam Daftar Aplikasi Pemerintah Kabupaten Jombang dan menyimpan source code ke dalam repositori Pemerintah Daerah.
  - j) Tim Pengembangan Aplikasi membuat laporan hasil inventarisasi aplikasi.



**BAB IX**  
**PEDOMAN AUDIT INFRASTRUKTUR**  
**SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK**

**I. PENDAHULUAN**

Pemerintah perlu melakukan audit Sistem Pemerintahan Berbasis Elektronik (SPBE) sebagai upaya untuk mendukung digital government yang partisipatif, kolaboratif, berkelanjutan, dan efektif. Hasil dari audit akan membantu pemerintah dalam melakukan perbaikan kualitas infrastruktur, aplikasi, keamanan SPBE dalam jangka panjang. Audit teknologi informasi dan komunikasi merupakan proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi. Tujuannya untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan atau standar yang telah ditetapkan, termasuk peraturan perundangan yang berlaku. Ruang lingkup audit terbagi dalam tata kelola dan manajemen, fungsionalitas dan kinerja, serta aspek TIK lainnya.

Secara umum, audit teknologi memiliki lima tujuan yang bermanfaat dalam mengatasi berbagai macam permasalahan. Tujuan tersebut berupa peningkatan kinerja, penilaian kepatuhan terhadap standar teknis serta peraturan perundangan yang berlaku, dan pencegahan atas risiko penggunaan teknologi. Kemudian untuk tujuan positioning atau perencanaan serta audit teknologi untuk investigasi. Tujuan audit teknologi dalam SPBE adalah untuk peningkatan kinerja, kepatuhan, pencegahan atas risiko penggunaan teknologi, dan sekaligus untuk perencanaan. Andrari menekankan bahwa audit tujuannya bukan mencari kesalahan, namun mencari celah untuk melakukan perbaikan. "Audit teknologi tidak untuk menyalahkan, tetapi untuk melakukan perbaikan Audit TIK SPBE terdiri dari 3 kegiatan utama, yaitu; Audit Infrastruktur, Audit Aplikasi dan Audit Keamanan. Sesuai dengan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik mengatur Audit TIK, dijelaskan bahwa

1. Audit Infrastruktur terdiri dari Infrastruktur SPBE Nasional dan Infrastruktur Instansi Pusat dan Daerah
2. Audit Aplikasi terdiri dari Aplikasi Umum dan Aplikasi khusus
3. Audit Keamanan terdiri dari Keamanan Infrastruktur SPBE Nasional, Keamanan Infrastruktur Instansi Pusat dan Daerah, Keamanan Aplikasi Umum dan Keamanan Aplikasi Khusus

**II. DEFINISI**

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. 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.
3. Audit Infrastruktur SPBE adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset Infrastruktur SPBE dengan tujuan untuk menetapkan tingkat kesesuaian antara Infrastruktur SPBE dengan kriteria dan/atau standar yang telah ditetapkan.
4. Auditor adalah orang yang memiliki kompetensi pengetahuan dan keterampilan khusus dengan tugas utama melakukan evaluasi atas pengendalian sistem elektronik yang dapat dipertanggungjawabkan

secara akademis maupun praktis.

5. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, serta pemulihan data.
6. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.
7. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran layanan SPBE.
8. Pusat Data Nasional adalah sekumpulan pusat data yang digunakan secara bagi pakai oleh instansi pusat dan pemerintah daerah, dan saling terhubung.
9. Jaringan Intra Pemerintah adalah jaringan interkoneksi tertutup yang menghubungkan antar jaringan intra instansi pusat dan pemerintah daerah.
10. Sistem Penghubung Layanan Pemerintah adalah perangkat terintegrasi yang terhubung dengan sistem penghubung layanan instansi pusat dan pemerintah daerah untuk pertukaran layanan SPBE antar instansi pusat dan/atau pemerintah daerah.
11. Lembaga Sertifikasi Profesi yang selanjutnya disingkat LSP adalah lembaga pelaksana kegiatan sertifikasi kompetensi Auditor teknologi informasi dan komunikasi dengan lingkup Audit Infrastruktur SPBE.
12. Lembaga Pelaksana Audit SPBE yang selanjutnya disingkat LATIK SPBE adalah lembaga pelaksana audit SPBE.
13. Auditee adalah instansi pusat dan pemerintah daerah yang menjadi objek dari pelaksanaan Audit Infrastruktur SPBE.

### **III. KEBIJAKAN PENYELENGGARAAN**

#### **A. AUDITOR INFRASTRUKTUR SPBE**

Auditor Infrastruktur SPBE merupakan Auditor Teknologi yang memiliki kemampuan teknis di bidang infrastruktur TIK. Ketua Tim Audit (Lead Auditor) wajib memiliki sertifikat kompetensi Auditor. Sertifikasi kompetensi Auditor teknologi dilaksanakan oleh Lembaga Sertifikasi Profesi (LSP) bidang kompetensi Auditor teknologi atau LSP yang mendapat pengakuan dari Badan. Pemberkasan dan penyeleksian pendaftaran Auditor dan Tim Audit SPBE dilakukan secara adil berdasarkan tanggal pemberkasan atau tanggal permintaan dan kelengkapan persyaratan berdasarkan dokumen yang valid. Pendaftaran Auditor dan Tim Audit SPBE dilakukan secara transparan dan tepat waktu.

Calon Auditor SPBE mengajukan permohonan Surat Tanda Registrasi sebagai Auditor SPBE kepada Kepala Badan Riset dan Inovasi Nasional. Permohonan pendaftaran dilengkapi dengan dokumen:

1. surat permohonan;
2. sertifikat kompetensi di bidang Audit infrastruktur TIK yang mendapat pengakuan dari Badan Riset dan Inovasi Nasional.

Kepala Badan Riset dan Inovasi Nasional menetapkan Surat Tanda Registrasi Auditor SPBE paling lambat 14 (empat belas) hari kerja setelah permohonan dinyatakan valid dan lengkap. Surat Tanda Registrasi berlaku sesuai dengan masa berlaku sertifikat kompetensi Auditor Infrastruktur SPBE, maksimal selama 5 tahun. Auditor SPBE yang telah memperoleh Surat Tanda Registrasi dinyatakan dalam Daftar Auditor SPBE. LATIK SPBE yang telah memperoleh surat tanda registrasi LATIK SPBE ditetapkan dengan Keputusan Kepala Badan.

Surat Tanda Registrasi Auditor SPBE dinyatakan tidak berlaku apabila:

1. melanggar kode etik;
2. meninggal dunia;
3. habis masa berlaku Surat Tanda Registrasi;

4. mengundurkan diri.

Masa berlaku Surat Tanda Registrasi dapat diperpanjang dengan cara melengkapi kembali dokumen pendaftaran. Prosedur Pendaftaran Auditor.

#### **IV. STANDAR PENYELENGGARAAN**

##### **A. Standar Pelaksanaan Audit Infrastruktur SPBE**

Standar Pelaksanaan Audit Infrastruktur SPBE adalah batasan minimal bagi Regulator dan Auditor untuk membantu proses pendaftaran Auditor dan LATIK SPBE terakreditasi, pelaksanaan Audit serta prosedur yang harus dilaksanakan atau diterapkan dalam rangka pencapaian tujuan Audit. Standar Pelaksanaan Audit Infrastruktur SPBE memiliki tujuan sebagai berikut:

1. Menetapkan prinsip-prinsip dasar bagi pelaksanaan Audit Infrastruktur SPBE;
2. Menyusun Kerangka Kerja regulasi Audit Infrastruktur SPBE dalam proses pendaftaran Auditor dan Lembaga Audit Terakreditasi;
3. Menyusun Kerangka Kerja dalam pemberian layanan jasa Audit Infrastruktur SPBE, guna menambah nilai kepada IPPD yang diaudit (Auditee) melalui perbaikan proses dan operasionalnya; dan
4. Menyusun dasar dalam melakukan evaluasi terhadap regulasi dan pelaksanaan Audit Infrastruktur SPBE guna mendorong rencana perbaikan.

Standar Pelaksanaan Audit Infrastruktur SPBE mencakup hal-hal sebagai berikut:

1. Standar Umum
  - a) Standar Umum memberikan prinsip dasar untuk mengatur Auditor Infrastruktur SPBE dalam melaksanakan tugasnya dan mengatur pendaftaran Auditor, serta LATIK SPBE terakreditasi yang akan memberikan layanan jasa Audit Infrastruktur SPBE sehingga pelaksanaan pekerjaan Audit Infrastruktur SPBE hingga pelaporannya dapat terlaksana dengan baik dan efektif.
  - b) Pimpinan LATIK SPBE harus mengembangkan dan menjaga jaminan kualitas dan program peningkatan yang mencakup semua aspek pelaksanaan Audit Infrastruktur SPBE.
  - c) Integritas Auditor Infrastruktur SPBE dan pelaksana pendaftaran diwujudkan melalui sikap independen, objektif, dan menjaga kerahasiaan. Dalam melaksanakan tugasnya, Auditor Infrastruktur SPBE dituntut untuk menjalankan hal-hal sebagai berikut:
    - 1) Memiliki pengetahuan (knowledge), keterampilan (skil), sikap (attitude) dan pengalaman (experience) yang sesuai dengan standar kompetensi Auditor, guna memenuhi tanggung jawabnya dalam pelaksanaan audit;
    - 2) Menggunakan keahlian profesionalnya dengan cermat dan seksama (due professional care) serta berhati-hati (prudent) dalam setiap penugasan;
    - 3) Senantiasa mengasah dan melatih kecermatan profesionalnya;
    - 4) Meningkatkan pengetahuan, keahlian, dan kompetensi lain yang diperlukannya dengan mengikuti Pendidikan dan pelatihan berkelanjutan;
    - 5) Mematuhi prosedur yang ditetapkan dan mematuhi aturan perundangan; dan
    - 6) Memiliki pengetahuan (knowledge), keterampilan (skil), sikap (attitude) dan pengalaman (experience) yang sesuai guna memenuhi tanggung jawabnya dalam pelaksanaan audit.
  - d) Tujuan, wewenang dan tanggung jawab suatu aktivitas Audit Infrastruktur SPBE harus didefinisikan dengan jelas, tertuang

dalam suatu dokumen formal berupa piagam audit (audit charter), surat tugas, atau dokumen dokumen yang setara. Surat tugas atau piagam audit (audit charter) wajib menjelaskan tujuan audit, ruang lingkup, kewenangan tim audit dan etika yang harus dipatuhi oleh tim audit.

## 2. Standar Pelaksanaan

- a) Ketua tim audit (Lead Auditor) harus secara efektif mengelola aktivitas audit untuk menjamin agar tujuan Audit Infrastruktur SPBE tercapai.
- b) Ketua tim audit (Lead Auditor) harus melakukan hal-hal sebagai berikut:
  - 1) Menyusun dan menetapkan rencana audit (audit plan) guna menentukan prioritas-prioritas dalam kegiatan Audit Infrastruktur SPBE yang konsisten dengan tujuan audit sesuai dengan piagam audit (audit charter);
  - 2) Menyampaikan rencana audit (audit plan) kepada pimpinan dan Auditee untuk dikaji dan diberi persetujuan, serta mengkomunikasikan dampak dari keterbatasan sumberdaya;
  - 3) Mengelola sumberdaya audit yang tepat, memadai, dan efektif untuk melaksanakan rencana audit yang telah disetujui;
- c) Tim Koordinasi mengajukan permintaan Audit Infrastruktur SPBE untuk satu atau lebih dari tujuan berikut:
  - 1) Peningkatan kinerja birokrasi dan pelayanan publik;
  - 2) Penilaian kesesuaian dengan standar/prosedur/ pedoman dan kesesuaian dengan rencana/ kebutuhan/kondisi;
  - 3) Identifikasi status teknologi yang dimiliki, identifikasi kemampuan teknologi, termasuk dalam hal ini adalah inventarisasi dan pemetaan aset teknologi;
  - 4) Perencanaan pengembangan sistem/ teknologi dan perencanaan perbaikan kelemahan; dan/atau
  - 5) Pengungkapan suatu sebab atau fakta terkait dengan suatu kejadian atau peristiwa yang biasanya berimplikasi pada kondisi yang membahayakan keselamatan atau keamanan.
- d) Pemeriksaan yang dilakukan oleh Auditee mencakup:
  - 1) Penerapan tata kelola dan manajemen infrastruktur SPBE;
  - 2) Fungsionalitas dan kinerja infrastruktur SPBE; dan
  - 3) Tingkat kepatuhan terhadap regulasi.
- e) Dalam hal merencanakan Audit Infrastruktur SPBE, Auditor harus mengembangkan dan mendokumentasikan rencana untuk setiap pelaksanaan Audit Infrastruktur SPBE, termasuk tujuan, lingkup, waktu, dan alokasi sumber daya bagi pelaksanaan audit. Perencanaan tersebut yang dituangkan dalam rencana audit (audit plan) dengan mempertimbangkan berbagai hal, antara lain:
  - 1) Sistem pengendalian internal dan kepatuhan Auditee terhadap acuan atau benchmark;
  - 2) Penetapan tujuan Audit Infrastruktur SPBE;
  - 3) Penetapan kecukupan lingkup; dan
  - 4) Penggunaan metodologi yang tepat.
- f) Dalam hal pelaksanaan audit Infrastruktur SPBE, Auditor Infrastruktur SPBE harus mengidentifikasi, menganalisis, mengevaluasi, dan mendokumentasikan informasi yang cukup untuk mencapai tujuan audit. Dalam melaksanakan audit tersebut, Auditor Infrastruktur SPBE harus:
  - 1) Memperoleh bukti-bukti audit yang cukup, handal, dan relevan untuk mendukung penilaian audit dan kesimpulan audit;
  - 2) Mendasarkan temuan dan kesimpulan audit pada analisis dan

- interpretasi yang memadai atas bukti-bukti audit;
- 3) Menyiapkan, mengelola dan menyimpan data dan informasi yang diperoleh selama pelaksanaan audit; dan 4. Disupervisi dengan baik untuk memastikan terjaminnya kualitas dan meningkatnya kemampuan Auditor.
  - g) Dalam hal komunikasi atas hasil Audit Infrastruktur SPBE, Auditor Infrastruktur SPBE harus mengkomunikasikan hasil pelaksanaan audit kepada pihak-pihak yang berkepentingan. Komunikasi tersebut harus mencakup tujuan dan ruang lingkup pelaksanaan audit, selain kesimpulan yang terkait, rekomendasi dan rencana tindak. Jika komunikasi final berisi kesalahan atau penghilangan yang signifikan, ketua tim audit (Lead Auditor) harus mengkomunikasikan informasi yang telah diperbaiki kepada semua pihak yang menerima komunikasi.
  - h) Aspek monitoring dalam aktivitas Audit Infrastruktur SPBE meliputi:
    - 1) Kepatuhan terhadap Kode Etik dan Standar Audit;
    - 2) Kesesuaian terhadap Piagam Audit;
    - 3) Kesesuaian terhadap Rencana Audit; dan
    - 4) Kesesuaian terhadap Protokol Audit
3. Standar Pelaporan
- a) Laporan hasil audit dibuat oleh Tim Audit dalam bentuk dokumen laporan audit dengan tepat waktu, lengkap, akurat, objektif, meyakinkan, jelas, dan ringkas.
  - b) Laporan audit harus mencantumkan batasan atau pengecualian yang berkaitan dengan pelaksanaan audit. Auditor dapat meminta tanggapan atau pendapat terhadap temuan, kesimpulan, dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh Auditee secara tertulis dari pejabat Auditee yang bertanggung jawab.
4. Standar Tindak Lanjut
- a) Pemantauan terhadap legalitas, kompetensi, dan kinerja Tim Audit dilakukan melalui mekanisme laporan tahunan pelaksanaan audit.
  - b) Dalam kondisi pemantauan terhadap tindak lanjut akan dilaksanakan, ketua tim audit (Lead Auditor) harus, menetapkan sebuah sistem pemantauan terhadap tindak lanjut temuan, kesimpulan dan rekomendasi audit oleh Auditee, mencakup cara berkomunikasi dengan Auditee, prosedur pemantauan, dan laporan status temuan.

## B. Tata Cara Pelaksanaan Audit Infrastruktur SPBE

### 1. Tata Cara Pelaksanaan Audit

Audit Infrastruktur SPBE dilakukan Tim Audit berdasarkan permintaan Tim Koordinasi. Audit Infrastruktur SPBE dilaksanakan mengikuti tata cara audit yang secara garis besar terbagi dalam tiga kelompok tahapan, yaitu:

- a) Tahap perencanaan (pre-audit);
- b) Tahap pelaksanaan lapangan (onsite audit); dan
- c) Tahap analisa data dan pelaporan (post audit).

Audit Infrastruktur SPBE dilakukan oleh sebuah tim audit yang terdiri dari posisi-posisi berikut dengan uraian tugas dan tanggung jawab sebagai berikut:

- a) Pengawas mutu, berperan melakukan monitoring dan evaluasi aktivitas audit untuk menjamin pelaksanaan audit sesuai dengan standar audit. Pengawas mutu harus memiliki kualifikasi Auditor teknologi utama atau yang setara;

- b) Lead Auditor, bertanggung jawab merencanakan audit teknologi, melaksanakan audit di lapangan, mengendalikan data dan melaporkan hasil audit teknologi. Lead Auditor harus mempunyai kualifikasi minimal setara dengan Auditor teknologi madya;
- c) Auditor, bertugas membantu Lead Auditor dalam aktivitas audit teknologi. Auditor harus mempunyai kualifikasi minimal setara dengan Auditor teknologi muda;
- d) Asisten Auditor, bertugas membantu Auditor dalam aktivitas audit teknologi;
- e) Teknisi, bertugas membantu Auditor dalam pengumpulan data lapangan;
- f) Narasumber, berperan memberi masukan yang berkaitan dengan isu, status teknologi, dan keilmuan yang relevan.
- g) Quick Assessment dilakukan untuk mengenali objek audit dengan mengidentifikasi: current issue, lokasi organisasi yang diaudit, struktur organisasi dari organisasi yang diaudit, proses bisnis dari organisasi, atau bagian yang diaudit.

Tim Audit Infrastruktur SPBE harus merencanakan tindakan audit dengan mendefinisikan hal-hal berikut:

- a) Tujuan audit;
- b) Lingkup;
- c) Pendekatan;
- d) Kriteria;
- e) Parameter;
- f) Acuan;
- g) Metode pengumpulan data;
- h) Penentuan objek;
- i) Data primer dan sekunder;
- j) Metode analisa;
- k) Deliverable; dan
- l) Perkiraan jadwal pelaksanaan.

Hal-hal tersebut harus dicantumkan dalam Rencana Audit (Audit Plan). Ketua tim audit dan Auditee harus menyepakati rencana audit sebelum tahap pelaksanaan audit. Dalam pelaksanaan kegiatan audit, tim Audit Infrastruktur SPBE harus:

- a) Menyusun protokol audit yang berisi detail instrument audit, antara lain:
  - (1) Daftar data, pertanyaan dan pengujian
  - (2) Formulir untuk mencatat data, jawaban, hasil observasi dan hasil pengujian;
- b) Menetapkan parameter acuan untuk setiap kriteria diperlukan untuk memberikan suatu acuan perbandingan;
- c) Melakukan pertemuan pembukaan dengan Auditee;
- d) Melaksanakan audit lapangan, melalui:
  - (1) Penelaahan dokumen;
  - (2) Wawancara;
  - (3) Observasi lapangan;
  - (4) Pengujian; dan
  - (5) Verifikasi bukti;
- e) Melakukan pertemuan penutupan dengan Auditee;
- f) Melakukan analisis bukti; dan
- g) Mengelola data.

Data status teknologi SPBE dikumpulkan secara objektif berdasarkan fakta yang ada pada Auditee. Deskripsi data dan informasi yang

dikumpulkan mengikuti kriteria. Temuan Audit Infrastruktur SPBE merupakan keadaan dimana fakta status aset teknologi SPBE Auditee tidak sesuai dengan persyaratan infrastruktur SPBE. Auditor dapat mengurangi atau menambahkan lingkup sepanjang relevan dengan objek dan rencana penggunaan hasil audit sesuai kebutuhan Auditee.

Monitoring memberikan informasi untuk suatu kegiatan audit yang sedang berjalan yang bertujuan untuk mengidentifikasi kemajuan dalam pelaksanaan audit. Monitoring dilakukan oleh tim pengawas mutu. Tim pengawas mutu harus menetapkan suatu proses tindak lanjut untuk memonitor dan meyakinkan bahwa tindak lanjut yang telah ditetapkan oleh Tim Audit diimplementasikan secara efektif. Tim pengawas mutu dapat berasal dari pihak eksternal. Evaluasi secara menyeluruh dilakukan setelah aktivitas audit selesai yang bertujuan untuk mengetahui kelebihan dan kekurangan aktivitas audit yang telah dilakukan dalam rangka meningkatkan kualitas pelaksanaan audit berikutnya. Evaluasi dilakukan oleh tim pengawas mutu setelah aktivitas audit selesai. Tim Pengawas mutu menyampaikan hasil evaluasi audit kepada Tim Koordinasi. Tim Koordinasi menetapkan kebijakan tindak lanjut berdasarkan hasil evaluasi audit.

## 2. Tata Cara Pelaporan Audit

Laporan audit disampaikan oleh ketua tim audit kepada Tim Koordinasi. Laporan mencakup latar belakang, tujuan, lingkup, pendekatan audit, kriteria dan acuan, metoda pengumpulan data, metode analisa, hasil analisis, temuan dan kesimpulan, dan rekomendasi. Pada setiap halaman dokumen laporan hasil audit diberi identifikasi (nomor dokumen) yang menggambarkan sekurangnya: tahun pelaksanaan audit, nomor urut atau nomor seri dokumen, domain Infrastruktur SPBE, Auditee dan kode pengendalian distribusi salinan dokumen.

Draft laporan direviu oleh ketua tim audit untuk memastikan konsistensi dengan tujuan dan ruang lingkup audit. Laporan Audit disahkan oleh pimpinan APIP. Laporan Audit diterbitkan dan dibuat rangkap dengan memberi identifikasi (nomor dokumen) untuk masing-masing salinan asli. Laporan Audit didistribusikan kepada Tim Koordinasi. Laporan hasil audit disampaikan oleh Tim Koordinasi kepada Auditee dan lembaga lain sesuai kesepakatan dengan Auditee. Laporan Periodik yang berisi ringkasan hasil audit disampaikan oleh Tim Koordinasi kepada Bupati satu kali dalam satu tahun dengan format sebagai berikut:

FORMAT LAPORAN PERIODIK  
AUDIT INFRASTRUKTUR SPBE

<b>A. Penyelenggaraan Audit</b>		
Judul Audit TIK	(isi judul)	
Tanggal Laporan Audit	(isi tanggal)	
Jenis Audit	(isi jenis audit)	
Lingkup Audit	(isi lingkup audit)	
<b>Ringkasan Hasil Audit</b>		
<b>Ringkasan Temuan (parameter)</b>	<b>Ringkasan Rekomendasi (parameter)</b>	
(temuan 1) jenis dan narasi	(rekomendasi 1) narasi singkat dan tenggat waktu	
(temuan 2)	(rekomendasi 2)	
<b>B. Tindak Lanjut Audit</b>		
<b>Informasi Tindak Lanjut Audit</b>		
Rekomendasi #1	Tenggat waktu	Tindak Lanjut #1
Rekomendasi #2	Tenggat waktu	Tindak Lanjut #2
Rekomendasi #3	Tenggat waktu	Tindak Lanjut #3

Auditor dapat meminta tanggapan atau pendapat terhadap temuan, kesimpulan dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh Auditee secara tertulis dari pejabat Auditee yang bertanggung jawab. Laporan pelaksanaan audit dibuat oleh Tim Koordinasi berdasarkan hasil pelaporan oleh Tim Audit disampaikan kepada Bupati dan lembaga lain sesuai ketentuan perundangan.

3. Tata Cara Tindak Lanjut Audit

Kesepakatan proses pemantauan dilakukan dalam bentuk observasi pada Auditee pada waktu yang disepakati oleh Tim Audit dan Auditee yang sekurang-kurangnya meliputi: lingkup, objek, jangka waktu, beban pembiayaan, dan penanggung-jawab. Pemantauan dapat dilakukan oleh Tim Audit atau Auditor lain yang disepakati. Konfirmasi terhadap hasil audit dilakukan paling banyak tiga kali. Pemantauan dilakukan dalam bentuk observasi pada Auditee pada waktu yang disepakati. Tindak lanjut perbaikan dari Auditee perlu dievaluasi oleh Auditor. Evaluasi dilakukan untuk menilai apakah saran tindak lanjut yang diberikan dapat diimplementasikan dan memberikan manfaat bagi Auditee.

4. Tata Cara Pembiayaan Audit

Pembiayaan untuk pelaksanaan Audit ditanggung oleh Auditee. Besaran biaya pelaksanaan audit didasarkan pada cakupan area audit sesuai dengan kompleksitas proses bisnis. Pembiayaan dan mekanisme pelaksanaannya dapat dilakukan melalui kontrak atau swakelola sesuai ketentuan peraturan perundang-undangan.

C. Panduan Teknis Audit Infrastruktur SPBE

1. Panduan Teknis Umum Audit Infrastruktur SPBE

Ruang lingkup Panduan Teknis Umum Audit Infrastruktur SPBE adalah sebagai berikut:



- a) Tata kelola infrastruktur SPBE;
- b) Manajemen infrastruktur SPBE; dan
- c) Fungsionalitas dan kinerja infrastruktur SPBE

Ruang lingkup panduan audit tata kelola infrastruktur SPBE mencakup aktivitas:

- 1) Evaluasi;
- 2) Pengarahan; dan
- 3) Pemantauan;

Ruang lingkup panduan audit manajemen infrastruktur SPBE terdiri atas tahapan:

- a) Perencanaan;
- b) Pengembangan;
- c) Pengoperasian; dan
- d) Pemantauan.

Audit manajemen infrastruktur mencakup aktivitas:

- a) Manajemen sistem pengendalian internal;
- b) Manajemen resiko;
- c) Manajemen aset;
- d) Manajemen pengetahuan;
- e) Manajemen sdm;
- f) Manajemen layanan;
- g) Manajemen perubahan; dan
- h) Manajemen data;

Ruang lingkup panduan fungsionalitas dan kinerja infrastruktur SPBE terdiri atas tahapan:

- a) Perencanaan;
- b) Pengembangan;
- c) Pengoperasian; dan
- d) Pemeliharaan.

Hal teknis yang diaudit difokuskan pada Fungsionalitas dan Kinerja Infrastruktur SPBE.

## 2. Panduan Teknis Jaringan Intra Pemerintah

Panduan teknis audit Jaringan Intra Pemerintah dimaksudkan sebagai panduan dalam pelaksanaan audit Jaringan Intra Pemerintah, instansi pusat dan pemerintah daerah. Audit teknis Jaringan Intra Pemerintah mencakup fungsionalitas dan kinerja. Lingkup panduan teknis audit Jaringan Intra Pemerintah terdiri atas:

- a) Perencanaan Jaringan Intra Pemerintah;
- b) Pengembangan Jaringan Intra Pemerintah;
- c) Pengoperasian Jaringan Intra Pemerintah; dan
- d) Pemeliharaan Jaringan Intra Pemerintah.

Jaringan Intra Pemerintah direncanakan dengan mengacu kepada Arsitektur SPBE Nasional, Arsitektur SPBE Instansi Pusat, atau Arsitektur SPBE Pemerintah Daerah, Peta Rencana SPBE Nasional, Peta Rencana SPBE Instansi Pusat dan Peta Rencana SPBE Pemerintah Daerah. Perencanaan Jaringan Intra Pemerintah disusun berdasarkan persyaratan Jaringan Intra Pemerintah dengan mempertimbangkan kebutuhan dan infrastruktur SPBE Nasional mencakup kebutuhan bisnis, kebutuhan jaringan dan rancangan jaringan.

Jaringan intra pemerintah dapat dikembangkan oleh tim internal organisasi atau dari pihak ketiga dengan mengacu kepada deskripsi dalam rancangan. Konfigurasi jaringan SPBE dapat dikustomisasi

dan dilengkapi dengan dokumentasi yang memadai. Uji coba terhadap jaringan intra pemerintah harus terdokumentasi dalam suatu rencana pengujian (test plan), rancangan pengujian (test design), prosedur pengujian (test procedures) dan laporan pengujian (test report). Jaringan Intra Pemerintah dilengkapi dengan dokumentasi penggunaan Jaringan Intra Pemerintah baik untuk operator maupun administrator. Dokumentasi tersebut mencakup:

- a) Penggunaan perangkat Jaringan Intra Pemerintah antara lain: cara instalasi, akses terhadap perangkat, operasi terhadap perangkat;
- b) Prosedur dan Tutorials; dan
- c) Gangguan dan penanganannya.

Pemeliharaan terhadap Jaringan Intra Pemerintah didokumentasikan dalam suatu dokumen yang mencakup pemeliharaan jaringan dan manajemen konfigurasi jaringan.

### 3. Panduan Teknis Audit Sistem Penghubung Layanan Pemerintah

Panduan teknis audit Sistem Penghubung Layanan Pemerintah dimaksudkan sebagai panduan dalam pelaksanaan audit Infrastruktur SPBE. Audit teknis Sistem Penghubung Layanan Pemerintah mencakup fungsionalitas dan kinerja. Lingkup panduan teknis audit Sistem Penghubung Layanan Pemerintah terdiri atas:

- a) Perencanaan Sistem Penghubung Layanan Pemerintah;
- b) Pengembangan Sistem Penghubung Layanan Pemerintah;
- c) Pengoperasian Sistem Penghubung Layanan Pemerintah; dan
- d) Pemeliharaan Sistem Penghubung Layanan Pemerintah.

Sistem Penghubung Layanan Pemerintah direncanakan dengan mengacu kepada arsitektur SPBE nasional, arsitektur SPBE instansi pusat, atau arsitektur SPBE pemerintah daerah, peta rencana SPBE nasional, peta rencana SPBE instansi pusat dan peta rencana SPBE pemerintah daerah. Perencanaan Sistem Penghubung Layanan Pemerintah mencakup prinsip, kebijakan, dan organisasi. Sistem Penghubung Layanan Pemerintah dapat dikembangkan oleh tim internal organisasi atau dari pihak ketiga dengan mengacu kepada deskripsi dalam rancangan.

Pengembangan Sistem Penghubung Layanan Pemerintah mencakup implementasi, pengujian dan instalasi. Uji coba terhadap Sistem Penghubung Layanan Pemerintah harus terdokumentasi dalam suatu rencana pengujian (test plan), rancangan pengujian (test design), prosedur pengujian (test procedures) dan laporan pengujian (test report).

Sistem Penghubung Layanan Pemerintah dilengkapi dengan dokumentasi penggunaan Sistem Penghubung Layanan Pemerintah baik untuk operator maupun administrator. Dokumentasi tersebut mencakup penyelenggaraan dan mekanisme kerja. Pemeliharaan terhadap jaringan intra pemerintah didokumentasikan dalam suatu dokumen pemeliharaan yang mencakup:

- a) Lingkup pemeliharaan;
- b) lokasi sumber daya; dan
- c) Pencatatan kinerja.

Kriteria penilaian audit infrastruktur SPBE yang terdiri atas Tata Kelola dan Manajemen, Pusat Data/Pusat Data Nasional, Jaringan Intra Pemerintah, dan Sistem Penghubung Layanan Pemerintah tercantum dalam Keputusan Kepala Badan Pengkajian Dan Penerapan Teknologi Republik Indonesia yang akan ditetapkan secara terpisah.

**BAB X**  
**PEDOMAN AUDIT APLIKASI**  
**SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK**

**I. PENDAHULUAN**

Pemerintah perlu melakukan audit Sistem Pemerintahan Berbasis Elektronik (SPBE) sebagai upaya untuk mendukung digital government yang partisipatif, kolaboratif, berkelanjutan, dan efektif. Hasil dari audit akan membantu pemerintah dalam melakukan perbaikan kualitas infrastruktur, aplikasi, keamanan SPBE dalam jangka panjang. Audit teknologi informasi dan komunikasi merupakan proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi. Tujuannya untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan atau standar yang telah ditetapkan, termasuk peraturan perundangan yang berlaku. Ruang lingkup audit terbagi dalam tata kelola dan manajemen, fungsionalitas dan kinerja, serta aspek TIK lainnya.

Secara umum, audit teknologi memiliki lima tujuan yang bermanfaat dalam mengatasi berbagai macam permasalahan. Tujuan tersebut berupa peningkatan kinerja, penilaian kepatuhan terhadap standar teknis serta peraturan perundangan yang berlaku, dan pencegahan atas risiko penggunaan teknologi. Kemudian untuk tujuan positioning atau perencanaan serta audit teknologi untuk investigasi. Tujuan audit teknologi dalam SPBE adalah untuk peningkatan kinerja, kepatuhan, pencegahan atas risiko penggunaan teknologi, dan sekaligus untuk perencanaan. Andrari menekankan bahwa audit tujuannya bukan mencari kesalahan, namun mencari celah untuk melakukan perbaikan. "Audit teknologi tidak untuk menyalahkan, tetapi untuk melakukan perbaikan Audit TIK SPBE terdiri dari 3 kegiatan utama, yaitu; Audit Infrastruktur, Audit Aplikasi dan Audit Keamanan. Sesuai dengan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik mengatur Audit TIK, dijelaskan bahwa

1. Audit Infrastruktur terdiri dari Infrastruktur SPBE Nasional dan Infrastruktur Instansi Pusat dan Daerah
2. Audit Aplikasi terdiri dari Aplikasi Umum dan Aplikasi khusus
3. Audit Keamanan terdiri dari Keamanan Infrastruktur SPBE Nasional, Keamanan Infrastruktur Instansi Pusat dan Daerah, Keamanan Aplikasi Umum dan Keamanan Aplikasi Khusus

**II. DEFINISI**

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. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan SPBE.
3. Audit Aplikasi SPBE adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset Aplikasi SPBE dengan tujuan untuk menetapkan tingkat kesesuaian antara Aplikasi SPBE dengan kriteria dan/atau standar yang telah ditetapkan.
4. Auditor adalah orang yang memiliki kompetensi pengetahuan dan keterampilan khusus dengan tugas utama melakukan evaluasi atas pengendalian sistem elektronik yang dapat dipertanggungjawabkan secara akademis maupun praktis.
5. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, serta pemulihan data.
6. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung

untuk melakukan pertukaran layanan SPBE.

7. Pusat Data Nasional adalah sekumpulan pusat data yang digunakan secara bagi pakai oleh instansi pusat dan pemerintah daerah, dan saling terhubung.
8. Sistem Penghubung Layanan Pemerintah adalah perangkat terintegrasi yang terhubung dengan sistem penghubung layanan instansi pusat dan pemerintah daerah untuk pertukaran layanan SPBE antar instansi pusat dan/atau pemerintah daerah.
9. Lembaga Sertifikasi Profesi yang selanjutnya disingkat LSP adalah lembaga pelaksana kegiatan sertifikasi kompetensi Auditor teknologi informasi dan komunikasi dengan lingkup Audit Aplikasi SPBE.
10. Lembaga Pelaksana Audit SPBE yang selanjutnya disingkat LATIK SPBE adalah lembaga pelaksana audit SPBE.
11. Auditee adalah instansi pusat dan pemerintah daerah yang menjadi objek dari pelaksanaan Audit Aplikasi SPBE.

### **III. KEBIJAKAN PENYELENGGARAAN**

#### **A. Auditor Aplikasi SPBE**

Auditor Aplikasi SPBE merupakan Auditor Teknologi yang memiliki kemampuan teknis di bidang Aplikasi TIK. Ketua Tim Audit (Lead Auditor) wajib memiliki sertifikat kompetensi Auditor. Sertifikasi kompetensi Auditor teknologi dilaksanakan oleh Lembaga Sertifikasi Profesi (LSP) bidang kompetensi Auditor teknologi atau LSP yang mendapat pengakuan dari Badan. Pemberkasan dan penyeleksian pendaftaran Auditor dan Tim Audit SPBE dilakukan secara adil berdasarkan tanggal pemberkasan atau tanggal permintaan dan kelengkapan persyaratan berdasarkan dokumen yang valid. Pendaftaran Auditor dan Tim Audit SPBE dilakukan secara transparan dan tepat waktu. Calon Auditor SPBE mengajukan permohonan Surat Tanda Registrasi sebagai Auditor SPBE kepada Kepala Badan Riset dan Inovasi Nasional. Permohonan pendaftaran dilengkapi dengan dokumen:

1. surat permohonan;
2. sertifikat kompetensi di bidang Audit Aplikasi TIK yang mendapat pengakuan dari Badan Riset dan Inovasi Nasional.

Kepala Badan Riset dan Inovasi Nasional menetapkan Surat Tanda Registrasi Auditor SPBE paling lambat 14 (empat belas) hari kerja setelah permohonan dinyatakan valid dan lengkap. Surat Tanda Registrasi berlaku sesuai dengan masa berlaku sertifikat kompetensi Auditor Aplikasi SPBE, maksimal selama 5 tahun. Auditor SPBE yang telah memperoleh Surat Tanda Registrasi dinyatakan dalam Daftar Auditor SPBE. LATIK SPBE yang telah memperoleh surat tanda registrasi LATIK SPBE ditetapkan dengan Keputusan Kepala Badan. Surat Tanda Registrasi Auditor SPBE dinyatakan tidak berlaku apabila:

1. melanggar kode etik;
2. meninggal dunia;
3. habis masa berlaku Surat Tanda Registrasi;
4. mengundurkan diri.

Masa berlaku Surat Tanda Registrasi dapat diperpanjang dengan cara melengkapi kembali dokumen pendaftaran. Prosedur Pendaftaran Auditor.

### **IV. STANDAR PENYELENGGARAAN**

#### **A. Standar Pelaksanaan Audit Aplikasi SPBE**

Standar Audit Aplikasi SPBE merupakan batasan minimal bagi Regulator dan Auditor guna membantu dalam proses pendaftaran Auditor dan LATIK SPBE terakreditasi, pelaksanaan Audit serta prosedur yang harus dilaksanakan atau diterapkan dalam rangka pencapaian tujuan Audit. Tujuan dari Standar Audit Aplikasi SPBE adalah sebagai

berikut:

1. Menetapkan prinsip-prinsip dasar bagi pelaksanaan Audit Aplikasi SPBE;
2. Menyusun Kerangka Kerja regulasi Audit Aplikasi SPBE dalam proses pendaftaran Auditor dan Lembaga Audit Terakreditasi;
3. Menyusun Kerangka Kerja dalam pemberian layanan jasa Audit Aplikasi SPBE, guna menambah nilai kepada Auditee melalui perbaikan proses dan operasionalnya;
4. Menyusun dasar dalam melakukan evaluasi terhadap regulasi dan pelaksanaan Audit Aplikasi SPBE guna mendorong rencana perbaikan.

Standar Audit Aplikasi SPBE mencakup hal-hal sebagai berikut:

1. Standar Umum

- a) Standar Umum memberikan prinsip dasar untuk mengatur Auditor aplikasi SPBE dalam melaksanakan tugasnya, dan mengatur pendaftaran Auditor dan LATIK SPBE terakreditasi yang akan memberikan layanan jasa Audit Aplikasi SPBE sehingga pelaksanaan pekerjaan Audit Aplikasi SPBE hingga pelaporannya dapat terlaksana dengan baik dan efektif
- b) Pimpinan LATIK SPBE harus mengembangkan dan menjaga jaminan kualitas dan program peningkatan yang mencakup semua aspek pelaksanaan Audit Aplikasi SPBE.
- c) Integritas Auditor aplikasi SPBE dan pelaksana pendaftaran diwujudkan melalui sikap independen, objektif dan menjaga kerahasiaan. Dalam melaksanakan tugasnya, Auditor aplikasi SPBE dituntut untuk menjalankan hal-hal sebagai berikut:
  - 1) Memiliki pengetahuan (knowledge), keterampilan (skil), sikap (attitude) dan pengalaman (experience) yang sesuai dengan standar kompetensi Auditor, guna memenuhi tanggung jawabnya dalam pelaksanaan audit;
  - 2) Menggunakan keahlian profesionalnya dengan cermat dan seksama (due professional care) serta berhati-hati (prudent) dalam setiap penugasan;
  - 3) Senantiasa mengasah dan melatih kecermatan profesionalnya;
  - 4) Meningkatkan pengetahuan, keahlian, dan kompetensi lain yang diperlukannya dengan mengikuti pendidikan dan pelatihan berkelanjutan;
  - 5) Mematuhi prosedur yang ditetapkan dan mematuhi aturan perundangan; dan
  - 6) Memiliki pengetahuan (knowledge), keterampilan (skil), sikap (attitude) dan pengalaman (experience) yang sesuai guna memenuhi tanggung jawabnya dalam pelaksanaan audit.
- d) Tujuan, wewenang dan tanggung jawab suatu aktivitas Audit Aplikasi SPBE harus didefinisikan dengan jelas, tertuang dalam suatu dokumen formal berupa piagam audit (audit charter), surat tugas, atau dokumen-dokumen yang setara. Surat Tugas atau piagam audit (audit charter) wajib menjelaskan tujuan audit, ruang lingkup, kewenangan tim audit dan etika yang harus dipatuhi oleh tim audit.
- e) Tim Koordinasi atau pimpinan institusi pemberi tugas audit memberikan tugas kepada tim audit dalam bentuk Surat Tugas atau dapat juga berupa piagam audit (audit charter) sebelum Audit Aplikasi SPBE dilaksanakan.

2. Standar Pelaksanaan

- a) Ketua tim audit (Lead Auditor) harus secara efektif mengelola aktivitas audit untuk menjamin agar tujuan Audit Aplikasi SPBE tercapai.
- b) Ketua tim audit (Lead Auditor) harus melakukan hal-hal sebagai

berikut:

- 1) Menyusun dan menetapkan rencana audit (audit plan) guna menentukan prioritas-prioritas dalam kegiatan Audit Aplikasi SPBE yang konsisten dengan tujuan audit sesuai dengan piagam audit (audit charter);
  - 2) Menyampaikan rencana audit (audit plan) kepada pimpinan dan Auditee untuk dikaji dan diberi persetujuan, serta mengkomunikasikan dampak dari keterbatasan sumberdaya;
  - 3) Mengelola sumberdaya audit yang tepat, memadai, dan efektif untuk melaksanakan rencana audit yang telah disetujui;
  - 4) Melakukan koordinasi dengan Tim Koordinasi SPBE untuk menjamin bahwa pelaksanaan Audit Aplikasi SPBE berjalan efektif dan efisien; dan
  - 5) Memberi laporan yang memadai kepada Tim Koordinasi SPBE mengenai tujuan, wewenang, tanggung jawab, dan kinerja audit.
- c) Tim Koordinasi wajib melaksanakan Aktivitas audit Aplikasi SPBE jika:
- 1) Peningkatan kinerja birokrasi dan pelayanan publik;
  - 2) Penilaian kesesuaian dengan standar/prosedur/ pedoman dan kesesuaian dengan rencana/ kebutuhan/kondisi;
  - 3) Identifikasi status teknologi yang dimiliki, identifikasi kemampuan teknologi, termasuk dalam hal ini adalah inventarisasi dan pemetaan aset teknologi;
  - 4) Perencanaan pengembangan sistem/ teknologi dan perencanaan perbaikan kelemahan; dan/atau
  - 5) Pengungkapan suatu sebab atau fakta terkait dengan suatu kejadian atau peristiwa yang biasanya berimplikasi pada kondisi yang membahayakan keselamatan atau keamanan.
- d) Pemeriksaan yang dilakukan oleh Auditee mencakup:
- 1) Penerapan tata kelola dan manajemen Aplikasi SPBE;
  - 2) Fungsionalitas dan kinerja Aplikasi SPBE; dan
  - 3) Tingkat kepatuhan terhadap regulasi.
- e) Dalam hal merencanakan Audit Aplikasi SPBE, Auditor harus mengembangkan dan mendokumentasikan rencana untuk setiap pelaksanaan Audit Aplikasi SPBE, termasuk tujuan, lingkup, waktu, dan alokasi sumber daya bagi pelaksanaan audit. Perencanaan tersebut yang dituangkan dalam rencana audit (audit plan) dengan mempertimbangkan berbagai hal, antara lain:
- 1) Sistem pengendalian internal dan kepatuhan Auditee terhadap acuan atau benchmark;
  - 2) Penetapan tujuan Audit Aplikasi SPBE;
  - 3) Penetapan kecukupan lingkup; dan
  - 4) Penggunaan metodologi yang tepat.
- f) Dalam hal pelaksanaan audit Aplikasi SPBE, Auditor Aplikasi SPBE harus mengidentifikasi, menganalisis, mengevaluasi, dan mendokumentasikan informasi yang cukup untuk mencapai tujuan audit. Dalam melaksanakan audit tersebut, Auditor Aplikasi SPBE harus:
- 1) Memperoleh bukti-bukti audit yang cukup, handal, dan relevan untuk mendukung penilaian audit dan kesimpulan audit;
  - 2) Mendasarkan temuan dan kesimpulan audit pada analisis dan interpretasi yang memadai atas bukti-bukti audit;
  - 3) Menyiapkan, mengelola dan menyimpan data dan informasi yang diperoleh selama pelaksanaan audit; dan
  - 4) Disupervisi dengan baik untuk memastikan terjaminnya kualitas dan meningkatnya kemampuan Auditor.

- g) Dalam hal komunikasi atas hasil audit Aplikasi SPBE, Auditor Aplikasi SPBE harus mengkomunikasikan hasil pelaksanaan audit kepada pihak-pihak yang berkepentingan. Komunikasi tersebut harus mencakup tujuan dan ruang lingkup pelaksanaan audit, selain kesimpulan yang terkait, rekomendasi dan rencana tindak.
  - h) Aspek monitoring dalam aktivitas Audit Aplikasi SPBE meliputi:
    - 1) Kepatuhan terhadap Kode Etik dan Standar Audit;
    - 2) Kesesuaian terhadap Piagam Audit;
    - 3) Kesesuaian terhadap Rencana Audit; dan
    - 4) Kesesuaian terhadap Protokol Audit
  - i) Tim pengawas mutu Tim Koordinasi menyampaikan hasil monitoring kepada Bupati secara berkala. Selanjutnya, Tim Koordinasi SPBE menetapkan kebijakan tindak lanjut berdasarkan hasil monitoring.
  - j) Evaluasi mencakup perencanaan, pelaksanaan dan pelaporan audit Aplikasi SPBE. Lalu, Tim pengawas mutu audit Tim Koordinasi SPBE menyampaikan hasil evaluasi audit kepada Bupati.
3. Standar Pelaporan
- a) Laporan hasil audit dibuat oleh Tim Audit dalam bentuk dokumen laporan audit dengan tepat waktu, lengkap, akurat, objektif, meyakinkan, jelas, dan ringkas.
  - b) Laporan audit harus mencantumkan batasan atau pengecualian yang berkaitan dengan pelaksanaan audit. Auditor dapat meminta tanggapan atau pendapat terhadap temuan, kesimpulan, dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh Auditee secara tertulis dari pejabat Auditee yang bertanggung jawab.
4. Standar Tindak Lanjut
- a) Pemantauan terhadap legalitas, kompetensi, dan kinerja Tim Audit dilakukan melalui mekanisme laporan tahunan pelaksanaan audit.
  - b) Dalam kondisi pemantauan terhadap tindak lanjut akan dilaksanakan, ketua tim audit (Lead Auditor) harus menetapkan sebuah sistem pemantauan terhadap tindak lanjut temuan, kesimpulan dan rekomendasi audit oleh Auditee, mencakup cara berkomunikasi dengan Auditee, prosedur pemantauan, dan laporan status temuan.
- B. Tata Cara Pelaksanaan Audit Aplikasi SPBE
1. Tata Cara Pelaksanaan Audit
- Audit Aplikasi SPBE dilakukan Tim Audit berdasarkan permintaan Tim Koordinasi. Audit Aplikasi SPBE dilaksanakan mengikuti tata cara audit yang secara garis besar terbagi dalam tiga kelompok tahapan, yaitu:
- a) Tahap perencanaan (pre-audit);
  - b) Tahap pelaksanaan lapangan (onsite audit); dan
  - c) Tahap analisa data dan pelaporan (post audit).

Adapun tiga kelompok tersebut meliputi hal-hal sebagai berikut:

- a) Penyiapan tim audit;
- b) Quick assessment;
- c) Penyiapan rencana audit;
- d) Penyepakatan rencana audit;
- e) Penyiapan protokol audit;
- f) Penetapan parameter acuan;
- g) Pertemuan pembukaan;
- h) Pelaksanaan lapangan;

- i) Pertemuan penutupan;
- j) Analisa data;
- k) Pengelolaan data;
- l) Penyusunan laporan;
- m) Proof-read laporan;
- n) Penyerahan laporan; dan
- o) Evaluasi aktivitas

Audit Aplikasi SPBE dilakukan oleh sebuah tim audit yang terdiri dari posisi-posisi berikut dengan uraian tugas dan tanggung jawab sebagai berikut:

- a) Pengawas mutu, berperan melakukan monitoring dan evaluasi aktivitas audit untuk menjamin pelaksanaan audit sesuai dengan standar audit. Pengawas mutu harus memiliki kualifikasi Auditor teknologi utama atau yang setara;
- b) Lead Auditor, bertanggung jawab merencanakan audit teknologi, melaksanakan audit di lapangan, mengendalikan data dan melaporkan hasil audit teknologi. Lead Auditor harus mempunyai kualifikasi minimal setara dengan Auditor teknologi madya;
- c) Auditor, bertugas membantu Lead Auditor dalam aktivitas audit teknologi. Auditor harus mempunyai kualifikasi minimal setara dengan Auditor teknologi muda;
- d) Asisten Auditor, bertugas membantu Auditor dalam aktivitas audit teknologi;
- e) Teknisi, bertugas membantu Auditor dalam pengumpulan data lapangan;
- f) Narasumber, berperan memberi masukan yang berkaitan dengan isu, status teknologi, dan keilmuan yang relevan.
- g) Quick Assessment dilakukan untuk mengenali objek audit dengan mengidentifikasi: current issue, lokasi organisasi yang diaudit, struktur organisasi dari organisasi yang diaudit, proses bisnis dari organisasi, atau bagian yang diaudit.

Tim Audit Aplikasi SPBE harus merencanakan tindakan audit dengan mendefinisikan hal-hal berikut:

- a) Tujuan audit;
- b) Lingkup;
- c) Pendekatan;
- d) Kriteria;
- e) Parameter;
- f) Acuan;
- g) Metode pengumpulan data;
- h) Penentuan objek;
- i) Data primer dan sekunder;
- j) Metode analisa;
- k) Deliverable; dan
- l) Perkiraan jadwal pelaksanaan.

Hal-hal tersebut harus dicantumkan dalam Rencana Audit (Audit Plan). Ketua tim audit dan Auditee harus menyepakati rencana audit sebelum tahap pelaksanaan audit. Dalam pelaksanaan kegiatan audit, tim Audit Aplikasi SPBE harus:

- a) Menyusun protokol audit yang berisi detail instrument audit, antara lain:
  - (1) Daftar data, pertanyaan dan pengujian
  - (2) Formulir untuk mencatat data, jawaban, hasil observasi dan



- hasil pengujian;
- b) Menetapkan parameter acuan untuk setiap kriteria diperlukan untuk memberikan suatu acuan perbandingan;
  - c) Melakukan pertemuan pembukaan dengan Auditee;
  - d) Melaksanakan audit lapangan, melalui:
    - (1) Penelaahan dokumen;
    - (2) Wawancara;
    - (3) Observasi lapangan;
    - (4) Pengujian; dan
    - (5) Verifikasi bukti;
  - e) Melakukan pertemuan penutupan dengan Auditee;
  - f) Melakukan analisis bukti; dan
  - g) Mengelola data.

Data status teknologi SPBE dikumpulkan secara objektif berdasarkan fakta yang ada pada Auditee. Deskripsi data dan informasi yang dikumpulkan mengikuti kriteria. Temuan Audit Aplikasi SPBE merupakan keadaan dimana fakta status aset teknologi SPBE Auditee tidak sesuai dengan persyaratan Aplikasi SPBE. Auditor dapat mengurangi atau menambahkan lingkup sepanjang relevan dengan objek dan rencana penggunaan hasil audit sesuai kebutuhan Auditee.

Monitoring memberikan informasi untuk suatu kegiatan audit yang sedang berjalan yang bertujuan untuk mengidentifikasi kemajuan dalam pelaksanaan audit. Monitoring dilakukan oleh tim pengawas mutu. Tim pengawas mutu harus menetapkan suatu proses tindak lanjut untuk memonitor dan meyakinkan bahwa tindak lanjut yang telah ditetapkan oleh Tim Audit diimplementasikan secara efektif. Tim pengawas mutu dapat berasal dari pihak eksternal. Evaluasi secara menyeluruh dilakukan setelah aktivitas audit selesai yang bertujuan untuk mengetahui kelebihan dan kekurangan aktivitas audit yang telah dilakukan dalam rangka meningkatkan kualitas pelaksanaan audit berikutnya. Evaluasi dilakukan oleh tim pengawas mutu setelah aktivitas audit selesai. Tim Pengawas mutu menyampaikan hasil evaluasi audit kepada Tim Koordinasi. Tim Koordinasi menetapkan kebijakan tindak lanjut berdasarkan hasil evaluasi audit.

#### 5. Tata Cara Pelaporan Audit

Laporan audit disampaikan oleh ketua tim audit kepada Tim koordinasi. Laporan mencakup latar belakang, tujuan, lingkup, pendekatan audit, kriteria dan acuan, metoda pengumpulan data, metode analisa, hasil analisis, temuan dan kesimpulan, dan rekomendasi. Pada setiap halaman dokumen laporan hasil audit diberi identifikasi (nomor dokumen) yang menggambarkan sekurang-kurangnya: tahun pelaksanaan audit, nomor urut atau nomor seri dokumen, domain Aplikasi SPBE, Auditee dan kode pengendalian distribusi salinan dokumen.

Draft laporan direviu oleh ketua tim audit untuk memastikan konsistensi dengan tujuan dan ruang lingkup audit. Laporan Audit disahkan oleh pimpinan APIP. Laporan Audit diterbitkan dan dibuat rangkap dengan memberi identifikasi (nomor dokumen) untuk masing-masing salinan asli. Laporan Audit didistribusikan kepada Tim Koordinasi. Laporan hasil audit disampaikan oleh Tim Koordinasi kepada Auditee dan lembaga lain sesuai kesepakatan dengan Auditee. Laporan Periodik yang berisi ringkasan hasil audit disampaikan oleh Tim Koordinasi kepada Bupati satu kali dalam satu tahun dengan format sebagai berikut:

FORMAT LAPORAN PERIODIK  
AUDIT APLIKASI SPBE

<b>A. Penanggung Jawab Penyelenggaraan Audit</b>	
Nama	(isi nama lengkap)
Jabatan	(isi jabatan resmi)
NIP #3	(isi Nomor induk pegawai)
Kontak	(isi nomor telepon dan surel ybs)

<b>A. Penyelenggaraan Audit</b>	
Judul Audit TIK	(isi judul)
Tanggal Laporan Audit	(isi tanggal)
Jenis Audit	(isi jenis audit)
Lingkup Audit	(isi lingkup audit)
<b>Ringkasan Hasil Audit</b>	
<b>Ringkasan Temuan (parameter)</b>	<b>Ringkasan Rekomendasi (parameter)</b>
(temuan 1) jenis dan narasi	(rekomendasi 1) narasi singkat dan tenggat waktu
(temuan 2)	(rekomendasi 2)

<b>B. Tindak Lanjut Audit</b>		
<b>Informasi Tindak Lanjut Audit</b>		
Rekomendasi #1	Tenggat waktu	Tindak Lanjut #1
Rekomendasi #2	Tenggat waktu	Tindak Lanjut #2
Rekomendasi #3	Tenggat waktu	Tindak Lanjut #3

kesimpulan dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh Auditee secara tertulis dari pejabat Auditee yang bertanggung jawab. Laporan pelaksanaan audit dibuat oleh Tim Koordinasi berdasarkan hasil pelaporan oleh Tim Audit disampaikan kepada Bupati dan lembaga lain sesuai ketentuan perundangan.

6. Tata Cara Tindak Lanjut Audit

Kesepakatan proses pemantauan dilakukan dalam bentuk observasi pada Auditee pada waktu yang disepakati oleh Tim Audit dan Auditee yang sekurang-kurangnya meliputi: lingkup, objek, jangka waktu, beban pembiayaan, dan penanggung-jawab. Pemantauan dapat dilakukan oleh Tim Audit atau Auditor lain yang disepakati. Konfirmasi terhadap hasil audit dilakukan paling banyak tiga kali. Pemantauan dilakukan dalam bentuk observasi pada Auditee pada waktu yang disepakati. Tindak lanjut perbaikan dari Auditee perlu dievaluasi oleh Auditor. Evaluasi dilakukan untuk menilai apakah saran tindak lanjut yang diberikan dapat diimplementasikan dan memberikan manfaat bagi Auditee.

7. Tata Cara Pembiayaan Audit

Pembiayaan untuk pelaksanaan Audit ditanggung oleh Auditee. Besaran biaya pelaksanaan audit didasarkan pada cakupan area audit sesuai dengan kompleksitas proses bisnis. Pembiayaan dan

mekanisme pelaksanaannya dapat dilakukan melalui kontrak atau swakelola sesuai ketentuan peraturan perundang-undangan.

### C. Panduan Teknis Audit Aplikasi SPBE

#### 1. Panduan Teknis Umum Audit Aplikasi SPBE

Panduan teknis Audit Aplikasi SPBE dimaksudkan sebagai acuan dalam menetapkan lingkup area audit aplikasi, kriteria audit, dan penilaian status teknologi aplikasi SPBE.

Ruang lingkup panduan audit tata kelola Aplikasi SPBE mencakup aktivitas:

- a) Evaluasi Tata Kelola;
- b) Pengarahan Tata Kelola; Dan
- c) Pemantauan Tata Kelola;

Audit Manajemen Aplikasi mencakup Aktivitas:

- a) Manajemen Sistem Pengendalian Internal;
- b) Manajemen Resiko;
- c) Manajemen Aset;
- d) Manajemen Pengetahuan;
- e) Manajemen Sdm;
- f) Manajemen Layanan;
- g) Manajemen Perubahan; Dan
- h) Manajemen Data;

Ruang Lingkup Panduan Fungsionalitas dan Kinerja Aplikasi SPBE terdiri atas tahapan:

- a) Perencanaan Aplikasi;
- b) Pengembangan Aplikasi;
- c) Pengoperasian Aplikasi; dan
- d) Pemeliharaan Aplikasi.

Perencanaan Aplikasi disusun dalam suatu dokumen menggunakan basis spesifikasi yang mencakup unsur:

- a) Kemampuan Aplikasi; dan
- b) Persyaratan Proses Bisnis Pemerintah Daerah.

Kemampuan Aplikasi mengacu kepada:

- a) Arsitektur SPBE secara berjenjang; dan
- b) Persyaratan Bisnis Organisasi.

Arsitektur SPBE terdiri atas arsitektur SPBE Nasional, arsitektur SPBE instansi pusat atau arsitektur SPBE pemerintah daerah. Persyaratan proses bisnis Auditee dirumuskan dengan mempertimbangkan kebutuhan, peluang dan proses bisnis. Persyaratan tersebut diterjemahkan ke dalam persyaratan aplikasi yang mencakup kebutuhan fungsi, antarmuka, data, kinerja dan batasan rancangan.

Rancangan aplikasi disusun berdasarkan persyaratan aplikasi serta memperhatikan kesesuaiannya terhadap ketentuan perundangan dan integrasi data. Rancangan tersebut beserta penjelasannya didokumentasikan sebagai Dokumen Deskripsi Rancangan Aplikasi. Aplikasi SPBE dikembangkan oleh tim internal Auditee dan/atau pihak ketiga dengan mengacu kepada dokumen Deskripsi Rancangan Aplikasi. Kode sumber (source code) aplikasi harus dilengkapi dengan dokumentasi yang memadai. Kode sumber (source code) aplikasi menggunakan open source, dapat dikustomisasi dan dilengkapi dengan dokumentasi yang memadai. Pengembangan aplikasi SPBE

harus disertai dengan uji coba fungsionalitasnya. Pembangunan aplikasi harus didokumentasikan dalam dokumen Prosedur Pembangunan Aplikasi (System build procedures) yang dilengkapi dengan panduan instalasi aplikasi untuk menerapkan aplikasi di lingkungan sistem yang ada. Aplikasi yang dikembangkan mengacu pada ketentuan perundangan yang berlaku.

Pengembangan aplikasi harus dilengkapi dengan dokumentasi penggunaan aplikasi dan tanggungjawab data pengguna. Penggunaan aplikasi mencakup pengguna dengan klasifikasi end-users, dan administrator. Dokumentasi penggunaan aplikasi mencakup:

- a) Penggunaan aplikasi secara umum, antara lain: cara instalasi, akses terhadap aplikasi, operasi terhadap data;
- b) Tutorials;
- c) Dokumen Teknis; dan
- d) Pesan kesalahan dan penanganannya. (Troubleshooting).

Kinerja pengoperasian aplikasi dapat dievaluasi dari fungsi komponen perangkat lunak Sistem Elektronik yang digunakan untuk menjalankan SPBE.

Kinerja sistem elektronik untuk mendukung fungsi Auditee dikelompokkan ke dalam 3 klasifikasi, yaitu:

- a) Mampu mendukung semua fungsi proses bisnis Auditee;
- b) Mampu mendukung sebagian fungsi proses bisnis Auditee; dan
- c) Belum mampu mendukung fungsi proses bisnis Auditee.

Pemeliharaan terhadap aplikasi didokumentasikan dalam suatu dokumen pemeliharaan yang mencakup:

- a) Lingkup pemeliharaan;
- b) Alokasi sumberdaya;
- c) Pencatatan kinerja; dan
- d) Urutan/rangkaian proses pemeliharaan.

Perubahan terhadap aplikasi didokumentasikan dalam suatu dokumen Software Configuration Management yang mencakup:

- a) Lingkup konfigurasi;
- b) Aktivitas dan manajemen konfigurasi;
- c) Sumberdaya konfigurasi; dan
- d) Penjadwalan manajemen konfigurasi.

**BAB XI**  
**PEDOMAN AUDIT KEAMANAN**  
**SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK**

**I. PENDAHULUAN**

Pemerintah perlu melakukan audit Sistem Pemerintahan Berbasis Elektronik (SPBE) sebagai upaya untuk mendukung digital government yang partisipatif, kolaboratif, berkelanjutan, dan efektif. Hasil dari audit akan membantu pemerintah dalam melakukan perbaikan kualitas infrastruktur, aplikasi, keamanan SPBE dalam jangka panjang. Audit teknologi informasi dan komunikasi merupakan proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi. Tujuannya untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan atau standar yang telah ditetapkan, termasuk peraturan perundangan yang berlaku. Ruang lingkup audit terbagi dalam tata kelola dan manajemen, fungsionalitas dan kinerja, serta aspek TIK lainnya.

Secara umum, audit teknologi memiliki lima tujuan yang bermanfaat dalam mengatasi berbagai macam permasalahan. Tujuan tersebut berupa peningkatan kinerja, penilaian kepatuhan terhadap standar teknis serta peraturan perundangan yang berlaku, dan pencegahan atas risiko penggunaan teknologi. Kemudian untuk tujuan positioning atau perencanaan serta audit teknologi untuk investigasi. Tujuan audit teknologi dalam SPBE adalah untuk peningkatan kinerja, kepatuhan, pencegahan atas risiko penggunaan teknologi, dan sekaligus untuk perencanaan. Andrari menekankan bahwa audit tujuannya bukan mencari kesalahan, namun mencari celah untuk melakukan perbaikan. "Audit teknologi tidak untuk menyalahkan, tetapi untuk melakukan perbaikan Audit TIK SPBE terdiri dari 3 kegiatan utama, yaitu; Audit Infrastruktur, Audit Aplikasi dan Audit Keamanan. Sesuai dengan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik mengatur Audit TIK, dijelaskan bahwa

1. Audit Infrastruktur terdiri dari Infrastruktur SPBE Nasional dan Infrastruktur Instansi Pusat dan Daerah
2. Audit Aplikasi terdiri dari Aplikasi Umum dan Aplikasi khusus
3. Audit Keamanan terdiri dari Keamanan Infrastruktur SPBE Nasional, Keamanan Infrastruktur Instansi Pusat dan Daerah, Keamanan Aplikasi Umum dan Keamanan Aplikasi Khusus

**II. DEFINISI**

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. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
3. Audit Keamanan SPBE adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset Keamanan SPBE dengan tujuan untuk menetapkan tingkat kesesuaian antara Keamanan SPBE dengan kriteria dan/atau standar yang telah ditetapkan.
4. Auditor adalah orang yang memiliki kompetensi pengetahuan dan keterampilan khusus dengan tugas utama melakukan evaluasi atas pengendalian sistem elektronik yang dapat dipertanggungjawabkan secara akademis maupun praktis.
5. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan,

- penyimpanan dan pengolahan data, serta pemulihan data.
6. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.
  7. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran layanan SPBE.
  8. Pusat Data Nasional adalah sekumpulan pusat data yang digunakan secara bagi pakai oleh instansi pusat dan pemerintah daerah, dan saling terhubung.
  9. Jaringan Intra Pemerintah adalah jaringan interkoneksi tertutup yang menghubungkan antar jaringan intra instansi pusat dan pemerintah daerah.
  10. Sistem Penghubung Layanan Pemerintah adalah perangkat terintegrasi yang terhubung dengan sistem penghubung layanan instansi pusat dan pemerintah daerah untuk pertukaran layanan SPBE antar instansi pusat dan/atau pemerintah daerah.
  11. Lembaga Sertifikasi Profesi yang selanjutnya disingkat LSP adalah lembaga pelaksana kegiatan sertifikasi kompetensi Auditor teknologi informasi dan komunikasi dengan lingkup Audit Keamanan SPBE.
  12. Lembaga Pelaksana Audit SPBE yang selanjutnya disingkat LATIK SPBE adalah lembaga pelaksana audit SPBE.
  13. Auditee adalah instansi pusat dan pemerintah daerah yang menjadi objek dari pelaksanaan Audit Keamanan SPBE.

### **III. KEBIJAKAN PENYELENGGARAAN**

#### **A. Auditor Keamanan SPBE**

Auditor Keamanan SPBE merupakan Auditor Teknologi yang memiliki kemampuan teknis di bidang keamanan TIK. Ketua Tim Audit (Lead Auditor) wajib memiliki sertifikat kompetensi Auditor. Sertifikasi kompetensi Auditor teknologi dilaksanakan oleh Lembaga Sertifikasi Profesi (LSP) bidang kompetensi Auditor teknologi atau LSP yang mendapat pengakuan dari Badan. Pemberkasan dan penyeleksian pendaftaran Auditor dan Tim Audit SPBE dilakukan secara adil berdasarkan tanggal pemberkasan atau tanggal permintaan dan kelengkapan persyaratan berdasarkan dokumen yang valid. Pendaftaran Auditor dan Tim Audit SPBE dilakukan secara transparan dan tepat waktu.

Calon Auditor SPBE mengajukan permohonan Surat Tanda Registrasi sebagai Auditor SPBE kepada Kepala Badan Riset dan Inovasi Nasional. Permohonan pendaftaran dilengkapi dengan dokumen:

1. surat permohonan;
2. sertifikat kompetensi di bidang Audit Keamanan TIK yang mendapat pengakuan dari Badan Riset dan Inovasi Nasional.

Kepala Badan Riset dan Inovasi Nasional menetapkan Surat Tanda Registrasi Auditor SPBE paling lambat 14 (empat belas) hari kerja setelah permohonan dinyatakan valid dan lengkap. Surat Tanda Registrasi berlaku sesuai dengan masa berlaku sertifikat kompetensi Auditor Keamanan SPBE, maksimal selama 5 tahun. Auditor SPBE yang telah memperoleh Surat Tanda Registrasi dinyatakan dalam Daftar Auditor SPBE. LATIK SPBE yang telah memperoleh surat tanda registrasi LATIK SPBE ditetapkan dengan Keputusan Kepala Badan. Surat Tanda Registrasi Auditor SPBE dinyatakan tidak berlaku apabila:

1. melanggar kode etik;
2. meninggal dunia;
3. habis masa berlaku Surat Tanda Registrasi;
4. mengundurkan diri.

Masa berlaku Surat Tanda Registrasi dapat diperpanjang dengan cara melengkapi kembali dokumen pendaftaran. Prosedur Pendaftaran

Auditor.

#### **IV. STANDAR PENYELENGGARAAN**

##### **A. Standar Pelaksanaan Audit Keamanan SPBE**

Standar Audit Keamanan SPBE merupakan batasan minimal bagi Regulator dan Auditor guna membantu dalam proses pendaftaran Auditor dan LATIK SPBE terakreditasi, pelaksanaan Audit serta prosedur yang harus dilaksanakan atau diterapkan dalam rangka pencapaian tujuan Audit. Tujuan dari Standar Audit Keamanan SPBE adalah sebagai berikut:

1. Menetapkan prinsip-prinsip dasar bagi pelaksanaan Audit Keamanan SPBE;
2. Menyusun Kerangka Kerja regulasi Audit Keamanan SPBE dalam proses pendaftaran Auditor dan Lembaga Audit Terakreditasi;
3. Menyusun Kerangka Kerja dalam pemberian layanan jasa Audit Keamanan SPBE, guna menambah nilai kepada Auditee melalui perbaikan proses dan operasionalnya;
4. Menyusun dasar dalam melakukan evaluasi terhadap regulasi dan pelaksanaan Audit Keamanan SPBE guna mendorong rencana perbaikan.

Standar Audit Keamanan SPBE mencakup hal-hal sebagai berikut:

1. Standar Umum
  - a) Standar Umum memberikan prinsip dasar untuk mengatur Auditor Keamanan SPBE dalam melaksanakan tugasnya, dan mengatur pendaftaran Auditor dan LATIK SPBE terakreditasi yang akan memberikan layanan jasa Audit Keamanan SPBE sehingga pelaksanaan pekerjaan Audit Keamanan SPBE hingga pelaporannya dapat terlaksana dengan baik dan efektif
  - b) Pimpinan LATIK SPBE harus mengembangkan dan menjaga jaminan kualitas dan program peningkatan yang mencakup semua aspek pelaksanaan Audit Keamanan SPBE.
  - c) Integritas Auditor Keamanan SPBE dan pelaksana pendaftaran diwujudkan melalui sikap independen, objektif dan menjaga kerahasiaan. Dalam melaksanakan tugasnya, Auditor Keamanan SPBE dituntut untuk menjalankan hal-hal sebagai berikut:
    - 1) Memiliki pengetahuan (knowledge), keterampilan (skil), sikap (attitude) dan pengalaman (experience) yang sesuai dengan standar kompetensi Auditor, guna memenuhi tanggung jawabnya dalam pelaksanaan audit;
    - 2) Menggunakan keahlian profesionalnya dengan cermat dan seksama (due professional care) serta berhati-hati (prudent) dalam setiap penugasan;
    - 3) Senantiasa mengasah dan melatih kecermatan profesionalnya;
    - 4) Meningkatkan pengetahuan, keahlian, dan kompetensi lain yang diperlukannya dengan mengikuti pendidikan dan pelatihan berkelanjutan;
    - 5) Mematuhi prosedur yang ditetapkan dan mematuhi aturan perundangan; dan
    - 6) Memiliki pengetahuan (knowledge), keterampilan (skil), sikap (attitude) dan pengalaman (experience) yang sesuai guna memenuhi tanggung jawabnya dalam pelaksanaan audit.
  - d) Tujuan, wewenang dan tanggung jawab suatu aktivitas Audit Keamanan SPBE harus didefinisikan dengan jelas, tertuang dalam suatu dokumen formal berupa piagam audit (audit charter), surat tugas, atau dokumen-dokumen yang setara. Surat Tugas atau piagam audit (audit charter) wajib menjelaskan tujuan audit,

ruang lingkup, kewenangan tim audit dan etika yang harus dipatuhi oleh tim audit.

- e) Tim Koordinasi atau pimpinan institusi pemberi tugas audit memberikan tugas kepada tim audit dalam bentuk Surat Tugas atau dapat juga berupa piagam audit (audit charter) sebelum Audit Keamanan SPBE dilaksanakan.
2. Standar Pelaksanaan
- a) Ketua tim audit (Lead Auditor) harus secara efektif mengelola aktivitas audit untuk menjamin agar tujuan Audit Keamanan SPBE tercapai.
  - b) Ketua tim audit (Lead Auditor) harus melakukan hal-hal sebagai berikut:
    - 1) Menyusun dan menetapkan rencana audit (audit plan) guna menentukan prioritas-prioritas dalam kegiatan Audit Keamanan SPBE yang konsisten dengan tujuan audit sesuai dengan piagam audit (audit charter);
    - 2) Menyampaikan rencana audit (audit plan) kepada pimpinan dan Auditee untuk dikaji dan diberi persetujuan, serta mengkomunikasikan dampak dari keterbatasan sumberdaya;
    - 3) Mengelola sumberdaya audit yang tepat, memadai, dan efektif untuk melaksanakan rencana audit yang telah disetujui;
    - 4) Melakukan koordinasi dengan Tim Koordinasi SPBE untuk menjamin bahwa pelaksanaan Audit Keamanan SPBE berjalan efektif dan efisien; dan
    - 5) Memberi laporan yang memadai kepada Tim Koordinasi SPBE mengenai tujuan, wewenang, tanggung jawab, dan kinerja audit.
  - c) Tim Koordinasi wajib melaksanakan Aktivitas audit Keamanan SPBE jika:
    - 1) Peningkatan kinerja birokrasi dan pelayanan publik;
    - 2) Penilaian kesesuaian dengan standar/prosedur/ pedoman dan kesesuaian dengan rencana/ kebutuhan/kondisi;
    - 3) Identifikasi status teknologi yang dimiliki, identifikasi kemampuan teknologi, termasuk dalam hal ini adalah inventarisasi dan pemetaan aset teknologi;
    - 4) Perencanaan pengembangan sistem/ teknologi dan perencanaan perbaikan kelemahan; dan/atau
    - 5) Pengungkapan suatu sebab atau fakta terkait dengan suatu kejadian atau peristiwa yang biasanya berimplikasi pada kondisi yang membahayakan keselamatan atau keamanan.
  - d) Pemeriksaan yang dilakukan oleh Auditee mencakup:
    - 1) Penerapan tata kelola dan manajemen Keamanan SPBE;
    - 2) Fungsionalitas dan kinerja Keamanan SPBE; dan
    - 3) Tingkat kepatuhan terhadap regulasi.
  - e) Dalam hal merencanakan Audit Keamanan SPBE, Auditor harus mengembangkan dan mendokumentasikan rencana untuk setiap pelaksanaan Audit Keamanan SPBE, termasuk tujuan, lingkup, waktu, dan alokasi sumber daya bagi pelaksanaan audit. Perencanaan tersebut yang dituangkan dalam rencana audit (audit plan) dengan mempertimbangkan berbagai hal, antara lain:
    - 1) Sistem pengendalian internal dan kepatuhan Auditee terhadap acuan atau benchmark;
    - 2) Penetapan tujuan Audit Keamanan SPBE;
    - 3) Penetapan kecukupan lingkup; dan
    - 4) Penggunaan metodologi yang tepat.
  - f) Dalam hal pelaksanaan audit Keamanan SPBE, Auditor Keamanan SPBE harus mengidentifikasi, menganalisis, mengevaluasi, dan mendokumentasikan informasi yang cukup untuk mencapai



tujuan audit. Dalam melaksanakan audit tersebut, Auditor Keamanan SPBE harus:

- 1) Memperoleh bukti-bukti audit yang cukup, handal, dan relevan untuk mendukung penilaian audit dan kesimpulan audit;
  - 2) Mendasarkan temuan dan kesimpulan audit pada analisis dan interpretasi yang memadai atas bukti-bukti audit;
  - 3) Menyiapkan, mengelola dan menyimpan data dan informasi yang diperoleh selama pelaksanaan audit; dan
  - 4) Disupervisi dengan baik untuk memastikan terjaminnya kualitas dan meningkatnya kemampuan Auditor.
- g) Dalam hal komunikasi atas hasil audit Keamanan SPBE, Auditor Keamanan SPBE harus mengkomunikasikan hasil pelaksanaan audit kepada pihak-pihak yang berkepentingan. Komunikasi tersebut harus mencakup tujuan dan ruang lingkup pelaksanaan audit, selain kesimpulan yang terkait, rekomendasi dan rencana tindak.
- h) Aspek monitoring dalam aktivitas Audit Keamanan SPBE meliputi:
- 5) Kepatuhan terhadap Kode Etik dan Standar Audit;
  - 6) Kesesuaian terhadap Piagam Audit;
  - 7) Kesesuaian terhadap Rencana Audit; dan
  - 8) Kesesuaian terhadap Protokol Audit
- i) Tim pengawas mutu Tim Koordinasi menyampaikan hasil monitoring kepada Bupati secara berkala. Selanjutnya, Tim Koordinasi SPBE menetapkan kebijakan tindak lanjut berdasarkan hasil monitoring.
- j) Evaluasi mencakup perencanaan, pelaksanaan dan pelaporan audit Keamanan SPBE. Lalu, Tim pengawas mutu audit Tim Koordinasi SPBE menyampaikan hasil evaluasi audit kepada Bupati.
3. Standar Pelaporan
- a) Laporan hasil audit dibuat oleh Tim Audit dalam bentuk dokumen laporan audit dengan tepat waktu, lengkap, akurat, objektif, meyakinkan, jelas, dan ringkas.
  - b) Laporan audit harus mencantumkan batasan atau pengecualian yang berkaitan dengan pelaksanaan audit. Auditor dapat meminta tanggapan atau pendapat terhadap temuan, kesimpulan, dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh Auditee secara tertulis dari pejabat Auditee yang bertanggung jawab.
4. Standar Tindak Lanjut
- a) Pemantauan terhadap legalitas, kompetensi, dan kinerja Tim Audit dilakukan melalui mekanisme laporan tahunan pelaksanaan audit.
  - b) Dalam kondisi pemantauan terhadap tindak lanjut akan dilaksanakan, ketua tim audit (Lead Auditor) harus menetapkan sebuah sistem pemantauan terhadap tindak lanjut temuan, kesimpulan dan rekomendasi audit oleh Auditee, mencakup cara berkomunikasi dengan Auditee, prosedur pemantauan, dan laporan status temuan.

## B. Tata Cara Pelaksanaan Audit Keamanan SPBE

### 1. Tata Cara Pelaksanaan Audit

Audit Keamanan SPBE dilakukan Tim Audit berdasarkan permintaan Tim Koordinasi. Audit Keamanan SPBE dilaksanakan mengikuti tata cara audit yang secara garis besar terbagi dalam tiga kelompok tahapan, yaitu:

- a) Tahap perencanaan (pre-audit);

- b) Tahap pelaksanaan lapangan (onsite audit); dan
- c) Tahap analisa data dan pelaporan (post audit).

Adapun tiga kelompok tersebut meliputi hal-hal sebagai berikut:

- a) Penyiapan tim audit;
- b) Quick assessment;
- c) Penyiapan rencana audit;
- d) Penyepakatan rencana audit;
- e) Penyiapan protokol audit;
- f) Penetapan parameter acuan;
- g) Pertemuan pembukaan;
- h) Pelaksanaan lapangan;
- i) Pertemuan penutupan;
- j) Analisa data;
- k) Pengelolaan data;
- l) Penyusunan laporan;
- m) Proof-read laporan;
- n) Penyerahan laporan; dan
- o) Evaluasi aktivitas

Audit Keamanan SPBE dilakukan oleh sebuah tim audit yang terdiri dari posisi-posisi berikut dengan uraian tugas dan tanggung jawab sebagai berikut:

- a) Pengawas mutu, berperan melakukan monitoring dan evaluasi aktivitas audit untuk menjamin pelaksanaan audit sesuai dengan standar audit. Pengawas mutu harus memiliki kualifikasi Auditor teknologi utama atau yang setara;
- b) Lead Auditor, bertanggung jawab merencanakan audit teknologi, melaksanakan audit di lapangan, mengendalikan data dan melaporkan hasil audit teknologi. Lead Auditor harus mempunyai kualifikasi minimal setara dengan Auditor teknologi madya;
- c) Auditor, bertugas membantu Lead Auditor dalam aktivitas audit teknologi. Auditor harus mempunyai kualifikasi minimal setara dengan Auditor teknologi muda;
- d) Asisten Auditor, bertugas membantu Auditor dalam aktivitas audit teknologi;
- e) Teknisi, bertugas membantu Auditor dalam pengumpulan data lapangan;
- f) Narasumber, berperan memberi masukan yang berkaitan dengan isu, status teknologi, dan keilmuan yang relevan.
- g) Quick Assessment dilakukan untuk mengenali objek audit dengan mengidentifikasi: current issue, lokasi organisasi yang diaudit, struktur organisasi dari organisasi yang diaudit, proses bisnis dari organisasi, atau bagian yang diaudit.

Tim Audit Keamanan SPBE harus merencanakan tindakan audit dengan mendefinisikan hal-hal berikut:

- a) Tujuan audit;
- b) Lingkup;
- c) Pendekatan;
- d) Kriteria;
- e) Parameter;
- f) Acuan;
- g) Metode pengumpulan data;
- h) Penentuan objek;
- i) Data primer dan sekunder;
- j) Metode analisa;
- k) Deliverable; dan

l) Perkiraan jadwal pelaksanaan.

Hal-hal tersebut harus dicantumkan dalam Rencana Audit (Audit Plan). Ketua tim audit dan Auditee harus menyepakati rencana audit sebelum tahap pelaksanaan audit. Dalam pelaksanaan kegiatan audit, tim Audit Infrastruktur SPBE harus:

- a) Menyusun protokol audit yang berisi detail instrument audit, antara lain:
  - (1) Daftar data, pertanyaan dan pengujian
  - (2) Formulir untuk mencatat data, jawaban, hasil observasi dan hasil pengujian;
- b) Menetapkan parameter acuan untuk setiap kriteria diperlukan untuk memberikan suatu acuan perbandingan;
- c) Melakukan pertemuan pembukaan dengan Auditee;
- d) Melaksanakan audit lapangan, melalui:
  - (1) Penelaahan dokumen;
  - (2) Wawancara;
  - (3) Observasi lapangan;
  - (4) Pengujian; dan
  - (5) Verifikasi bukti;
- e) Melakukan pertemuan penutupan dengan Auditee;
- f) Melakukan analisis bukti; dan
- g) Mengelola data.

Data status teknologi SPBE dikumpulkan secara objektif berdasarkan fakta yang ada pada Auditee. Deskripsi data dan informasi yang dikumpulkan mengikuti kriteria. Temuan Audit Infrastruktur SPBE merupakan keadaan dimana fakta status aset teknologi SPBE Auditee tidak sesuai dengan persyaratan infrastruktur SPBE. Auditor dapat mengurangi atau menambahkan lingkup sepanjang relevan dengan objek dan rencana penggunaan hasil audit sesuai kebutuhan Auditee.

Monitoring memberikan informasi untuk suatu kegiatan audit yang sedang berjalan yang bertujuan untuk mengidentifikasi kemajuan dalam pelaksanaan audit. Monitoring dilakukan oleh tim pengawas mutu. Tim pengawas mutu harus menetapkan suatu proses tindak lanjut untuk memonitor dan meyakinkan bahwa tindak lanjut yang telah ditetapkan oleh Tim Audit diimplementasikan secara efektif. Tim pengawas mutu dapat berasal dari pihak eksternal. Evaluasi secara menyeluruh dilakukan setelah aktivitas audit selesai yang bertujuan untuk mengetahui kelebihan dan kekurangan aktivitas audit yang telah dilakukan dalam rangka meningkatkan kualitas pelaksanaan audit berikutnya. Evaluasi dilakukan oleh tim pengawas mutu setelah aktivitas audit selesai. Tim Pengawas mutu menyampaikan hasil evaluasi audit kepada Tim Koordinasi. Tim Koordinasi menetapkan kebijakan tindak lanjut berdasarkan hasil evaluasi audit.

8. Tata Cara Pelaporan Audit

Laporan audit disampaikan oleh ketua tim audit kepada Tim Koordinasi. Laporan mencakup latar belakang, tujuan, lingkup, pendekatan audit, kriteria dan acuan, metoda pengumpulan data, metode analisa, hasil analisis, temuan dan kesimpulan, dan rekomendasi. Pada setiap halaman dokumen laporan hasil audit diberi identifikasi (nomor dokumen) yang menggambarkan sekurang-kurangnya: tahun pelaksanaan audit, nomor urut atau nomor seri dokumen, domain Keamanan SPBE, Auditee dan kode pengendalian distribusi salinan dokumen.

Draft laporan direviu oleh ketua tim audit untuk memastikan

konsistensi dengan tujuan dan ruang lingkup audit. Laporan Audit disahkan oleh pimpinan APIP. Laporan Audit diterbitkan dan dibuat rangkap dengan memberi identifikasi (nomor dokumen) untuk masing-masing salinan asli. Laporan Audit didistribusikan kepada Tim Koordinasi. Laporan hasil audit disampaikan oleh Tim Koordinasi kepada Auditee dan lembaga lain sesuai kesepakatan dengan Auditee. Laporan Periodik yang berisi ringkasan hasil audit disampaikan oleh Tim Koordinasi kepada Bupati satu kali dalam satu tahun dengan format sebagai berikut:

**FORMAT LAPORAN PERIODIK  
AUDIT KEAMANAN SPBE**

<b>A. Penanggung Jawab Penyelenggaraan Audit</b>	
Nama	(isi nama lengkap)
Jabatan	(isi jabatan resmi)
NIP	(isi Nomor induk pegawai)
Kontak	(isi nomor telepon dan surel ybs)

<b>A. Penyelenggaraan Audit</b>	
Judul Audit TIK	(isi judul)
Tanggal Laporan Audit	(isi tanggal)
Jenis Audit	(isi jenis audit)
Lingkup Audit	(isi lingkup audit)
<b>Ringkasan Hasil Audit</b>	
<b>Ringkasan Temuan (parameter)</b>	<b>Ringkasan Rekomendasi (parameter)</b>
(temuan 1) jenis dan narasi	(rekomendasi 1) narasi singkat dan tenggat waktu
(temuan 2)	(rekomendasi 2)

<b>B. Tindak Lanjut Audit</b>		
<b>Informasi Tindak Lanjut Audit</b>		
Rekomendasi #1	Tenggat waktu	Tindak Lanjut #1
Rekomendasi #2	Tenggat waktu	Tindak Lanjut #2
Rekomendasi #3	Tenggat waktu	Tindak Lanjut #3

kesimpulan dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh Auditee secara tertulis dari pejabat Auditee yang bertanggung jawab. Laporan pelaksanaan audit dibuat oleh Tim Koordinasi berdasarkan hasil pelaporan oleh Tim Audit disampaikan kepada Bupati dan lembaga lain sesuai ketentuan perundangan.

9. Tata Cara Tindak Lanjut Audit

Kesepakatan proses pemantauan dilakukan dalam bentuk observasi pada Auditee pada waktu yang disepakati oleh Tim Audit dan Auditee yang sekurang-kurangnya meliputi: lingkup, objek, jangka waktu, beban pembiayaan, dan penanggung-jawab. Pemantauan dapat dilakukan oleh Tim Audit atau Auditor lain yang disepakati. Konfirmasi terhadap hasil audit dilakukan paling banyak tiga kali.

Pemantauan dilakukan dalam bentuk observasi pada Auditee pada waktu yang disepakati. Tindak lanjut perbaikan dari Auditee perlu dievaluasi oleh Auditor. Evaluasi dilakukan untuk menilai apakah saran tindak lanjut yang diberikan dapat diimplementasikan dan memberikan manfaat bagi Auditee.

#### 10. Tata Cara Pembiayaan Audit

Pembiayaan untuk pelaksanaan Audit ditanggung oleh Auditee. Besaran biaya pelaksanaan audit didasarkan pada cakupan area audit sesuai dengan kompleksitas proses bisnis. Pembiayaan dan mekanisme pelaksanaannya dapat dilakukan melalui kontrak atau swakelola sesuai ketentuan peraturan perundang-undangan.

### C. Panduan Teknis Audit Keamanan SPBE

#### 1. Panduan Teknis Umum Audit Keamanan SPBE

Panduan teknis Audit Keamanan SPBE dimaksudkan sebagai acuan dalam menetapkan lingkup area audit keamanan, kriteria audit, dan penilaian status teknologi Keamanan SPBE.

Ruang lingkup panduan audit tata kelola Keamanan SPBE mencakup aktivitas:

- a) Evaluasi Tata Kelola;
- b) Pengarahan Tata Kelola; Dan
- c) Pemantauan Tata Kelola;

Audit Manajemen Keamanan mencakup Aktivitas:

- a) Manajemen Sistem Pengendalian Internal;
- b) Manajemen Resiko;
- c) Manajemen Aset;
- d) Manajemen Pengetahuan;
- e) Manajemen Sdm;
- f) Manajemen Layanan;
- g) Manajemen Perubahan; Dan
- h) Manajemen Data;

Ruang Lingkup Panduan Fungsionalitas dan Kinerja Keamanan SPBE terdiri atas tahapan:

- a) Perencanaan Keamanan;
- b) Pengembangan Keamanan;
- c) Pengoperasian Keamanan; dan
- d) Pemeliharaan Keamanan.

Perencanaan Keamanan disusun dalam suatu dokumen menggunakan basis spesifikasi yang mencakup unsur:

- a) Kemampuan Keamanan; dan
- b) Persyaratan Proses Bisnis Pemerintah Daerah.

Kemampuan Keamanan mengacu kepada:

- a) Arsitektur SPBE secara berjenjang; dan
- b) Persyaratan Bisnis Organisasi.

Arsitektur SPBE terdiri atas arsitektur SPBE Nasional, arsitektur SPBE instansi pusat atau arsitektur SPBE pemerintah daerah. Persyaratan proses bisnis Auditee dirumuskan dengan mempertimbangkan kebutuhan, peluang dan proses bisnis. Persyaratan tersebut diterjemahkan ke dalam persyaratan keamanan yang mencakup kebutuhan fungsi, antarmuka, data, kinerja dan batasan rancangan.

Rancangan keamanan disusun berdasarkan persyaratan keamanan

serta memperhatikan kesesuaiannya terhadap ketentuan perundangan dan integrasi data. Rancangan tersebut beserta penjelasannya didokumentasikan sebagai Dokumen Deskripsi Rancangan Keamanan. Keamanan SPBE dikembangkan oleh tim internal Auditee dan/atau pihak ketiga dengan mengacu kepada dokumen Deskripsi Rancangan Keamanan. Pengembangan keamanan SPBE harus disertai dengan uji coba fungsionalitasnya. Pembangunan keamanan harus didokumentasikan dalam dokumen Prosedur Pembangunan keamanan (Safety build procedures) yang dilengkapi dengan panduan instalasi keamanan untuk menerapkan keamanan di lingkungan sistem yang ada. Keamanan yang dikembangkan mengacu pada ketentuan perundangan yang berlaku. Pengembangan keamanan harus dilengkapi dengan dokumentasi penggunaan keamanan dan tanggungjawab data pengguna. Penggunaan keamanan mencakup pengguna dengan klasifikasi end-users, dan administrator. Dokumentasi penggunaan keamanan mencakup:

- a) Penggunaan keamanan secara umum, antara lain: cara instalasi, akses terhadap keamanan, operasi terhadap infrastruktur dan aplikasi;
- b) Tutorials;
- c) Dokumen Teknis; dan
- d) Pesan kesalahan dan penanganannya. (Troubleshooting).

Kinerja pengoperasian keamanan dapat dievaluasi dari fungsi komponen perangkat lunak Sistem Elektronik yang digunakan untuk menjalankan SPBE.

Kinerja sistem elektronik untuk mendukung fungsi Auditee dikelompokkan ke dalam 3 klasifikasi, yaitu:

- a) Mampu mendukung semua fungsi proses bisnis Auditee;
- b) Mampu mendukung sebagian fungsi proses bisnis Auditee; dan
- c) Belum mampu mendukung fungsi proses bisnis Auditee.

Pemeliharaan terhadap keamanan didokumentasikan dalam suatu dokumen pemeliharaan yang mencakup:

- a) Lingkup pemeliharaan;
- b) Alokasi sumberdaya;
- c) Pencatatan kinerja; dan
- d) Urutan/rangkaian proses pemeliharaan.

Perubahan terhadap keamanan didokumentasikan dalam suatu dokumen Safety Configuration Management yang mencakup:

- a) Lingkup konfigurasi;
- b) Aktivitas dan manajemen konfigurasi;
- c) Sumberdaya konfigurasi; dan
- d) Penjadwalan manajemen konfigurasi.

#### D. Instrumen Audit Keamanan

Informasi Umum Domain Audit Keamanan SPBE			
A. Jenis	Sederhana	Sedang	Kompleks
Aplikasi SPBE	Aplikasi Khusus Instansi Pusat	Aplikasi Khusus Pemerintah Daerah	Aplikasi Umum SPBE Nasional
Pusat Data Nasional	Instansi Pusat	Pemerintah Daerah	Nasional
Jaringan Intra	Instansi Pusat	Pemerintah Daerah	Nasional
Sistem Penghubung Layanan	Instansi Pusat	Pemerintah Daerah	Nasional
B. Umum			
Jumlah Personil TI	< 5 orang	6-10 orang	> 10 orang
Jumlah Pengguna	< 100 pengguna	100-1000 pengguna	> 1000 pengguna

Jenis Dampak Kegagalan	Operasional saja	Operasional dan Finansial	Operasional, Finansial, dan Legal
<b>C. Aplikasi SPBE</b>			
Sebaran peladen	Terpusat	Terdistribusi Dalam Negeri	Terdistribusi Dalam & Luar Negeri
Platform Teknologi	1 jenis	2-3 jenis	> 3 jenis
Waktu Pengembangan	< 3 bulan	3-12 bulan	> 12 bulan
Usia Sistem	< 1 tahun	1-3 tahun	> 3 tahun
Transaksi per hari	< 5000	5000 s.d. 50.000	> 50.000
Pola Pemrosesan	<i>Batch</i>	<i>Realtime</i>	<i>Hybrid</i>
Cakupan Proses Bisnis	< 30 %	30-60%	> 60%
<b>D. Pusat Data Nasional</b>			
Pengelolaan	Alih Daya, Sewa	Mandiri	Campuran
Strata SNI	Strata 1-2	Strata 3	Strata 4
Sertifikasi	Belum Ada	SNI 27001	SNI 27001 dan Standar Lain
<b>E. Jaringan Intra</b>			
Pengelolaan	Alih Daya, Sewa	Mandiri	Campuran
Cakupan Jaringan	<i>Local Area Network, Campus Area Network</i>	<i>Metropolitan Area Network, Virtual Private Network</i>	<i>Wide Area Network, Nasional</i>
Media Jaringan	Kabel	Nirkabel	Kabel & Nirkabel
<b>F. Sistem Penghubung Layanan</b>			
Cakupan Sistem	Intra Instansi Pusat atau Intra Pemerintah Daerah	Antar Instansi Pusat atau Antar Pemerintah Daerah	Nasional
Sifat Sistem	Tertutup	Semi Terbuka	Terbuka
Konten Sistem	Data	Aplikasi	Layanan
Sifat Informasi	Terbuka	Terbatas	Tertutup

## **BAB XII PENUTUP**

Di dalam kegiatan Pemantauan dan Evaluasi SPBE, penilaian tingkat kematangan atas penerapan SPBE pada Instansi Pusat dan Pemerintah Daerah mengukur kapabilitas proses yang mencakup kebijakan SPBE, proses tata kelola SPBE, dan proses manajemen SPBE serta mengukur kapabilitas layanan yang mencakup layanan administrasi pemerintahan berbasis elektronik dan layanan publik berbasis elektronik. Nilai tingkat kematangan atas penerapan SPBE yang direpresentasikan dalam bentuk indeks SPBE menunjukkan kemampuan Instansi Pusat dan Pemerintah Daerah dalam penerapan SPBE.

Untuk memudahkan memahami tingkat kemampuan, nilai indeks SPBE dikelompokkan ke dalam 5 (lima) predikat yaitu memuaskan, sangat baik, baik, cukup, dan kurang. Hasil penilaian atas penerapan SPBE pada Instansi Pusat dan Pemerintah Daerah dapat digunakan oleh Instansi Pusat dan Pemerintah Daerah sebagai acuan untuk melakukan perbaikan penerapan SPBE dan peningkatan kualitas layanan SPBE, serta dapat digunakan sebagai landasan penyusunan kebijakan SPBE nasional. Keikutsertaan Instansi Pusat dan Pemerintah Daerah secara berkesinambungan dalam kegiatan Pemantauan dan Evaluasi SPBE menjadi penting untuk dapat mengukur kemajuan penerapan SPBE.

Sebagai bagian dari penilaian Reformasi Birokrasi, hasil penilaian pada kegiatan Pemantauan dan Evaluasi SPBE turut berperan dalam mendorong Instansi Pusat dan Pemerintah Daerah untuk penerapan tata kelola pemerintahan yang baik. Hal ini mencerminkan bahwa SPBE turut berkontribusi dalam penerapan sistem, proses, dan prosedur kerja yang transparan, efektif, efisien, dan terukur sehingga tata kelola pemerintahan berbasis elektronik dapat diwujudkan.

Pedoman pada Domain Manajemen SPBE ini ditetapkan agar setiap unit kerja di lingkungan Pemerintah Kabupaten Jombang memiliki acuan dalam melaksanakan Penerapan SPBE di lingkungannya masing-masing.

**BUPATI JOMBANG,**



**MUNDJIDAH WAHAB**