SALINAN

BUPATI ROKAN HULU
PROVINSI RIAU

PERATURAN BUPATI ROKAN HULU
NOMOR 34 TAHUN 2024

TENTANG

PERUBAHAN ATAS PERATURAN BUPATI ROKAN HULU NOMOR 17 TAHUN 2022 TENTANG PENYELENGGARAAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PEMERINTAH KABUPATEN ROKAN HULU

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI ROKAN HULU,

Menimbang :

a. bahwa dalam rangka pelaksanaan sistem Pemerintahan Berbasis Elektronik maka perlu didukung oleh pengendalian keamanan informasi yang terpadu sehingga Peraturan Bupati Rokan Hulu Nomor 17 Tahun 2022 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Rokan Hulu, perlu diubah;
b. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a, perlu ditetapkan dengan Peraturan Bupati Rokan Hulu Tentang Perubahan atas Peraturan Bupati Rokan Hulu Nomor 17 Tahun 2022 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Rokan Hulu;

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang - Undang Nomor 53 Tahun 1999 tentang Pembentukan Kabupaten Pelalawan, Kabupaten Rokan Hulu, Kabupaten Rokan Hilir, Kabupaten Siak, Kabupaten Karimun, Kabupaten Natuna, Kabupaten Kuantan Singingi dan Kota Batam sebagaimana telah diubah beberapa kali, terakhir dengan Undang-Undang Republik Indonesia Nomor 34 Tahun 2008 tentang Perubahan Ketiga Atas Undang -Undang Republik Indonesia Nomor 53 Tahun 1999 (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 107, Tambahan Lembaran Negara Republik Indonesia Nomor 4880);
3. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008, Tambahan Lembaran Negara Republik Indonesia Nomor 5952); sebagaimana telah diubah dengan Undang- undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);

4. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
5. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan perundang- undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234); sebagaimana telah diubah dengan undang-undang republik Indonesia nomor 15 tahun 2019 tentang perubahan atas undang-undang republik Indonesia nomor 12 tahun 2011 (lembaga Negara republik indonesia tahun 2019 nomor 183, tambahan lembaran Negara Republik Indonesia Nomor 6398);
6. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali, terakhir dengan Undang-Undang Republik Indonesia Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
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 Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 994);
10. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik;
11. Peraturan Daerah Kabupaten Rokan Hulu Nomor 4 Tahun 2009 tentang Rencana Pembangunan Jangka Panjang Daerah (RPJPD) Kabupaten Rokan Hulu Tahun 2005-2025;
12. Peraturan Bupati Rokan Hulu Nomor 17 Tahun 2022 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Rokan Hulu.

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG PERUBAHAN ATAS PERATURAN BUPATI ROKAN HULU NOMOR 17 TAHUN 2022 TENTANG PENYELENGGARAAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PEMERINTAH KABUPATEN ROKAN HULU.

Pasal I

Beberapa ketentuan dalam Peraturan Bupati Rokan Hulu Nomor 17 Tahun 2022 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Rokan Hulu (Berita Daerah Kabupaten Rokan Hulu Tahun 2022 Nomor 17) diubah sebagai berikut :

1. Ketentuan Pasal 1 diubah sehingga berbunyi sebagai berikut :

Pasal 1

Dalam Peraturan Bupati ini, yang dimaksud dengan:
1. Daerah adalah Kabupaten Rokan Hulu.
2. Pemerintah Daerah adalah Pemerintah Kabupaten Rokan Hulu.
3. Bupati adalah Bupati Rokan Hulu.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Rokan Hulu.
5. Perangkat Daerah adalah Perangkat Daerah di Lingkungan Pemerintah Kabupaten Rokan Hulu.
6. Dinas adalah Dinas Komunikasi dan Informatika Kabupaten Rokan Hulu.
7. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
8. Tata Kelola SPBE adalah kerangka kerja yang memastikan terlaksananya pengaturan, pengarahan dan pengendalian dalam penerapan SPBE secara terpadu.
9. Manajemen SPBE adalah serangkaian proses untuk mencapai penerapan SPBE yang efektif, efisien dan berkesinambungan, serta layanan SPBE yang berkualitas.
10. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
11. Arsitektur SPBE Pemerintah Daerah adalah kerangka dasar yang mendeskripsikan integrasi proses bisnis, data dan informasi,
12. Peta Rencana SPBE Pemerintah Daerah adalah dokumen yang mendeskripsikan arah dan langkah penyiapan dan pelaksanaan SPBE yang terintegrasi.
13. Proses Bisnis adalah sekumpulan kegiatan yang terstruktur dan saling terkait dalam pelaksanaan tugas dan fungsi instansi pusat dan pemerintah daerah masing-masing.
14. 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.
15. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data dan pemulihan data.
16. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik atau pun nonelektronik.
17. Interoperabilitas adalah koordinasi dan kolaborasi antara proses bisnis dan antara sistem elektronik, dalam rangka pertukaran data, informasi atau layanan SPBE.

18. Jaringan Intra Pemerintah Daerah Adalah Jaringan Tertutup Yang Menghubungkan Antara Simpul Jaringan Dalam Pemerintah Daerah.
19. Jaringan antar Perangkat Daerah (WAN) adalah jaringan yang menghubungkan antar perangkat daerah.
20. Jaringan antar Perangkat Daerah (LAN) adalah jaringan yang menghubungkan komputer dengan perangkat pendukungnya dan dapat berkomunikasi didalam Perangkat Daerah.
21. Perangkat khusus Perangkat Daerah adalah perangkat khusus yang di butuhkan oleh Perangkat Daerah tertentu guna mendukung uraian tugas pokok dan fungsi antara lain seperti system sensor, radio frequency identification (RFID), dan sejenisnya.
22. System penghubung layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran layanan SPBE.
23. Aplikasi SPBE adalah satu atau sekumpulan programkomputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan SPBE.
24. Aplikasi umum adalah aplikasi SPBE yang sama, standard, dan digunakan secara bagi pakai oleh instansi pusat dan pemerintah daerah lain.
25. Aplikasi khusus adalah aplikasi SPBE yang dibangun, dikembangkan, digunakan, dan dikelola oleh instansi pusat atau pemeritah daerah tertentu untuk mememuhi kebutuhan khusus yang bukan kebutuhan instansi pusat dan pemerintah daerah lain.
26. Aplikasi khusus berbagi pakai adalah aplikasi khusus yang digunakan oleh satu Perangkat Daerah.
27. Aplikasi khusus Perangkat Daerah adalah aplikasi khusus yang digunakan oleh satu Perangkat Daerah.
28. Repositori Adalah tempat penyimpanan aplikasi, source-code, dan berbagai dokumentasi aplikasi lainnya.
29. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
30. Pelayanan level 1, yang selanjutnya disebut dengan service desctier 2 adalah staf atau unit di PD yang memiliki tugas dan wewenang sebagai pihak pertama yang dihubungi layanan TIK (single poin contact) untuk selanjutnya menyelesaikan permasalahan TIK dan PD pemilik layanan.
31. Pelayanan level 2, yang selanjutnya disebut dengan service desk ties 2 Adalah unit di dinas ynag memiliki tugas dan wewenang menyelesaikan permasalahan TIK PD yang tidak mampu di selesaikan oleh service desktier1.
32. Audit teknologi informasi dan komunikasi adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap asset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriterian dan / atau standaryang telah ditetapkan.
33. Teknologi informasi dan komunikasi, yang selanjutnya di singkat TIK adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, membuat laporan menganalisis memindahkan informasi dan / atau menyebarkan informasi antar media.
34. Perangkat Daerah mandiri TIK adalah Perangkat Daerah yang dinilai telah mampu membangun, dan mengelola aplikasi dan/ atau insfrastruktur SPBE.
35. Perangkat Daerah pemilik layanan Perangkat Daerah berdasarkan uraian tugas dan fungsinya merupakan penanggung-jawab layanan dimaksud.
36. Sumberdaya manusia teknologi informasi komunikasi, yang selanjutnya disingkat sumber daya manusia TIK adalah pegawai pada setiap Perangkat Daerah yang berhubungan dengan pengelolaan teknologi informasi dan komunikasi.

37. Instansi pusat adalah kementrian, lembaga pemerintah nonkementrian, kesekretariatan lembaga Negara, kesekretariatan lembaga nonstruktural, dan lembaga pemerintah lainnya.
38. *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.
39. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
40. Pusat Data Daerah adalah sekumpulan Pusat Data yang digunakan secara bagi pakai oleh Pemerintah Daerah, dan saling terhubung.

2. Pasal 25 diubah sehingga berbunyi sebagai berikut :

Pasal 25

(1) Keamanan SPBE mencakup penjaminan kerahasiaan, penjaminan keutuhan, penjaminan ketersediaan, penjaminan keaslian dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan informasi, Infrastruktur SPBE dan Aplikasi SPBE;
(2) Penjaminan kerahasiaan sebagaimana dimaksud pada ayat (1) dilakukan melalui penetapan klasifikasi keamanan, pembatasan akses dan pengendalian keamanan lainnya.
(3) Penjaminan keutuhan sebagaimana dimaksud pada ayat (1) dilakukan melalui pendeteksian modifikasi;
(4) Penjaminan ketersediaan sebagaimana dimaksud pada ayat(1) dilakukan melalui penyediaan cadangan dan pemulihan;
(5) Penjaminan keaslian sebagaimana dimaksud pada ayat (1) dilakukan melalui penyediaan mekanisme verifikasi dan validasi;
(6) Penjaminan kenirsangkalan (nonrepudiation) sebagaimana dimaksud pada ayat (1) dilakukan melalui penerapan tanda tangan digital dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat digital;
(7) Standar teknis dan prosedur keamanan Aplikasi SPBE sebagaimana dimaksud pada ayat (1) diterapkan pada:
    a. aplikasi berbasis web; dan
    b. aplikasi berbasis *mobile*.
(8) Aplikasi berbasis web sebagaimana dimaksud pada ayat (7) huruf a merupakan aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet.
(9) Aplikasi berbasis *mobile* sebagaimana dimaksud pada ayat (7) huruf b merupakan aplikasi yang dalam pengoperasiannya dapat berjalan diperangkat bergerak, dan memiliki sistem operasi yang mendukung perangkat lunak secara *standalone*.
(10) Aplikasi SPBE sebagaimana dimaksud pada ayat (1) harus dilakukan pengujian keamanan setiap periode tertentu yang dilakukan dengan:
    a. mengidentifikasi persyaratan minimum keamanan yang belum diterapkan;
    b. memastikan pengkodean pemrograman aplikasi yang dibuat tidak memiliki kerawanan;
    c. melakukan pemindaian otomatis dan/atau pengujian penetrasi sistem;
    d. mengidentifikasi kerentanan dan mengelola ancaman sejak awal siklus pengembangan Aplikasi SPBE; dan menganalisis kerentanan.

3. Pasal 26 diubah sehingga berbunyi sebagai berikut :

Pasal 26

(1) Perangkat Daerah harus menerapkan keamanan SPBE sebagaimana dimaksud dalam Pasal 25 ayat (1).
(2) Dalam menerapkan Keamanan SPBE dan menyelesaikan permasalahan keamanan SPBE, Perangkat Daerah dapat melakukan konsultasi dan/atau koordinasi dengan Perangkat Daerah yang bertanggungjawab di bidang persandian.
(3) Penerapan Keamanan SPBE harus memenuhi standar teknis dan prosedur keamanan SPBE yang ditetapkan oleh dinas.
(4) Standar teknis dan prosedur Keamanan SPBE sebagaimana dimaksud dalam Pasal 26 ayat (3) diterapkan diterapkan untuk:
    a. keamanan data dan informasi;
    b. keamanan Aplikasi SPBE;
    c. keamanan Sistem Penghubung Layanan;
    d. keamanan Jaringan Intra; dan
    e. keamanan Pusat Data Daerah.
(5) Standar teknis dan prosedur Keamanan SPBE sebagaimana dimaksud pada ayat (4) tercantum dalam lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini;
(6) dalam melaksanakan teknis SPBE sebagaimana dimaksud pada ayat (4) dibentuk tim;
(7) Tim sebagaimana dimaksud pada ayat (6) ditetapkan dengan Keputusan Bupati.

4. Pasal 33 diubah sehingga berbunyi sebagai berikut :

Pasal 33

(1) Manajemen keamanan informasi sebagaimana dimaksud dalam Pasal 31 ayat (1) huruf b, bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan informasi;
(2) Manajemen keamanan informasi sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses yang meliputi penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja dan perbaikan berkelanjutan terhadap keamanan informasi dalam SPBE;
(3) Manajemen keamanan informasi sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan pedoman manajemen keamanan informasi SPBE yang ditetapkan sesuai ketentuan peraturan perundang-undangan;
(4) Pemerintah daerah menggunakan tanda tangan elektronik sesuai ketentuan peraturan perundang-undangan;
(5) Dalam pelaksanaan manajemen keamanan informasi, PD berkoordinasi dan dapat melakukan konsultasi dengan dinas.
(6) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (2) dilakukan dengan cara :
    a. Menentukan isu internal keamanan informasi SPBE dalam organisasi; dan
    b. Menentukan isu eksternal keamanan informasi SPBE.
(7) Isu internal keamanan informasi SPBE dalam organisasi sebagaimana dimaksud pada ayat (1) huruf a didefinisikan berdasarkan area yang menjadi prioritas organisasi terhadap pelaksanaan kemanan informasi SPBE.

(8) Area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) paling sedikit meliputi :
   a. data dan informasi SPBE;
   b. aplikasi SPBE;
   c. aset infrastruktur SPBE; dan
   d. kebijakan keamanan informasi SPBE yang telah dimiliki.

(9) Isu eksternal keamanan informasi SPBE sebagaimana dimaksud pada ayat (6) huruf b didefinisikan sesuai dengan ketentuan peraturan Perundang-undangan; dan

(10) Proses sebagaimana dimaksud dalam ayat (2) tercantum dalam lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal II

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Rokan Hulu.

Ditetapkan di Pasir Pengaraian
pada tanggal 27 Agustus 2024

BUPATI ROKAN HULU,

ttd

S U K I M A N

Diundangkan di Pasir Pengaraian
pada tanggal 27 Agustus 2024

SEKRETARIS DAERAH
KABUPATEN ROKAN HULU,

ttd

MUHAMMAD ZAKI

BERITA DAERAH KABUPATEN ROKAN HULU TAHUN 2024 NOMOR : 34

Salinan sesuai aslinya,
KEPALA BAGIAN HUKUM,

H. ERINALDI, SH, MH
Pembina IV.a
NIP. 19840916 201001 1 008

LAMPIRAN I
PERATURAN BUPATI ROKAN HULU
NOMOR 34 TAHUN 2024
TENTANG
PERUBAHAN ATAS PERATURAN BUPATI ROKAN HULU NOMOR 17 TAHUN 2022 TENTANG PENYELENGGARAAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PEMERINTAH KABUPATEN ROKAN HULU

STANDAR TEKNIS DAN PROSEDUR KEAMANAN SPBE

Standar teknis dan prosedur keamanan Aplikasi SPBE, yang menjadi acuan bagi Perangkat Daerah di lingkungan Pemerintah Kabupaten Rokan Hulu dalam implementasi keamanan aplikasi SPBE.

I. Standar teknis keamanan data dan informasi terdiri atas terpenuhinya aspek:
   a. kerahasiaan;
   b. keaslian;
   c. keutuhan;
   d. kenirsangkalan; dan
   e. ketersediaan.
   1. Aspek kerahasiaan dilakukan dengan prosedur:
      a) menetapkan klasifikasi informasi;
      b) menerapkan enkripsi dengan sistem kriptografi; dan
      c) menerapkan pembatasan akses terhadap data dan informasi sesuai dengan kewenangan dan kebijakan yang telah ditetapkan.
   2. Aspek keaslian dilakukan dengan prosedur:
      a) menyediakan mekanisme verifikasi;
      b) menyediakan mekanisme validasi; dan
      c) menerapkan sistem *hash function.*
   3. Aspek keutuhan dilakukan dengan prosedur:
      a) menerapkan pendeteksian modifikasi; dan
      b) menerapkan tanda tangan elektronik tersertifikasi.
   4. Aspek kenirsangkalan dilakukan dengan prosedur:
      a) menerapkan tanda tangan elektronik tersertifikasi; dan
      b) penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.
   5. Aspek ketersediaan dilakukan dengan prosedur:
      a) menerapkan sistem pencadangan secara berkala;
      b) membuat perencanaan untuk menjamin data dan informasi dapat selalu diakses; dan
      c) menerapkan sistem pemulihan.

II. Standar teknis keamanan aplikasi berbasis web terdiri atas terpenuhinya fungsi:
   a. autentikasi;
   b. manajemen sesi;
   c. persyaratan kontrol akses;
   d. validasi input;
   e. kriptografi pada verifikasi statis;
   f. penanganan eror dan pencatatan log;
   g. proteksi data;
   h. keamanan komunikasi;
   i. pengendalian kode berbahaya;
   j. logika bisnis;

k. *file*;
l. keamanan API dan *web service*; dan
m. keamanan konfigurasi.

1. Fungsi autentikasi dilakukan dengan prosedur:
   a) menggunakan manajemen kata sandi untuk proses autentikasi;
   b) menerapkan verifikasi kata sandi pada sisi server;
   c) mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;
   d) mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;
   e) mengatur mekanisme pemulihan kata sandi;
   f) menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi; dan
   g) menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.
2. Fungsi manajemen sesi dilakukan dengan prosedur:
   a) menggunakan pengendali sesi untuk proses manajemen sesi;
   b) menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;
   c) mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi;
   d) mengatur kondisi dan jangka waktu habis sesi;
   e) validasi dan pencantuman *session id*;
   f) pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi; dan
   g) pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna.
3. Fungsi persyaratan kontrol akses dilakukan dengan prosedur:
   a) menetapkan otorisasi pengguna untuk membatasi kontrol akses;
   b) mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi;
   c) mengatur antarmuka pada sisi administrator; dan
   d) mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan.
4. Fungsi validasi input dilakukan dengan prosedur:
   a) menerapkan fungsi validasi input pada sisi server;
   b) menerapkan mekanisme penolakan input jika terjadi kesalahan validasi;
   c) memastikan *runtime environment* aplikasi tidak rentan terhadap serangan validasi input;
   d) melakukan validasi positif pada seluruh input;
   e) melakukan filter terhadap data yang tidak dipercaya;
   f) menggunakan fitur kode dinamis;
   g) melakukan pelindungan terhadap akses yang mengandung konten skrip; dan
   h) melakukan pelindungan dari serangan injeksi basis data.
5. Fungsi kriptografi pada verifikasi statis dilakukan dengan prosedur:
   a) menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang- undangan;
   b) melakukan autentikasi data yang dienkripsi;
   c) menerapkan manajemen kunci kriptografi; dan
   d) membuat angka acak yang menggunakan generator angka acak kriptografi.

6. Fungsi penanganan eror dan pencatatan log dilakukan dengan prosedur:
   a) mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;
   b) menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani;
   c) tidak mencantumkan informasi yang dikecualikan dalam pencatatan log;
   d) mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;
   e) mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah;
   f) melakukan enkripsi pada data yang disimpan untuk mencegah injeksi log; dan
   g) melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.
7. Fungsi proteksi data dilakukan dengan prosedur:
   a) melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;
   b) melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi;
   c) melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan;
   d) melakukan penentuan jumlah parameter;
   e) memastikan data disimpan dengan aman;
   f) menentukan metode untuk menghapus dan engekspor data sesuai permintaan pengguna; dan
   g) membersihkan memori setelah tidak diperlukan.
8. Fungsi keamanan komunikasi dilakukan dengan prosedur:
   a) menggunakan komunikasi terenkripsi;
   b) mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna;
   c) mengatur jenis algoritma yang digunakan dan alat pengujiannya; dan
   d) mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik.
   e) Fungsi pengendalian kode berbahaya dilakukan dengan prosedur:
   f) menggunakan analisis kode dalam kontrol kode berbahaya;
   g) memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan;
   h) mengatur izin terkait fitur atau sensor terkait privasi;
   i) mengatur pelindungan integritas; dan
   j) mengatur mekanisme fitur pembaruan.
9. Fungsi logika bisnis dilakukan dengan prosedur:
   a) memproses alur logika bisnis dalam urutan langkah dan waktu yang realistis;
   b) memastikan logika bisnis memiliki batasan dan validasi;
   c) memonitor aktivitas yang tidak biasa;
   d) membantu dalam kontrol antiotomatisasi; dan
   e) memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.
10. Fungsi *file* dilakukan dengan prosedur:
   a) mengatur jumlah *file* untuk setiap pengguna dan kuota ukuran *file* yang diunggah;
   b) melakukan validasi *file* sesuai dengan tipe konten yang diharapkan;

c) melakukan pelindungan terhadap metadata input dan metadata *file*;
d) melakukan pemindaian *file* yang diperoleh dari sumber yang tidak dipercaya; dan
e) melakukan konfigurasi server untuk mengunduh *file* sesuai ekstensi yang ditentukan.

11. Fungsi keamanan API dan *web service* dilakukan dengan prosedur:
    a) melakukan konfigurasi layanan web;
    b) memverifikasi *uniform resource identifier* API tidak menampilkan informasi yang berpotensi sebagai celah keamanan;
    c) membuat keputusan otorisasi;
    d) menampilkan metode RESTful *hypertext transfer protocol* apabila input pengguna dinyatakan valid;
    e) menggunakan validasi skema dan verifikasi sebelum menerima input;
    f) menggunakan metode pelindungan layanan berbasis web; dan
    g) menerapkan kontrol antiotomatisasi.
12. Fungsi keamanan konfigurasi dilakukan dengan prosedur:
    a) Mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan;
    b) mendokumentasi, menyalin konfigurasi, dan semua dependensi;
    c) menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan;
    d) memvalidasi integritas aset jika aset aplikasi diakses secara eksternal; dan
    e) menggunakan respons aplikasi dan konten yang aman.

III. Standar teknis keamanan aplikasi berbasis mobile terdiri atas terpenuhinya fungsi:
    a. penyimpanan data dan persyaratan privasi;
    b. kriptografi;
    c. autentikasi dan manajemen sesi;
    d. komunikasi jaringan;
    e. interaksi platform;
    f. kualitas kode dan pengaturan *build;* dan
    g. ketahanan.

1. Prosedur penyimpanan data dan persyaratan privasi dilakukan dengan:
    a) menyimpan seluruh data dan informasi yang dikecualikan hanya dalam fasilitas penyimpanan kredensial sistem;
    b) membatasi pertukaran data dan informasi yang dikecualikan dengan *third party;*
    c) menonaktifkan *cache keyboard* pada saat memasukkan data dan informasi yang dikecualikan;
    d) melindungi informasi yang dikecualikan saat terjadi *inter process communication;* dan
    e) melindungi data dan informasi yang dikecualikan yang dimasukkan melalui antarmuka pengguna.
2. Prosedur kriptografi dilakukan dengan :
    a) menghindari penggunaan kriptografi simetrik dengan *hardcoded key;*
    b) mengimplementasikan metode kriptografi yang sudah teruji sesuai kebutuhan;
    c) menghindari penggunaan protokol kriptografi atau algoritme kriptografi yang obsolet;
    d) menghindari penggunaan kunci kriptografi yang sama; dan
    e) menggunakan pembangkit kunci acak yang memenuhi kriteria keacakan kunci.

3. Prosedur autentikasi dan manajemen sesi dilakukan dengan:
   a) menerapkan autentikasi pada *remote endpoint* terhadap aplikasi yang menyediakan akses pengguna untuk layanan jarak jauh;
   b) menggunakan *session identifier* yang acak tanpa perlu mengirimkan kredensial pengguna apabila menggunakan *stateful* manajemen sesi;
   c) memastikan server menyediakan token yang telah ditandatangani menggunakan algoritme yang aman apabila menggunakan autentikasi *stateless* berbasis token;
   d) memastikan *remote endpoint* memutus sesi yang ada saat pengguna *log out*;
   e) menerapkan pengaturan sandi pada *remote endpoint*;
   f) membatasi jumlah percobaan *log in* pada *remote endpoint*;
   g) menentukan masa berlaku sesi dan masa kedaluwarsa token pada *remote endpoint*; dan
   h) melakukan otorisasi pada *remote endpoint*.
4. Fungsi komunikasi jaringan dilakukan dengan prosedur:
   a) menerapkan *secure socket layer* atau *transport layer security* yang tidak obsolet secara konsisten; dan
   b) memverifikasi sertifikat *remote endpoint*.
   c) Fungsi interaksi platform dilakukan dengan prosedur:
   d) memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan;
   e) melakukan validasi terhadap seluruh input dari sumber eksternal dan pengguna;
   f) menghindari pengiriman fungsionalitas sensitif melalui skema *custom uniform resource locator* dan fasilitas *inter process communication*;
   g) menghindari penggunaan *JavaScript* dalam *WebView*;
   h) menggunakan protokol *hypertext transfer protocol secure* pada *WebView*; dan
   i) mengimplementasikan penggunaan serialisasi API yang aman.
5. Fungsi kualitas kode dan pengaturan *build* dilakukan dengan prosedur:
   a) menandatangani aplikasi dengan sertifikat yang valid;
   b) memastikan aplikasi dalam mode rilis;
   c) menghapus simbol *debugging* dari *native binary*;
   d) menghapus kode *debugging* dan kode bantuan pengembang;
   e) mengidentifikasi kelemahan seluruh komponen *third party*;
   f) yang tidak sah;
   g) mendeteksi dan merespons *debugger*;
   h) mencegah *executable file* melakukan perubahan pada sumber daya perangkat;
   i) mendeteksi dan merespons keberadaan perangkat *reverse engineering*;
   j) mencegah aplikasi berjalan dalam emulator;
   k) mendeteksi perubahan kode dan data diruang memori;
   l) menentukan mekanisme penanganan eror;
   m) mengelola memori secara aman; dan
   n) mengaktifkan fitur keamanan yang tersedia.
6. Fungsi ketahanan dilakukan dengan prosedur:
   a) mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi
   b) menerapkan fungsi *devicebinding* dengan menggunakan *property* unik pada perangkat;
   c) melindungi seluruh *file* dan *library* pada aplikasi; dan

d) menerapkan metode *obfuscation* (metode yang membingungkan, dan tidak membuat sesuatu tidak mudah dimengerti. Ia bukan mengacak tanpa aturan)

IV. Standar teknis keamanan Sistem Penghubung Layanan terdiri atas:
a. keamanan interoperabilitas data dan informasi;
b. kontrol sistem integrasi;
c. kontrol perangkat integrator;
d. keamanan API dan *web service;* dan
e. keamanan migrasi data.

1. Keamanan interoperabilitas data dan informasi dilakukan dengan prosedur:
a) menerapkan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik;
b) menerapkan sistem enkripsi data;
c) memastikan data dan informasi selalu dapat diakses sesuai otoritasnya; dan
d) menerapkan sistem *hash function* pada *file*.
e) Kontrol sistem integrasi dilakukan dengan prosedur:
f) menerapkan protokol *secure socket layer* atau protokol *transport layer security* versi terkini pada sesi pengiriman data dan informasi;
g) menerapkan *internet protocol security* untuk mengamankan transmisi data dalam jaringan berbasis *transmission control protocol/internet protocol*;
h) menerapkan sistem anti *distributed denial of service*;
i) menerapkan autentikasi untuk memverifikasi identitas eksternal antar Layanan SPBE yang terhubung;
j) menerapkan manajemen keamanan sesi;
k) menerapkan pembatasan akses pengguna berdasarkan otorisasi yang telah ditetapkan;
l) menerapkan validasi input;
m) menerapkan kriptografi pada verifikasi statis;
n) menerapkan sertifikat elektronik pada *web authentication*;
o) menerapkan penanganan eror dan pencatatan *log*;
p) menerapkan proteksi data dan jalur komunikasi;
q) menerapkan pendeteksi virus untuk memeriksa beberapa konten *file*;
r) menetapkan perjanjian tingkat layanan dengan standar paling rendah 95% (sembilan puluh lima per seratus); dan
s) memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.

2. Kontrol perangkat integrator dilakukan dengan prosedur:
a. menggunakan sistem operasi dan perangkat lunak dengan *security patches* terkini;
b. menggunakan anti virus dan anti-*spyware* terkini;
c. mengaktifkan fitur keamanan pada peramban web;
d. menerapkan *firewall* dan *host-based intrusion detection systems*;
e. mencegah instalasi perangkat lunak yang belum terverifikasi;
f. mencegah akses terhadap situs yang tidak sah;dan
g. mengaktifkan sistem *recovery* dan *restore* pada perangkat integrator.

3. Keamanan API dan *web service* dilakukan dengan prosedur:
a. menerapkan protokol *secure socket layer* atau protokol *transport layer security* diantara pengirim dan penerima API;
b. menerapkan protokol *open authorization* versi terkini untuk menjembatani interaksi antara *resource owner*, *resource server* dan/atau *third party*;

c. menampilkan metode RESTful *hypertext transfer protocol* apabila input pengguna dinyatakan valid;
d. melindungi layanan web RESTful yang menggunakan *cookie* dari *cross-site request forgery*; dan
e. memvalidasi parameter yang masuk oleh penerima API untuk memastikan data yang diterima valid dan tidak menyebabkan kerusakan.

4. Keamanan migrasi data dilakukan dengan prosedur:
   a) memastikan migrasi data dilakukan secara bertahap dan terprogram oleh sistem;
   b) memastikan aplikasi yang menggunakan sistem basis data lama tetap dipertahankan sampai sistem pendukung basis data baru dapat berjalan atau berfungsi dengan normal;
   c) mendokumentasikan format sistem basis data lama secara rinci;
   d) melakukan pencadangan seluruh data yang tersimpan pada sistem sebelum melakukan migrasi data;
   e) menerapkan teknik kriptografi pada proses penyimpanan dan pengambilan data; dan
   f) melakukan validasi data ketika proses migrasi data selesai.

V. Standar teknis keamanan Jaringan Intra diterapkan pada jaringan Intra Pemerintah Daerah Kabupaten Rokan Hulu, terdiri atas:
a. aspek administrasi keamanan Jaringan Intra;
b. kontrol akses dan autentikasi;
c. persyaratan perangkat dan aplikasi keamanan Jaringan Intra;
d. kontrol keamanan *gateway*;
e. kontrol keamanan *accesspoint*pada jaringan nirkabel; dan
f. kontrol konfigurasi *access point* pada jaringan nirkabel.

1. Aspek administrasi keamanan Jaringan Intra dilakukan dengan prosedur:
   a) menyusun dan mengevaluasi dokumen arsitektur Jaringan Intra;
   b) mengidentifikasi seluruh aset infrastruktur jaringan;
   c) menyusun dan menetapkan standar operasional prosedur terkait pemeliharaan keamanan Jaringan Intra; dan
   d) membuat laporan pengawasan keamanan jaringan secara periodik.
2. Kontrol akses dan autentikasi dilakukan dengan prosedur:
   a) menempatkan perangkat infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah;
   b) menggunakan autentikasi untuk mengakses Jaringan Intra;
   c) menerapkan pembatasan akses dalam Jaringan Intra;
   d) mematikan atau membatasi *protocol, port,* dan layanan yang tidak digunakan;
   e) menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya;
   f) menerapkan fungsi *honeypot* untuk menganalisis celah keamanan berdasarkan jenis serangan;
   g) menerapkan *virtual private network* dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan;
   h) memberikan kewenangan hanya kepada administrator untuk menginstal perangkat lunak dan/atau mengubah konfigurasi sistem dalam Jaringan Intra;
   i) menerapkan *secure endpoints*;
   j) memblokir layanan yang tidak dikenal;
   k) menerapkan *secure socket layer* atau *transport layer security* versi terkini pada jalur akses Jaringan Intra; dan

l) menerapkan *server* perantara saat *client* mengakses *server database* dalam rangka pemeliharaan.

3. Persyaratan perangkat dan *aplikasi* keamanan Jaringan Intra dilakukan dengan prosedur:
   a) menggunakan perangkat security information and event management untuk network logging dan monitoring;
   b) menerapkan sistem deteksi dini kerentanan keamanan perangkat jaringan;
   c) menggunakan perangkat firewall;
   d) menggunakan perangkat intrusion detection systems dan intrusion prevention systems;
   e) menerapkan virtual private network terenkripsi untuk penggunaan akses jarak jauh secara terbatas;
   f) menerapkan kontrol update patching pada infrastruktur Jaringan Intra dan sistem komputer;
   g) menggunakan perangkat web application firewall;
   h) menggunakan perangkat load balancer untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi;
   i) memperbarui teknologi keamanan perangkat keras dan perangkat lunak untuk meminimalisasi celah peretas;
   j) mengunduh perangkat lunak melalui enterprise software distribution system; dan
   k) menerapkan sertifikat elektronik.
4. Kontrol keamanan *gateway* dilakukan dengan prosedur:
   a) menerapkan content filtering;
   b) menerapkan inspection packet filtering untuk memeriksa packet yang masuk pada Jaringan Intra;
   c) menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat gateway;
   d) memastikan perangkat gateway yang menghubungkan antar Jaringan Intra tidak terkoneksi langsung dengan jaringan publik;
   e) melaksanakan manajemen traffic gateway; dan
   f) memastikan port tidak dibuka secara default.
5. Kontrol keamanan *access point* pada jaringan nirkabel dilakukan dengan prosedur:
   a) menerapkan protokol keamanan *access point* nirkabel dan teknologi enkripsi terkini;
   b) menerapkan *mediaaccess control* pada *address filtering*;
   c) menerapkan *dedicated service set identifier;*
   d) menerapkan pembatasan jangkauan radio transmisi dan pengguna jaringan;
   e) menerapkan pembatasan terkait penambahan perangkat nirkabel yang dipasang secara tidak sah;
   f) menerapkan manajemen *vulnerability* secara berkala dan berkelanjutan; dan
   g) melakukan *patching firmware* secara rutin.
6. Kontrol konfigurasi *access point* pada jaringan nirkabel dilakukan dengan prosedur:
   a) menggunakan kata sandi yang kuat;
   b) menggunakan protokol model *authentication authorization* dan *accounting* pada perangkat infrastruktur jaringan untuk *management user* atau otentikasi *administrator access point*;
   c) memastikan fitur akses konfigurasi jarak jauh hanya dapat digunakan dalam kondisi darurat dengan menerapkan kontrol keamanan*;*

d) mengisolasi atau melakukan segmentasi jaringan area lokal nirkabel; dan
e) menonaktifkan antarmuka nirkabel, layanan, dan aplikasi yang tidak digunakan.

VI. Standar teknis keamanan Pusat Data Daerah terdiri atas:
a. persyaratan keamanan fisik dan manajemen Pusat Data Daerah; dan
b. persyaratan koneksi perangkat ke Pusat Data Daerah.

1. Persyaratan keamanan fisik dan manajemen Pusat Data Daerah dilakukan dengan prosedur sesuai dengan Standar Nasional Indonesia yang terkait dengan Pusat Data.
2. Persyaratan koneksi perangkat ke Pusat Data Daerah dilakukan dengan prosedur:
   a) memastikan keamanan perangkat yang terkoneksi ke infrastruktur Pusat Data Daerah;
   b) memutus akses fisik atau *logic* dari perangkat yang tidak terotorisasi;
   c) memastikan akses tingkat administrator ke server dan perangkat jaringan utama tidak boleh dilakukan secara *remote*;
   d) memastikan hanya personil yang berwenang yang boleh menggunakan komputer di area Pusat Data Daerah;
   e) melakukan *backup* informasi dan perangkat lunak yang berada di Pusat Data Daerah secara berkala;
   f) memastikan perangkat komputer Pusat Data Daerah terbebas dari virus dan *malware*;
   g) melakukan pembatasan akses pemanfaatan *removable media* di area Pusat Data Daerah;
   h) memastikan pengaktifan konfigurasi *port universal serial bus* telah mendapatkan izin dari personil yang berwenang;
   i) memastikan setiap perangkat yang akan terkoneksi ke infrastruktur Pusat Data Daerah menggunakan *internet protocol address* dan *hostname* yang telah ditentukan; dan
   j) menerapkan *server* perantara saat *client* mengakses *server database* dalam rangka pemeliharaan.

BUPATI ROKAN HULU,

ttd

S U K I M A N

Salinan sesuai aslinya,
KEPALA BAGIAN HUKUM,

H. ERINALDI, SH, MH
Pembina IV.a
NIP. 19840916 201001 1 008

LAMPIRAN II
PERATURAN BUPATI ROKAN HULU
NOMOR 34 TAHUN 2024
TENTANG
PERUBAHAN ATAS PERATURAN BUPATI ROKAN HULU NOMOR 17 TAHUN 2022 TENTANG PENYELENGGARAAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PEMERINTAH KABUPATEN ROKAN HULU

PROSES KEAMANAN INFORMASI

Manajemen keamanan informasi dilakukan melalui serangkaian proses yang meliputi penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja dan perbaikan berkelanjutan terhadap keamanan informasi dalam SPBE;

I. Perencanaan terhadap keamanan informasi dalam SPBE
   a. Perencanaan terhadap keamanan informasi dalam SPBE dilakukan oleh pelaksana teknis Keamanan SPBE.
   b. Perencanaan terhadap keamanan informasi dalam SPBE dilakukan dengan merumuskan:
      1. program kerja Keamanan SPBE yang disusun berdasarkan kategori risiko Keamanan SPBE , paling sedikit meliputi :
         a) edukasi kesadaran Keamanan SPBE, yang dilaksanakan paling sedikit melalui kegiatan:
            1) sosialisasi; dan
            2) pelatihan.
         b) penilaian kerentanan Keamanan SPBE, dilaksanakan paling sedikit melalui:
            1) menginventarisasi seluruh aset SPBE meliputi data dan informasi, aplikasi, dan infrastruktur;
            2) mengidentifikasi kerentanan dan ancaman terhadap aset SPBE; dan
            3) mengukur tingkat risiko keamanan SPBE.
         c) peningkatan Keamanan SPBE , dilaksanakan berdasarkan hasil dari penilaian kerentanan keamanan SPBE , paling sedikit melalui:
            1) menerapkan standar teknis dan prosedur Keamanan SPBE; dan
            2) menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE.
         d) penanganan insiden Keamanan SPBE, dilaksanakan paling sedikit melalui:
            1) mengidentifikasi sumber serangan;
            2) menganalisis informasi yang berkaitan dengan insiden selanjutnya;
            3) memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
            4) mendokumentasi bukti insiden yang terjadi; dan
            5) memitigasi atau mengurangi dampak risiko Keamanan SPBE.
         e) audit Keamanan SPBE.
      2. target realisasi program kerja Keamanan SPBE yang ditetapkan berdasarkan kebutuhan Pemerintah Daerah.

II. Dukungan terhadap keamanan informasi dalam SPBE
   a. Dukungan pengoperasian terhadap keamanan informasi dalam SPBE dilakukan oleh koordinator SPBE.
   b. Dukungan pengoperasian terhadap keamanan informasi dalam SPBE dilakukan dengan meningkatkan kapasitas terhadap:
      1. sumber daya manusia Keamanan SPBE, paling sedikit harus memiliki kompetensi:
         a) keamanan infrastruktur teknologi, informasi dan komunikasi; dan
         b) keamanan aplikasi.
      2. Untuk memenuhi kompetensi sumber daya manusia Keamanan SPBE, Pemerintah Daerah paling sedikit melakukan kegiatan:
         a) pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi, informasi dan komunikasi dan keamanan aplikasi; dan
         b) bimbingan teknis mengenai standar Keamanan SPBE.
      3. anggaran Keamanan SPBE, disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

III. Evaluasi kinerja terhadap keamanan informasi dalam SPBE
   1. Evaluasi kinerja keamanan informasi dalam SPBE dilakukan oleh koordinator SPBE.
   2. Evaluasi kinerja keamanan informasi dalam SPBE dilakukan terhadap pelaksanaan Keamanan SPBE.
   3. Evaluasi kinerja keamanan informasi dalam SPBE dilaksanakan dengan:
      a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan SPBE;
      b. menetapkan indikator kinerja pada setiap area proses;
      c. memformulasi pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
      d. menganalisis efektifitas pelaksanaan Keamanan SPBE; dan
      e. mendukung dan merealisasikan program audit Keamanan SPBE.
   4. Evaluasi kinerja keamanan informasi dalam SPBE dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

IV. Perbaikan berkelanjutan terhadap keamanan informasi dalam SPBE
   a. Perbaikan berkelanjutan dilakukan oleh pelaksana teknis Keamanan SPBE.
   b. Perbaikan berkelanjutan merupakan tindak lanjut dari hasil evaluasi kinerja.
   c. Perbaikan berkelanjutan dilakukan dengan:
   d. mengatasi permasalahan dalam pelaksanaan Keamanan SPBE; dan
   e. memperbaiki pelaksanaan Keamanan SPBE secara periodik.

BUPATI ROKAN HULU,

ttd

S U K I M A N

Salinan sesuai aslinya,
KEPALA BAGIAN HUKUM,

H. ERINALDI, SH, MH
Pembina IV.a
NIP. 19840916 201001 1 008