BUPATI SELUMA

PERATURAN BUPATI SELUMA

NOMOR .33.. TAHUN 2019

TENTANG

MANAJEMEN PENGAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN SELUMA

DENGAN RAHMAT TUHAN YANG MANA ESA

BUPATI SELUMA,

Menimbang : a. bahwa dalam rangka keamanan data dan informasi di Lingkungan Pemerintah Kabupaten Seluma, perlu menyusun sebuah system manajemen pengamanan informasi, agar kerahasiaan, integritas,dan ketersediaan informasi tetap terjaga;

b. bahwa untuk memberikan arah, landasan dan kepastian hukum kepada semua pihak yang terlibat dalam penyelenggaraan Sistem Pemerintahan Yang Berbasis Elektronik (SPBE) maka di perlukan sistem manajemen pengamanan informasi di Lingkungan Pemerintah Kabupaten Seluma;

c. bahwa berdasarkan pertimbangan sebagaimanadimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Bupati Seluma tentang Manajemen Pengamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) Kabupaten Seluma;

Mengingat : 1. Undang-Undang Nomor 3 Tahun 2003 tentang Pembentukan Kabupaten Mukomuko, Kabupaten Seluma dan Kabupaten Kaur di Propinsi Bengkulu (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 23, Tambahan Lembaran Negara Republik Indonesia Nomor 4266);

2. 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);

3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik dan TransaksiElektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);

4. 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);

5. Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 114, Tambahan Lembaran Negara Republik Indonesia Nomor 5887);

6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

7. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita

Negara Republik Indonesia Tahun 2016 nomor 551);

8. Peraturan Menteri Pendayagunaan Aparatur Negara dan Repormasi Birokrasi Nomor 5 Tahun 2018 tentang Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia tahun 2018 Nomor 154);
9. Peraturan Bupati Seluma Nomor 31 Tahun 2016 tentang Kedudukan, Susunan Organisasi dan Tata Kerja Dinas Daerah Kabupaten Seluma sebagaimana telah diubah beberapa kali terakhir dengan Peraturan Bupati Seluma Nomor 256 Tahun 2017 tentang Perubahan Kedua Atas Peraturan Bupati Seluma Nomor 31 Tahun 2016 tentang Kedudukan, Susunan Organisasi dan Tata Kerja Dinas Daerah Kabupaten Seluma (Berita Daerah Kabupaten Seluma Tahun 2017 Nomor 265);

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI SELUMA TENTANG MANAJEMEN PENGAMANAN INFORMASI SISTEM PEMERINTAHAN YANG BERBASIS ELEKTRONIK (SPBE).

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan :

1. Daerah adalah Kabupaten Seluma.
2. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintah daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Kepala Daerah adalah Bupati Seluma.

4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Seluma;
5. Organisasi Perangkat Daerah yang selenjutnya disebut OPD adalah OPD dilingkungan pemerintah daerah.
6. Organisasi perangkat daerah Dinas Komunikasi Dan Informatika yang selanjutnya disebut OPD Diskominfo adalah unsur pembantu kepala daerah dalam penyelenggaraan urusan komunikasi dan informatika.
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. Pelayanan Publik adalah kegiatan atau rangkaian kegiatan dalam rangka pemenuhan kebutuhan pelayanan sesuai dengan peraturan perundang-undangan bagi setiap warga negara dan penduduk atas barang,jasa, dan/atau pelayanan administratif yang disediakan oleh penyelenggara pelayanan publik.
9. Manajemen Pengamanan Informasi SPBE adalah pengaturan kewajiban bagi Pengguna SPBE dalam penerapan manajemen SPBE berdasarkan asas Risiko.
10. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi.
11. Pengguna adalah pegawai Pemerintah Kabupaten Seluma dan atau pihak ketiga serta tidak terbatas pada pengelola SPBE dan kelompok kerja yang diberikan hak mengakses system SPBE di lingkungan Pemerintah Kabupaten Seluma.
12. Pengguna SPBE adalah instansi pusat, pemerintah daerah, pegawai Aparatur Sipil Negara, perorangan, masyarakat, pelaku usaha, dan pihak lain yang memanfaatkan Layanan SPBE.
13. Risiko adalah kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negative terhadap pencapaian sasaran kinerja dari layanan Sistem Elektronik.
14. Manajemen risiko adalah serangkaian proses identifikasi, analisis, pengendalian, pemantauan, dan evaluasi terhadap risiko.

15. Infrastruktur adalah sarana dan prasarana TIK berupa perangkat keras, kabel jaringan, ruang data center, server, storage, switch, router, leptop, dekstop, perangkat copy dan cetak, pheriperal dan sejenisnya.
16. Aset informasi Pemerintah Kabupaten Seluma adalah aset dalam bentuk:
    a. Data/dokumen, meliputi: data peraturan daerah dan perundang-undangan, data kependudukan, data kesehatan, data pertanian, data pendidikan, data daerah rawan bencana, data luas wilayah, data pembangunan kabupaten, data hak kekayaan intelektual, data gaji, data kepegawaian, data penawaran dan kontrak, dokumen perjanjian kerahasiaan, kebijakan pemerintah daerah, hasil penelitian, bahan pelatihan, prosedur operasional, rencana kelangsungan kegiatan, dan hasil audit.
    b. Perangkat lunak, meliputi: perangkat lunak aplikasi, perangkat lunak sistem, dan perangkat bantu pengembangan system.
    c. Aset fisik, meliputi: perangkat komputer, perangkat jaringan dan komunikasi, *removable media*, dan perangkat pendukung;dan
    d. Aset tak berwujud, meliputi: pengetahuan, pengalaman, keahlian, citra, dan reputasi.
17. Aset tak berwujud adalah jenis asset yang tidak memiliki wujud fisik, misalnya pengetahuan, pengalaman, keahlian, citra, dan reputasi. Aset ini mempunyai umur lebih dari satu tahun (aset tidak lancar) dan dapat diamortisasi selama periode pemanfaatannya, yang biasanya tidak lebih dari 40 (empat puluh) tahun.
18. *Backup* adalah sebuah proses pembuatan gandaan/duplikat/ cadangan dari aset informasi yang dilakukan sebagai upaya pengamanan dan pemulihan sebagai bagian dari manajemen risiko.
19. Daftar inventaris aset informasi adalah kumpulan informasi yang memuat bentuk, pemilik, lokasi, retensi, dan hal-hal yang terkait dengan asset informasi.

20. Dokumen manajemen pengamanan informasi SPBE Pemerintah Kabupaten Seluma adalah dokumen terkait pelaksanaan manajemen pengamanan informasi SPBE yang meliputi antara lain dokumen standar, prosedur, dan catatan penerapan manajemen pengamanan informasi SPBE.
21. Pemilik aset informasi adalah unit kerja yang memiliki kewenangan terhadap asset informasi.
22. Perangkat jaringan adalah peralatan jaringan komunikasi data seperti: *modem, hub, switch, router,* dan lain-lain.
23. Perangkat lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya.
24. Perangkat pendukung adalah peralatan pendukung untuk menjamin beroperasinya perangkat keras dan perangkat jaringan serta untuk melindunginya dari kerusakan. Contoh perangkat pendukung adalah *Uninterruptible Power Supply* (UPS), pembangkit tenaga listrik/ generator, antena komunikasi.
25. Perangkat pengolah informasi adalah setiap system pengolah informasi, layanan atau infrastruktur seperti komputer,server, faksimili, telepon, mesin*fotocopy.*
26. Auditor Manajemen Pengamanan Informasi SPBE yang selanjutnya disebut Auditor adalah orangyang melakukan audit berdasarkan Peraturan Bupati ini;

BAB II
MAKSUD DAN TUJUAN

Pasal 2

(1) Adapun maksud peraturan Bupati ini adalah untuk mengatur mengenai penerapan Manajemen Pengamanan Informasi SPBE oleh Pengguna SPBE untuk Pelayanan Publik berdasarkan asas Risiko;
(2) Adapun tujuan Peraturan Bupati ini adalah untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko dalam SPBE.

Pasal 3

Penerapan Manajemen Pengamanan Informasi SPBE oleh Penguna SPBE untuk Pelayanan Publik sebagaimana dimaksud dalam Pasal 2 ayat (1) meliputi:

a. organisasi perangkat daerah yang terdiri dari Dinas, Badan, Kantor, Kecamatan, Kelurahan dan puskesmas;
b. badan hukum lain yang menyelenggarakan Pelayanan Publik dalam rangka pelaksanaan tugas daerah.

Pasal4

(1) Kategorisasi Sistem Elektronik berdasarkan asas Risiko sebagaimana dimaksud dalam Pasal 2 ayat (1) terdiri atas:
    a. Sistem Elektronik strategis;
    b. Sistem Elektronik tinggi;
    c. Sistem Elektronik rendah.
(2) Sistem Elektronik strategis sebagaimana dimaksud pada ayat (1) huruf a merupakan Sistem Elektronik yang berdampak serius terhadap kepentingan umum, Pelayanan Publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan Negara;
(3) Sistem Elektronik tinggi sebagaimana dimaksud pada ayat (1) huruf b merupakan Sistem Elektronikyang berdampak terbatas pada kepentingan sector dan/atau daerah tertentu.
(4) Sistem Elektronik rendah sebagaimana dimaksud pada ayat (1) huruf c merupakan Sistem Elektronik lainnya yang tidak termasuk pada ayat (2) dan ayat (3).

BAB III

TANGGUNGJAWAB

Bagian Satu

Umum

Pasal 5

(1) Manajemen Pengamanan Informasi SPBE di Lingkungan Pemerintah Kabupaten Seluma dikoordinasikan oleh pejabat

yang berperan sebagai *ChiefInformation Officer* (CIO) Pemerintah Kabupaten seluma, yang sekaligus berperan sebagai *Chief Information Security Officer* (CISO) Pemerintah Kabupaten Seluma, dalam hal ini adalah Dinas Komunikasi dan Informatika atau OPD Diskominfo ;

(2) OPD Diskominfo dapat membentuk Satuan Tugas Keamanan Informasi SPBE;

(3) OPD Diskominfo wajib menerapkan prinsip manajemen risiko dalam rangka pelaksanaan pengamanan dan perlindungan infrastruktur SPBE dan aset informasi dengan mengikuti ketentuan mengenai Penerapan Manajemen Risiko di Lingkungan Pemerintah Kabupaten Seluma;

(4) OPD Diskominfo melakukan evaluasi terhadap pelaksanaan Manajemen pengamanan Informasi SPBE secara berkala untuk menjamin efektivitas dan meningkatkan keamanan informasi di Lingkungan Pemerintah Kabupaten Seluma;

Bagian Kedua

Pengendalian Keamanan Informasi

Pasal 6

Pengendalian Keamanan Informasi dalam Manajemen Pengamanan Informasi SPBE terdiri dari :

(1) Pengendalian Organisasi;

(2) Pengendalian Pengelolaan Aset Informasi;

(3) Pengendalian keamanan informasi dari sisi sumber daya manusia;

(4) Pengendalian Keamanan Fisik dan Lingkungan;

(5) Pengendalian Pengelolaan Operasional;

(6) Pengendalian akses;

(7) Pengendalian keamanan informasi dalam pengadaan, pengembangan, dan pemeliharaan system informasi; dan

(8) Pengendalian pengelolaan gangguan kemanan informasi;

Pasal 7

Pengendalian Organisasi dalam Manajemen Pengamanan Informasi SPBE sebagaimana dimaksud dalam pasal 6 ayat (1) dapat di jelaskan sebagai berikut :

(1) OPD Diskominfo berkewajiban untuk mengkaji perjanjian kerahasiaan pihak-pihak internal dan eksternal secara berkala untuk menjaga asset informasi;
(2) OPD Diskominfo memfasilitasi perjanjian kerja sama dengan pihak-pihak berwenang diluar Pemerintah Kabupaten Seluma yang terkait dengan keamanan informasi;
(3) OPD Diskominfo memfasilitasi kerja sama dengan komunitas keamanan informasi diluar Pemerintah Kabupaten Seluma melalui pelatihan, seminar, atau forum lain yang relevan dengan keamanan informasi; dan
(4) OPD Diskominfo berkewajiban menerapkan pengendalian keamanan informasi berdasarkan hasil penilaian risiko untuk mencegah atau mengurangi dampak risiko terkait dengan pemberian akses kepada pihak ketiga.

Pasal 8

Pengendalian Manajemen Pengamanan Informasi SPBE sebagaimana dimaksud pasal 6 ayat (2) mengenai Pengendalian Pengelolaan Aset Informasi dapat di jelasakan bahwa:

(1) OPD Diskominfo bertanggung jawab terhadap keamanan asset informasi, meliputi :
    a. Mengidentifikasi aset informasi dan mendokumentasikannya dalam daftar inventaris asetinformasi;
    b. Menetapkan pemilik aset informasi di setiap OPD;
    c. Menetapkan aset informasi yang terkait dengan perangkat pengolah informasi;dan
    d. Aturan penggunaan aset informasi.
(2) Aset informasi diklasifikasikan sesuai tingkat kerahasiaan, nilai, tingkat kritikalitas, serta aspekhukumnya;
(3) Apabila ketentuan sebagaimana dimaksud Pasal 8 ayat (1) huruf a tidak dapat di penuhi dan merupakan aset yang tidak dapat di pindah alihkan di karenakan hal-hal yang terkait dalam aset

tersebut maka OPD pemegang Aset dapat menyampaikan kepada OPD Diskominfo sebagai pihak yang bertanggungjawab atas keamanan aset informasi tersebut;

Pasal 9

Pengendalian keamanan informasi dari sisi sumber daya manusia dalam pelaksanaan Manajemen Pengamanan Informasi SPBE sebagaimana dimaksud Pasal 6 ayat (3) yaitu:

(1) Seluruh pegawai bertanggung jawab untuk menjaga keamanan informasi Pemerintah Kabupaten Seluma;
(2) Pihak ketiga wajib menyetujui dan menandatangani syarat dan perjanjian untuk menjaga keamanan informasi Pemerintah Kabupaten Seluma;
(3) Peran dan tanggung jawab pegawai dan pihak ketigaterhadap keamanan informasi harus didefinisikan, didokumentasikan, dan dikomunikasikan kepada yang bersangkutan;
(4) OPD melakukan pemeriksaan data pribadi yang diberikan oleh pegawai baru dan pihak ketiga sesuai dengan ketentuan yang berlaku;
(5) Seluruh pegawai wajib mendapatkan pendidikan/pelatihan/sosialisasi keamanan sistem informasi secara berkala sesuai tingkat tanggungjawabnya;
(6) Pihak ketiga diberikan sosialisasi untuk meningkatkan kepedulian terhadap keamanan informasi (jika di perlukan);
(7) Seluruh pegawai dan pihak ketiga yang melanggar manajemen pengamanan informasi SPBE di lingkungan Pemerintah Kabupaten Seluma akan diberikan sanksi atau tindakan disiplin sesuai dengan ketentuan yangberlaku;
(8) Kepatuhan pegawai terhadap manajemen pengamanan informasi SPBE di lingkungan Pemerintah Kabupaten Seluma wajib diawasi oleh atasan masing-masing;
(9) Pegawai yang berhenti bekerja atau mutasi wajib mengembalikan seluruh aset informasi yang dipergunakan selama bekerja sesuai dengan ketentuan yang berlaku;
(10) Pihak ketiga yang habis masa kontrak kerjanya wajib mengembalikan seluruh aset informasi yang dipergunakan

selama bekerja di Pemerintah Kabupaten Seluma;

(11) OPD wajib menghentikan hak penggunaan asset informasi bagi pegawai yang sedang dalam pemeriksaan dan/atau menjalani proses hukum terkait dengan dugaan pelanggaran manajemen pengamanan informasi SPBE di lingkungan Pemerintah Kabupaten Seluma;dan

(12) OPD wajib mencabut hak akses terhadap akses informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi bekerja di Pemerintah Kabupaten Seluma.

Pasal 10

Pengendalian Keamanan Fisik dan Lingkungan dalam manajemen pengamanan informasi SPBE sebagimana dimaksud pasal 6 ayat (4) yaitu :

(1) Pengamanan area

a. Seluruh pegawai, pihak ketiga, dan tamu yangmemasuki lingkungan area Pusat Data/Ruang Server wajib mematuhi aturan yang berlaku di Lingkungan Pemerintah Kabupaten Seluma;

b. Ketentuan rinci tentang pengamanan area lingkungan kerja di Lingkungan Pemerintah Kabupaten Seluma diatur dalam standar Oprasional Prosedur (SOP) tentang keamanan fisik dan lingkungan.

(2) Pengamanan perangkat atau infrastruktur SPBE

a. Perangkat atau infrastruktur pengolah informasi seperti server dan perangkat pendukung lainnya wajib ditempatkan di OPD Diskominfo dan di posisikan sedemikian rupa untuk mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang;

b. Perangkat pendukung wajib dipasang untuk menjamin beroperasinya perangkat pengolah informasi dan secara berkala wajib diperiksa dan diuji ulang kinerjanya;

c. Perangkat pengolah informasi wajib dipelihara secara berkala untuk menjamin ketersediaan, keutuhan, dan fungsinya;

d. Penggunaan perangkat yang dibawa ke luar dari lingkungan

Pemerintah Kabupaten Seluma wajib disetujui oleh Pejabat yang berwenang;

e. Perangkat pengolah informasi penyimpan data yang sudahtidak digunakan lagi wajib disanitasi sebelum digunakan kembali atau dihapuskan/dimusnahkan;

f. Penanganan perangkat pengolah informasi penyimpan data di Lingkungan Pemerintah Kabupaten Seluma sesuai dengan standar penanganan media penyimpan data yang ditetapkan dalam Standar Pengelolaan Data Elektronik di Lingkungan Pemerintah Kabupaten Seluma.

g. Apabila ketentuan sebagaimana dimaksud pada ayat (2) huruf a tidak dapat di penuhi dan merupakan Perangkat atau infrastruktur pengolah informasi yang tidak dapat di pindah alihkan dikarenakan telah diatur dalam peraturan atau ketentuan atas perangkat atau infrastruktur pengolah informasi maka OPD pemegang Perangkat atau infrastruktur pengolah informasi dapat menyampaikan kepada OPD Diskominfo sebagai pihak yang bertanggungjawab atas perangkat atau infrastruktur pengolah informasi tersebut;

Pasal 11

Pengendalian PengelolaanOperasional sebagaimana dimaksud Pasal 6 ayat (5) dalam pelaksanaan manajemen pengamanan informasi SPBE yaitu dapat dilakukan dengan :

(1) Prosedur operasional dan tanggungjawab

a. OPD Diskominfo berkewajiban mendokumentasikan, memelihara, dan menyediakan seluruh prosedur operasional yang terkait dengan penggunaan perangkat pengolah informasi sesuai dengan peruntukannya.

b. Mengendalikan perubahan terhadap perangkat pengolah informasi.

c. Melakukan pemisahan informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA untuk menghindari adanya pegawai yang memiliki pengendalian eksklusif terhadap seluruh aset informasi dan perangkat pengolahnya.

d. Melakukan pemisahan perangkat pengembangan, pengujian,

dan operasional untuk mengurangi risiko perubahan atau akses oleh pihak yang tidak berwenang terhadap system operasional.

(2) Pengelolaan layanan oleh pihakketiga

a. Wajib memastikan bahwa pengendalian keamanan informasi, definisi layanan, dan tingkat layanan yang tercantum dalam kesepakatan penyediaan layanan telah diterapkan, dioperasikan dan dipelihara oleh pihak ketiga.

b. Wajib melakukan pemantauan terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh pihak ketiga secara berkala.

c. Wajib memperhatikan kritikalitas, proses yang terkait dan hasil penilaian ulang risiko layanan apabila terjadi perubahan pada layanan yang disediakan pihak ketiga.

(3) Perencanaan dan penerimaan sistem

a. OPD Diskominfo wajib memantau penggunaan perangkat pengolah informasi dan membuat perkiraan pertumbuhan kebutuhan kedepan untuk memastikan ketersediaan kapasitas;

b. OPD Diskominfo wajib menetapkan kriteria penerimaan untuk sistem informasibaru, pemutakhiran dan versi baru serta melakukan pengujian sebelum penerimaan.

(4) OPD Diskominfo Wajib menerapkan sistem yang dapat melakukan pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan;

(5) *Backup*

a. Setiap OPD Wajib melakukan *backup* informasi dan perangkat lunakyang berada di Pusat Data secara berkala.

b. Proses *backup* di Pemerintah Kabupaten Seluma sesuai dengan *backup* data yang ditetapkan dalam Standar Pengelolaan Data Elektronik di Lingkungan Pemerintah Kabupaten Seluma.

Pasal 12

Dalam Penerapan manajemen pengamanan informasi SPBE perlu adanya Pengendalian akses keamanan Informasi sebagaimana dimaksud dalam Pasal 6 ayat (6) yaitu terdiri dari :

(1) Pengelolaan akses pengguna; dan
(2) Tanggung jawab pengguna;
(3) Pengendalian akses jaringan;
(4) Pengendalian akses ke system operasi;
(5) Pengendalian akses ke aplikasi dan system informasi;
(6) *Mobile computing* dan *teleworking*.

Pasal 13

Pengelolaan akses pengguna sebagaimana dimaksud pada Pasal 12 ayat (1) dengan beberapa cara yaitu :

(1) OPD Diskominfo wajib menyusun prosedur pengelolaan hak akses pengguna sesuai dengan peruntukannya.
(2) OPD Diskominfo wajib membatasi dan mengendalikan penggunaan hak akses khusus.
(3) OPD Diskominfo wajib mengatur pengelolaan kata sandi pengguna;
(4) OPD Diskominfo wajib memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya.

Pasal 14

Tanggung jawab pengguna sebagaimana dimaksud dalam Pasal 12 ayat (2) menyebutkan bahwa:

(1) Setiap OPD pengguna SPBE wajib mematuhi aturan pembuatan dan penggunaan kata sandi;
(2) Memastikan perangkat pengolah informasi yang digunakan mendapatkan perlindungan terutama saat ditinggalkan;dan
(3) Melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang.

Pasal 15

Pengendalian akses jaringan sebagaimana dimaksud dalam Pasal 12

ayat (3) menyebutkan bahwa :

(1) OPD Diskominfo Wajib mengatur akses pengguna dalam mengakses jaringan Pemerintah Kabupaten Seluma sesuai dengan peruntukannya;

(2) OPD Diskominfo Wajib menerapkan proses otorisasi pengguna untuk setiap akses ke dalam jaringan internal melalui koneksi eksternal;

(3) Akses ke perangkat keras dan perangkat lunak untuk diagnose harus dikontrol berdasarkan prosedur dan hanya digunakan oleh pegawai yang diberikan wewenang untuk melakukan pengujian, pemecahan masalah, serta pengembangan system, dan *port* pada fasilitas jaringan yang tidak dibutuhkan dalam kegiatan atau fungsi layanan wajib di nonaktifkan.

(4) OPD Diskominfo Wajib memisahkan jaringan untuk pengguna, system informasi, dan layanan informasi.

(5) OPD Diskominfo Wajib menerapkan mekanisme pengendalian akses pengguna sesuai dengan persyaratan pengendalian akses.

(6) Pengendalian *routing* jaringan internal Pemerintah Kabupaten Seluma wajib dilakukan sesuai pengendalian akses dan kebutuhan layanan informasi.

Pasal 16

Pengendalian akses ke system operasi sebagaimana dimaksud dalam Pasal 12 ayat (4) menyebutkan :

(1) Akses ke sistem operasi wajib dikontrol dengan menggunakan prosedur akses yangaman.

(2) Setiap pengguna wajib memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya, dan proses otorisasi pengguna wajib menggunakan teknik autentikasi yang sesuai untuk memvalidasi identitas dari pengguna.

(3) Sistem pengelolaan kata sandi wajib mudah untuk digunakan dan dapat memastikan kualitas sandi yang dibuat pengguna.

(4) Wajib membatasi dan mengendalikan penggunaan *system utilities;*

(5) Fasilitas*sessiontime-out* wajib diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan

apabila tidak ada aktivitas pengguna setelah periode tertentu.

(6) Wajib membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA.

Pasal 17

Pengendalian akses ke aplikasi dan system informasi sebagaimana dimaksud dalam Pasal 12 ayat (5) menyebutkan bahwa :

(1) OPD Diskominfo wajib memastikan bahwa akses terhadap aplikasi dan sistem informasi hanya diberikan kepada pengguna sesuai peruntukannya;

(2) Aplikasi dan sistem informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA wajib diletakkan pada lokasi terpisah untuk mengurangi kemungkinan diakses oleh pihak yang tidak berwenang.

Pasal 18

Mobile computing dan*teleworking* sebagaimana dimaksud dalam Pasal 12 ayat (6) dalam pengendalian akses yaitu:

(1) Membangun kepedulian pengguna perangkat *mobilecomputing*dan *Teleworking* akan risiko-risiko keamanan yangterus meningkat terhadap informasi yang tersimpan dalamperangkat*mobilecomputing*;

(2) Pengguna perangkat *mobile computing* dan *teleworking*wajib mengikuti prosedur yang terkait penggunaan perangkat *mobile computing* dan *teleworking* untuk menjaga keamanan perangkat dan informasi di dalamnya.

Pasal 19

Pengendalian keamanan informasi dalam pengadaan, pengembangan, dan pemeliharaan system informasi sebagaimana di maksud dalam Pasal 6 ayat)7) yaitu :

(1) Menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi yang relevan sebelum pengadaan, pengembangan, atau pemeliharaan sistem informasi baru;

(2) Pengelolaan informasi pada aplikasi;

(3) Keamanan file system;

(4) Keamanan dalam proses pengembangan dan pendukung;
(5) Pengelolaan kerentanan teknis;

Pasal 20

Pengelolaan informasi pada aplikasi dalam pengendalian keamanan informasi sebagaimana dimaksud pada Pasal 19 ayat (2) dapat dijelaskan bahwa :

(1) Data yang akan dimasukkan ke aplikasi wajib diperiksa terlebih dahulu kebenaran dan kesesuaiannya.
(2) Setiap aplikasi wajib disertakan proses validasi untuk mendeteksi bahwa informasi yang dihasilkan utuh dan sesuai dengan yang diharapkan.
(3) Data keluaran aplikasi wajib divalidasi untuk memastikan data yang dihasilkan adalah benar.

Pasal 21

Keamanan file sistem sebagimana dimaksud dalam Pasal 19 ayat (3) dapat di jelaskan sebagai berikut :

(1) Wajib mempunyai prosedur untuk pengendalian perangkat lunak pada system operasional.
(2) Menentukan sistem pengujian data, melindunginya dari kemungkinan kerusakan, kehilangan atau perubahan oleh pihak yang tidak berwenang.
(3) Mengendalikan ke kode program secara ketat dan salinan versi terkini dari perangkat lunak disimpan di tempat yang aman.

Pasal 22

Keamanan dalam proses pengembangan dan pendukung sebagaimana dimaksud dalam Pasal 19 ayat (4) menyebutkan bahwa:

(1) Wajib mengendalikan perubahan pada sistem operasi dengan penggunaan prosedur pengendalian perubahan.
(2) Wajib mengendalikan perubahan terhadap perangkat lunak yang dikembangkan sendiri maupun pihak ketiga.
(3) Wajib meninjau dan menguji sistem operasi dan/atau perangkat lunak untuk memastikan tidak ada dampak merugikan pada

proses operasional atau keamanan informasi Pemerintah Kabupaten Seluma pada saat terjadi perubahan sistem operasi dan/atau perangkat lunak, untuk informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA.

(4) Wajib mencegah kemungkinan terjadinya kebocoran informasi.

(5) Wajib melakukan supervisi dan memantau pengembangan perangkat lunak oleh pihak ketiga.

Pasal 23

Pengelolaan kerentanan teknis sebagaimana dimaksud dalam pasal 19 ayat (5) dapat dijelaskan bahwa :

(1) Wajib mengumpulkan informasi kerentanan teknis secara berkala dari seluruh sistem informasi yang digunakan maupun komponen pendukung sistem informasi.

(2) Wajib melakukan evaluasi dan penilaian risiko terhadap kerentanan teknis yang ditemukan dalam sistem informasi serta menetapkan pengendalian yang tepat terhadap risiko terkait.

Pasal 24

Pengendalian pengelolaan gangguan kemanan informasi dalam manajemen pengamanan informasi SPBE sebagaimanan dimaksud Pasal 6 ayat (8) yaitu:

(1) Pegawai dan pihak ketiga wajib melaporkan kepada OPD Diskominfo sesegera mungkin pada saat menemui kelemahan atau terjadi gangguan keamanan informasi dalam sistem atau layanan SPBE di Lingkungan Pemerintah Kabupaten Seluma.

(2) Pengelolaan gangguan keamanan informasi dan perbaikannya :

a. Masing-masing wajib menyusun prosedur dan menguraikan tanggung jawab pegawai, terkait dalam rangka memastikan gangguan keamanan informasi dapat ditangani secara cepat dan efektif.

b. Seluruh gangguan keamanan informasi yang terjadi wajib dicatat dalam suatu basis data dan/atau buku catatan pelaporan gangguan keamanan informasi, yang menjadi masukan pada proses peningkatan penanganan gangguan keamanan informasi, serta dievaluasi dan dianalisa untuk

perbaikan dan pencegahan agar gangguan keamanan informasi tidak terulang.

c. Mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap manajemen pengamanan informasi SPBE di Lingkungan Pemerintah Kabupaten Seluma.

Bagian Kedua

Pengelolaan KeamananJaringan

Pasal 25

(1) OPD Diskominfo wajib mengelola dan melindungi jaringan dari berbagai bentuk ancaman;

(2) OPD Diskominfo wajib mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan serta mencantum kannya dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh pihak ketiga.

Bagian Ketiga

Penanganan Media PenyimpanData

Pasal 26

(1) OPD Diskominfo wajib membuat prosedur yang mengatur penanganan media penyimpan data untuk melindungi asset informasi;

(2) Penanganan media penyimpanan data di lingkungan Pemerintah Kabupaten Seluma sesuai dengan standar penanganan media penyimpan data yang ditetapkan dalam Standar Pengelolaan Data Elektronik di Lingkungan Pemerintah Kabupaten Seluma.

Bagian Keempat

Pertukaran Informasi

Pasal 27

(1) Pertukaran informasi dan perangkat lunak antara Pemerintah Kabupaten Seluma dengan pihak ketiga dilakukan atas kesepakatan tertulis kedua belah pihak;

(2) Pemilik informasi wajib melakukan penilaian risiko yang memadai sebelum melaksanakan pertukaran informasi;

(3) Wajib menerapkan pengendalian keamanan informasi untuk

pengiriman informasi melalui surat elektronik atau pengiriman informasi melalui jasa layanan pengiriman dalam rangka menghindari akses pihak yang tidak berwenang;

BABIV

STANDAR

Pasal 28

(1) Penerapan kebijakan manajemen pengamanan informasi SPBE di Lingkungan Pemerintah Kabupaten Seluma
   a. Wajib menggunakan catatan penerapan untuk mengukur kepatuhan dan efektivitas penerapan manajemen pengamanan informasi SPBE;
   b. Catatan penerapan manajemen pengamanan informasi SPBE sebagaimana tersebut dalam angka 1, meliputi Formulir-formulir sesuai prosedur operasional yang dijalankan, Catatan gangguan keamanan informasi, Catatan dari sistem, Catatan pengunjung di *securearеas*, Kontrak dan perjanjian layanan, Perjanjian kerahasiaan dan Laporan Audit.

(2) Penyusunan dokumen pendukung kebijakan keamanan informasi wajib memuat:
   a. Tujuan dan ruang lingkup dokumen pendukung kebijakan keamanan informasi;
   b. Kerangka kerja setiap tujuan/sasaran pengendalian keamanan informasi;
   c. Metodologi penilaian risiko;
   d. Penjelasan singkat mengenai standar, prosedur, dan kepatuhan termasuk persyaratan peraturan yang wajib dipenuhi, pengelolaan kelangsungan kegiatan, konsekuensi apabila terjadi pelanggaran.
   e. Pengendalian dokumen, wajib mengendalikan dokumen manajemen pengamanan informasi SPBE di lingkungan Pemerintah Kabupaten Seluma untuk menjaga kemutakhiran dokumen, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan dan mencegah akses oleh pihak yang tidak berwenang.

f. Menempatkan dokumen manajemen pengamanan informasi SPBE Pemerintah Kabupaten Seluma di semua area operasional sehingga mudah diakses oleh pengguna di unit kerja masing-masing sesuai peruntukannya.

Bagian Kesatu

Pengendalian organisasi keamanan informasi

Pasal 29

(1) Kepala Dinas Kominfo sebagai pejabat yang berperan sebagai CISO di lingkungan Pemerintah Kabupaten Seluma bertanggung jawab untuk:
   a. Mengkoordinasikan perumusan dan penyempurnaan manajemen pengamanan informasi SPBE diLingkungan Pemerintah Kabupaten Seluma;
   b. Memelihara dan mengendalikan penerapan manajemen pengamanan informasiSPBE di seluruh area yang menjadi tujuan sasaran pengendalian;
   c. Menetapkan target keamanan informasi setiap tahunnya serta menyusun rencana kerja;
   d. Memastikan efektivitas dan konsistensi penerapan manajemen pengamanan informasi SPBE serta mengukur kinerja keseluruhan;dan
   e. Melaporkan kinerja dan capaian penerapan manajemen pengamanan informasi SPBE di Lingkungan Pemerintah Kabupaten Seluma kepada Bupati Seluma.
(2) Dinas Kominfo sebagai Satuan Tugas Keamanan Informasi bertanggung jawab untuk:
   a. Memastikan manajemen pengamanan informasi SPBE di Lingkungan Pemerintah Kabupaten Seluma diterapkan secara efektif;
   b. Memastikan langkah-langkah perbaikan sudah dilakukan berdasarkan saran dan rekomendasi yang diberikan dalam pelaksanaan evaluasi dan/atau audit penerapan manajemen pengamanan informasi SPBE;
   c. Memastikan peningkatan kesadaran, kepedulian, dan kepatuhan seluruh pegawai terhadap manajemen

pengamanan informasi SPBE;

d. Melaporkan kinerja penerapan manajemen pengamanan informasi SPBE sesuai ruang lingkup tanggung jawabnya kepada Kepala Pusat Data dan Teknologi Informasi sebagai pejabat yang berperan sebagai CISO,untuk digunakan sebagai dasar peningkatan keamanan informasi;
e. Mengkoordinasikan penanganan gangguan keamanan informasi di tingkat Pemerintah Kabupaten Seluma;dan
f. Memastikan terlaksanyanya audit internal terhadap penerapan manajemen pengamanan informasi SPBE paling sedikit 1 (satu) kali dalam 3 (tiga)tahun.

Bagian Kedua

Pengendaliankepatuhan

Pasal 30

Kepatuhan terkait audit system informasi dalam manajemen pengamanan SPBE wajib memperhatikan hal-hal sebagai berikut:

(1) Persyaratan audit wajib disetujui oleh CIO Pemerintah Kabupaten Seluma dan/atau Pimpinan Unit Eselon II;
(2) Ruang lingkup pemeriksaan/audit wajib disetujui dan dikendalikan oleh pihak berwenang;
(3) Pemeriksaan perangkat lunak dan data wajib dibatasi untuk akses baca saja;
(4) Selain akses baca saja diizinkan untuk salinan dari *file* sistem yang di isolasi, yang wajib dihapus bila audit telah selesai,atau diberikan perlindungan yang tepat jika ada kewajiban untuk menyimpan *file* tersebut di bawah persyaratan dokumentasi audit;
(5) Sumber daya untuk melakukan pemeriksaan wajib secara jelas diidentifikasi dan tersedia;
(6) Persyaratan untuk pengolahan khusus atau tambahan wajib diidentifikasi dan disepakati;
(7) Semua akses wajib dipantau dan dicatat untuk menghasilkan jejak audit, dan untuk data dan system informasi sensitive wajib mempertimbangkan pencatatan waktu (*timestamp*) pada jejak audit;

(8) Semua prosedur, persyaratan, dan tanggung jawab wajib didokumentasikan;dan

(9) Auditor wajib independen dari kegiatan yang diaudit.

BAB V

KETENTUAN PENUTUP

Pasal 31

Peraturan Bupati ini berlaku sejak tanggal diundangkan.

Agar setiap orang dapat mengetahuinya, memerintahkan pengundangan Peraturan ini dengan penempatannya dalam Berita Daerah Kabupaten Seluma.

Ditetapkan di Tais
pada tanggal 23 Agustus 2019
BUPATI SELUMA

H. BUNDRA JAYA

Diundangkan di Tais
Pada tanggal ..23... Agustus 2019
SEKRETARIS DAERAH,

IRIHADI

BERITA DAERAH KABUPATEN SELUMA TAHUN 2019 NOMOR 33