BUPATI PADANG PARIAMAN
PROVINSI SUMATERA BARAT

KEPUTUSAN BUPATI PADANG PARIAMAN
NOMOR 107/KEP/BPP/2023

TENTANG

MANAJEMEN LAYANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

BUPATI PADANG PARIAMAN,

Menimbang :

a. bahwa untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan Sistem Pemerintahan Berbasis Elektronik (SPBE) kepada Pengguna SPBE, dan untuk memberikan dukungan terhadap layanan publik berbasis elektronik dan layanan administrasi pemerintahan berbasis elektronik agar Layanan SPBE tersebut dapat berjalan secara berkesinambungan, berkualitas, responsif, dan adaptif;

b. bahwa untuk menjalankan proses pelayanan kepada pengguna, pengoperasian layanan, dan pengelolaan Aplikasi SPBE agar Layanan SPBE dapat berjalan berkesinambungan dan berkualitas, perlu menyusun manajemen layanan SPBE;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Bupati Padang Pariaman tentang Manajemen Layanan Sistem Pemerintahan Berbasis Elektronik;

Mengingat :

1. Undang-Undang Nomor 12 Tahun 1956 tentang Pembentukan Daerah Otonom Kabupaten Dalam Lingkungan Daerah Propinsi Sumatera Tengah (Lembaran Negara Republik Indonesia Tahun 1956 Nomor 25);
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) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
3. Undang–Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
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 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 Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);

6. Undang–Undang Nomor 1 Tahun 2022 tentang Hubungan Keuangan Antara Pemerintah Pusat dan Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6757);
7. 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);
8. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 215, Tambahan Lembaran Negara Republik Indonesia Nomor 5357);
9. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
10. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
11. Peraturan Daerah Kabupaten Padang Pariaman Nomor 10 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Padang Pariaman Tahun 2016 Nomor 10, Tambahan Lembaran Daerah Kabupaten Padang Pariaman Nomor 10) sebagaimana telah diubah dengan Peraturan Daerah Nomor 7 Tahun 2021 tentang Perubahan Atas Peraturan Daerah Nomor 10 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Padang Pariaman Tahun 2021 Nomor 7, Tambahan Lembaran Daerah Kabupaten Padang Pariaman Nomor 5);

MEMUTUSKAN:

Menetapkan : KEPUTUSAN BUPATI PADANG PARIAMAN TENTANG SISTEM MANAJEMEN LAYANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

KESATU : Manajemen Layanan Sistem Pemerintahan Berbasis Elektronik merupakan serangkaian proses untuk mencapai penerapan SPBE yang efektif, efisien, dan berkesinambungan, serta layanan SPBE yang berkualitas.

KEDUA : Manajemen layanan SPBE sebagaimana dimaksud Diktum KESATU, mencakup empat fungsi utama, yaitu:

a. pengelolaan pusat layanan SPBE;
b. pengelolaan pengoperasian layanan SPBE;
c. pengelolaan kompetensi teknis SPBE; dan
d. pengelolaan aplikasi SPBE.

- 3 -

KETIGA : Penerapan Manajemen Layanan SPBE berpedoman pada Standar Nasional Indonesia dan/atau Standar Internasional di bidang manajemen layanan teknologi informasi

KEEMPAT : Pedoman Manajemen Layanan Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Padang Pariaman tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan ini.

KELIMA : Segala biaya yang timbul sehubungan dengan pelaksanaan Keputusan ini, dibebankan pada Anggaran Pendapatan dan Belanja Daerah Kabupaten Padang Pariaman Tahun Anggaran berjalan melalui Dokumen Pelaksanaan Anggaran Dinas Komunikasi dan Informatika Kabupaten Padang Pariaman.

KEENAM : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Parit Malintang
pada tanggal 27 September 2023

BUPATI PADANG PARIAMAN,

SUHATRI BUR

Tembusan disampaikan kepada Yth:
1. Sdr. Inspektur Kabupaten Padang Pariaman di Parit Malintang;
2. Sdr. Kepala Badan Pengelola Keuangan Daerah Kabupaten Padang Pariaman di Parit Malintang; dan
3. Sdr. yang bersangkutan.

LAMPIRAN
KEPUTUSAN BUPATI PADANG PARIAMAN
NOMOR 107/KEP/BPP/2023
TANGGAL27 September 2023
TENTANG
MANAJEMEN LAYANAN SISTEM
PEMERINTAHAN BERBASIS ELEKTRONIK

BAB 1. PEDOMAN MANAJEMEN KEAMANAN INFORMASI

1.1 ASET INFORMASI YANG DIMAKSUD MENCAKUP:

1. Data/dokumen: data ekonomi dan keuangan, data gaji, data kepegawaian, dokumen tender dan kontrak, kebijakan Pemerintah Kabupaten Padang Pariaman, hasil penelitian/analisis pasar, bahan pelatihan, prosedur operasional, rencana kelangsungan bisnis (business continuity plan), rencana kerja tahunan, dan hasil audit;
2. Perangkat lunak: perangkat lunak aplikasi, perangkat lunak sistem, perangkat bantu pengembangan sistem, dan perangkat bantu lainnya (antivirus, sistem monitor);
3. Aset fisik: peralatan komputer, mobile device, peralatan jaringan dan komunikasi, removable media (misalnya: flashdisk, CD, DVD, disket), dan peralatan penunjang lainnya (misalnya: UPS, pembangkit tenaga listrik/generator, antena komunikasi);
4. Aset tak berwujud (intangible), termasuk pengetahuan, pengalaman dan keahlian, citra dan reputasi.

1.2 ARAHAN MANAJEMEN UNTUK KEAMANAN INFORMASI

1. Penyelenggaraan layanan TI harus dilakukan dengan menerapkan strategi dan kontrol-kontrol keamanan informasi sesuai ketentuan peraturan perundang- undangan. Dalam hal ketentuan peraturan perundang-undangan belum tersedia, maka dapat berpedoman pada Standar Nasional Indonesia dan/atau standar internasional.
2. Seluruh informasi penting yang dikelola dan disimpan dalam file elektronik (softcopy) atau dokumen tercetak (hardcopy) harus dilindungi terhadap kemungkinan kerusakan, kesalahan penggunaan secara sengaja atau tidak sengaja, dicegah dari akses oleh pengguna (pengguna) yang tak berwenang dan dihindari dari ancaman terhadap

kerahasiaan (confidentiality), keutuhan (integrity) dan/atau ketersediaannya (availability).

3. Tim Koordinasi SPBE meningkatkan kepedulian (awareness), pengetahuan dan pemahaman tentang tata kelola keamanan informasi bagi pegawai dan pihak eksternal melalui pendidikan, pelatihan, dan sosialisasi secara berkala dengan memanfaatkan media komunikasi yang tersedia.
4. Seluruh pegawai dan pihak eksternal harus menjaga dan melindungi keamanan informasi dan sistem informasi yang dikelola dan digunakan serta mematuhi kebijakan dan prosedur keamanan informasi yang berlaku.
5. Seluruh kerawanan dan gangguan/insiden keamanan informasi yang terjadi dalam penyelenggaraan layanan TI harus dilaporkan ke pimpinan unit kerja yang bertanggung jawab terhadap keamanan informasi dan ditindaklanjuti segera.
6. Penggunaan aset TI dan perubahan yang terjadi terhadapnya harus diidentifikasi, dianalisis dan dikendalikan risikonya dengan menerapkan kontrol-kontrol keamanan yang memadai sehingga potensi risiko yang mungkin terjadi dapat diminimalisir. Pelaksanaan pengukuran dan pengendalian risiko SPBE sesuai dengan ketentuan peraturan perundang-undangan.
7. Setiap pengecualian terhadap pedoman ini dan kebijakan turunannya harus mendapatkan persetujuan dari Pimpinan unit kerja di Sekretariat Jenderal yang menyelenggarakan fungsi pengelolaan data, informasi, dan teknologi informasi.
8. Kesesuaian terhadap pedoman ini akan dipantau secara berkala minimum 1 (satu) tahun sekali dan setiap pelanggaran yang terjadi dapat dikenakan sanksi atau tindakan disiplin sesuai dengan peraturan yang berlaku.

1.3 KOMPONEN ORGANISASI KEAMANAN INFORMASI

1. Organisasi Internal
   a) Menetapkan tujuan implementasi pengamanan informasi dengan jelas dan tepat sesuai kebutuhan Pemerintah Kabupaten Padang Pariaman dan regulasi yang berlaku.
   b) Menyetujui Kebijakan dan Pedoman Manajemen Keamanan Informasi.

c) Mengalokasikan tugas, tanggung jawab dan sumber daya untuk implementasi keamanan informasi.

d) Menjalankan program security awareness training untuk seluruh lapisan pegawai.

e) Meninjau efektivitas implementasi kebijakan dan pedoman keamanan SPBE.

2. Perangkat Bergerak (Mobile Device)

a) Menjaga perangkat bergerak ditempatkan di kendaraan (termasuk mobil), ruang publik, kamar hotel, tempat pertemuan, pusat konferensi, dan daerah lain yang tidak dilindungi di luar lingkungan Pemerintah Kabupaten Padang Pariaman.

b) Perangkat bergerak yang membawa informasi penting dan sensitif tidak boleh dibiarkan tanpa pengawasan dan jika memungkinkan harus diamankan secara fisik terkunci atau menggunakan kunci khusus.

c) Saat menggunakan perangkat bergerak di tempat umum, pengguna harus memastikan bahwa data tidak dapat dibaca oleh orang yang tidak berwenang.

d) Laptop dan gawai yang berisi file rahasia Pemerintah Kabupaten Padang Pariaman, termasuk namun tidak terbatas pada Data Kepegawaian, Laporan Audit, dan data rahasia lainnya harus dilindungi dengan kata sandi atau metode autentikasi lainnya.

e) Semua insiden kehilangan atau pencurian perangkat bergerak yang berisi informasi rahasia dan sensitif harus segera dilaporkan ke pengelola barang milik negara di masing-masing unit kerja dan unit pelaksana teknis maksimal 1 x 24 jam.

f) Dalam kondisi tertentu, jika perangkat bergerak berisi informasi rahasia Pemerintah Kabupaten Padang Pariaman, yang memerlukan perbaikan harus dilakukan oleh pihak eksternal yang tidak memiliki perjanjian kerjasam a dengan Pemerintah Kabupaten Padang Pariaman, maka terlebih dahulu harus diinformasikan kepada unit kerja di masing-masing unit organisasi yang menyelenggarakan fungsi pengelolaan data, informasi dan teknologi informasi untuk dilakukan penghapusan, pemindahan atau penonaktifan informasi atau konfigurasi sebelum dilakukan perbaikan oleh pihak eksternal. Pegawai yang menggunakan peralatan perangkat bergerak kantor bertanggung

jawab untuk melakukan reguler pencadangan data.

g) Perlindungan data sensitif harus dilaksanakan sesuai dengan Klasifikasi Informasi.

h) Dalam hal perangkat bergerak ditinggalkan, aturan untuk perangkat pengguna tanpa pengawasan harus diterapkan sesuai dengan Penggunaan Aset Informasi.

3. Teleworking

a) Teleworking adalah perangkat/peralatan informasi dan komunikasi yang digunakan untuk memungkinkan pegawai melakukan pekerjaan mereka di luar kantor Pemerintah Kabupaten Padang Pariaman.

b) Kegiatan teleworking hanya diizinkan kepada pegawai yang bersangkutan memenuhi syarat-syarat sebagai berikut:

1) Mendapat persetujuan atasan langsung pegawai yang bersangkutan.

2) Pegawai yang diizinkan untuk melakukan kegiatan teleworking harus mencegah akses tidak berwenang oleh keluarga, teman, tamu, atau pihak yang tidak berwenang lainnya terhadap perangkat dan atau informasi milik Pemerintah Kabupaten Padang Pariaman.

3) Penggunaan aplikasi untuk kontrol jarak jauh dikoordinasikan dengan unit kerja di Sekretariat Jenderal yang menyelenggarakan fungsi-fungsi pengelolaan data, informasi, dan teknologi informasi.

4. Working Collaboration

1) Working Collaboration adalah perangkat yang digunakan untuk bekerja sama tanpa harus bertatap muka.

2) Penggunaan perangkat working collaboration melalui persetujuan Kepala unit kerja di Sekretariat Jenderal yang menyelenggarakan fungsi-fungsi pengelolaan data, informasi, dan teknologi informasi.

3) Saat melakukan working collaboration, pengguna harus memastikan bahwa data tidak dapat diakses oleh orang yang tidak berwenang.

1.4 KEAMANAN SUMBER DAYA MANUSIA

1. Sebelum Jadi Pegawai

a) Verifikasi atas calon pegawai dilakukan dengan mengacu kepada prosedur rekrutmen yang diatur dalam kebijakan dan prosedur kepegawaian yang berlaku.

b) Sebagai syarat tanggung jawab keamanan informasi, setiap calon pegawai harus menandatangani dokumen Pernyataan Menjaga Rahasia yang merupakan bagian dari perjanjian kerja/pakta integritas.

2. Selama Jadi Pegawai

a) Semua pegawai dan pihak eksternal di Pemerintah Kabupaten Padang Pariamanharus mendapatkan pengetahuan tentang keamanan informasi.

b) Pegawai dan pihak eksternal terkait yang terlibat dalam pengelolaan keamanan informasi harus mendapatkan pendidikan dan pelatihan yang memadai.

c) Program pelatihan dan kepedulian (awareness) harus dilakukan secara berkala sekurang-kurangnya 1 (satu) tahun sekali.

d) Harus ada proses pendisiplinan yang resmi dan terkomunikasikan terhadap penindakan pegawai yang melakukan pelanggaran keamanan informasi sesuai dengan ketentuan peraturan perundangan-undangan.

3. Penghentian dan Perubahan Kepegawaian

a) Pengembalian aset milik Pemerintah Kabupaten Padang Pariaman oleh pegawai yang berhenti bekerja sesuai prosedur yang berlaku.

b) Aset yang harus dikembalikan meliputi manual, dokumentasi, tanda pengenal, kartu akses, komputer, dan barang-barang lainnya yang dipinjam.

c) Pencabutan hak akses terhadap sistem informasi yang dimiliki pegawai dan pihak eksternal lainnya diatur sesuai dengan Pengendalian Hak Akses.

1.5 MANAJEMEN KEAMANAN ASET

1. Tanggung Jawab Terhadap Keamanan Aset

a) Inventarisasi Aset

1) Tanggung jawab pegawai dan pengguna eksternal terhadap aset yang dikuasainya diatur dalam Penggunaan Aset Informasi.

2) Yang termasuk dengan aset informasi adalah namun tidak terbatas pada:

- Informasi: data pegawai, data keuangan, dokumentasi sistem dan sebagainya
- Perangkat lunak aplikasi dan sistem
- Perangkat keras seperti komputer, alat komunikasi, removable media dan sebagainya
- Layanan pendukung seperti jaringan komunikasi dan

listrik

- o Sumber daya manusia termasuk keahlian, pengalaman dan kualifikasi.

3) Setiap unit kerja harus mengidentifikasi dan menginventarisasi seluruh aset informasi yang kritikal yang dimiliki serta memelihara aset tersebut agar selalu ter-update.

4) Inventaris aset harus dilengkapi dengan informasi yang jelas mengenai aset yang bersangkutan sesuai dalam Daftar Inventaris Aset

b) Kepemilikan Aset

1) Pemilik aset memiliki tanggung jawab untuk mengklasifikasikan aset informasi dengan tepat dan secara berkala melakukan peninjauan ulang terhadap pembatasan akses dan klasifikasi informasi.

2) Semua pegawai dan pengguna pihak eksternal harus mengembalikan semua aset yang dikuasainya ketika terjadi penghentian kepegawaian, kontrak atau perjanjian mereka.

2. Klasifikasi Informasi

a) Informasi harus diklasifikasikan sesuai persyaratan hukum, nilai, kekritisan dan kerentanan terhadap pengungkapan atau modifikasi yang tidak sah.

b) Klasifikasi aset informasi terdiri atas Publik, Internal, dan Rahasia.

c) Metode klasifikasi informasi dan penanganan aset mengacu pada nilai informasi, sensitifitas/kekritisan informasi, tingkat kerahasiaan dan tingkat kerawanannya bagi Pemerintah Kabupaten Padang Pariaman.

d) Setiap dokumen yang di dalamnya terdapat informasi yang diklasifikasikan harus diberi label sesuai dengan klasifikasi dari informasi yang bersangkutan.

3. Pedoman Klasifikasi Informasi

Penentuan klasifikasi informasi pada prinsipnya berada di tangan pemilik informasi untuk menetapkan suatu informasi hanya bisa digunakan secara internal atau bisa disebarluaskan ke pihak lain. Metode klasifikasi informasi mengacu hal berikut:

a. Nilai informasi - berdasarkan dampak negatif terhadap Pemerintah Kabupaten Padang Pariaman dalam menjalankan tugas dan fungsinya, reputasi, berpotensi menimbulkan risiko keamanan publik, berpotensi digunakan pihak lain untuk mengancam ketersediaan sistem atau layanan yang diberikan Pemerintah Kabupaten Padang Pariaman, yang dinilai dalam penilaian risiko.

b. Sensitivitas dan kekritisan informasi - berdasarkan risiko tertinggi dihitung untuk setiap item informasi selama

penilaian risiko.

c. Hukum dan kewajiban kontrak.

4. Tingkat Kerahasiaan

Tabel 4.1 Tingkat Kerahasiaan

Tingkat Kerahasiaan	Deskripsi	Contoh
Publik	Informasi yang tidak rahasia dan dapat dipublikasikan ke masyarakat umum tanpa ada implikasi bagi Pemerintah Kabupaten Padang Pariaman. Hilangnya ketersediaan informasi sebagai akibat dari system downtime dianggap sebagai risiko yang dapat diterima.	Brosur-brosur layanan yang didistribusikan secara luas. Informasi yang tersedia pada website resmi Pemerintah Kabupaten Padang Pariaman yang dapat diakses oleh publik. Laporan keuangan yang wajib di-publish keluar sesuai persyaratan yang dibuat oleh pemerintah.
Internal	Informasi yang Penggunaannya terbatas pada internal Pemerintah Kabupaten Padang Pariaman. Penggunaan oleh publik atau pihak eksternal harus mendapatkan persetujuan dari pemilik informasi. Penggunaan informasi ini tanpa izin akan berdampak pada efektivitas operasional Pemerintah Kabupaten Padang Pariaman, menyebabkan kerugian keuangan, menyebabkan kepercayaan masyarakat terhadap Pemerintah Kabupaten Padang Pariaman menjadi turun. Harus disimpan dalam tempat yang tertutup dan dihancurkan jika tidak akan digunakan lagi. Ini adalah klasifikasi default untuk informasi yang diolah atau dihasilkan dari setiap aktivitas Pemerintah Kabupaten Padang Pariaman jika klasifikasi belum ditetapkan.	Norma, Standar, Prosedur, dan Kriteria (NSPK) yang digunakan di seluruh unit kerja. Laporan progres pekerjaan Nota dinas, surat dinas dan memo dinas. Risalah rapat.

Rahasia	Informasi berdampak serius terhadap kepentingan umum, Pelayanan Publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara. Akses ke informasi dibatasi hanya dalam lingkup Pemerintah Kabupaten Padang Pariaman . Penanganan pada level tertinggi untuk aspek integritas, kerahasiaan, dan ketersediaan secara khusus sangat diperlukan. Penyebaran informasi ini ke pihak eksternal/lain harus dengan persetujuan	Gaji atau informasi personal lainnya terkait kepegawaian. Informasi akuntansi dan laporan keuangan internal yang belum di- publish. NDA (Non-Disclosure Agreement) dengan mitra atau pihak eksternal. Hasil audit/pemeriksaan yang sedang dilakukan. Dokumen pengadaan yang sedang berlangsung

5. Klasifikasi Ulang

Pemilik aset harus mengkaji dokumentasi aset informasi setiap 1 (satu) tahun sekali.

6. Pelabelan Informasi

a) Dokumen kertas - tingkat kerahasiaan ditandai di sudut kanan atas halaman utama atau bagian depan atau amplop yang membawa dokumen.

b) Dokumen elektronik - tingkat kerahasiaan ditunjukkan di sudut kanan dokumen utama.

c) Surat elektronik - tingkat kerahasiaan ditunjukkan di baris pertama dari tubuh surat elektronik.

d) Informasi yang dikirimkan secara lisan dan tertulis lainnya - tingkat kerahasiaan informasi rahasia yang akan disampaikan dalam komunikasi tatap muka, melalui telepon, aplikasi berbagi pesan, atau media komunikasi lain, harus dikomunikasikan tingkat kerahasiaannya sebelum menyampaikan informasi itu sendiri dan/atau memanfaatkan fitur kanal rahasia yang dimiliki aplikasi tersebut.

7. Kendali Informasi Rahasia

Tabel 4.2 Kendali Informasi Rahasia

Jenis	Publik	Internal	Rahasia
Dokumen Kertas	- Dokumen dapat diperoleh oleh publik. - Dokumen dapat dikirimkan via mesin fax. - dokumen dapat dicetak.	- hanya orang yang memiliki izin untuk mengakses. Jika dokumen dikirim keluar Pemerintah Kabupaten Padang Pariaman, dokumen harus tercatat sebelum terkirim dokumen hanya dapat disimpan dalam ruangan tanpa akses public - dokumen harus dipastikan dikeluarkan dari mesin printer atau mesin fax. -	- Dokumen harus tersimpan di dalam tempat yang terkunci - Dokumen hanya dapat dipindahkan di dalam atau di luar Pemerintah Kabupaten Padang Pariaman dengan amplop tertutup Jika dokumen dikirim keluar Pemerintah Kabupaten Padang Pariaman, dokumen harus dikirimkan dengan bukti tanda terima. - Dokumen harus segera dikeluarkan dari mesin printer atau mesin fax. - Hanya pemilik dokumen yang dapat menggandakan dokumen. - Hanya pemilik dokumen yang dapat menghancurkan dokumen.
Dokumen Elektronik	- dokumen dapat disimpan dalam keadaan tanpa pengamanan - dokumen tidak diwajibkan disimpan dalam tempat tertentu.	- hanya personil yang berwenang yang mempunyai akses. - Ketika file dipertukarkan melalui layanan	- dokumen harus tersimpan dalam keadaan terenkripsi.

		seperti FTP, pesan singkat, dan lain-lain, harus dilindungi kata sandi.	
	- dokumen dapat dipertukarkan via layanan seperti FTP, pesan singkat, dan lain-lain.	- akses ke sistem informasi dimana dokumen tersimpan harus dilindungi kata sandi yang kuat. - Pastikan layar sudah dalam keadaan terkunci pada saat meninggalkan tempat kerja. - Layar dimana dokumen ditampilkan harus secara otomatis terkunci setelah 3 menit layar tidak aktif.	- Hanya personil yang berwenang atas dokumen, yang dapat mengakses bagian sistem informasi dimana dokumen tersimpan. - Ketika file dipertukarkan melalui layanan seperti FTP, pesan singkat, dll, harus dienkripsi. - Hanya pemilik dokumen yang dapat menghapus Dokumen.
Sistem Informasi	- akses terhadap sistem informasi dapat dilakukan oleh siapa pun.	- hanya personil yang berwenang yang mempunyai akses. - akses ke sistem informasi harus dilindungi oleh kata sandi yang kuat. - Pastikan layar sudah dalam keadaan terkunci pada saat meninggalkan tempat kerja. - Layar harus secara otomatis terkunci setelah setelah 3 menit layar tidak aktif. - sistem informasi hanya dapat berada ruangan dengan akses fisik dikendalikan.	- Perlakuan sistem informasi klasifikasi di internal berlaku juga di sistem informasi klasifikasi rahasia ini. - pengguna harus log-out dari sistem informasi jika telah meninggalkan tempat kerja baik sementara atau permanen. - informasi harus dihapus dengan algoritma yang menjamin penghapusan aman.
		- sistem informasi hanya dapat berada di kamar dengan akses fisik dikendalikan.	

Surat elektronik	Surat elektronik yang dikirimkan harus menggunakan akun surat elektronik resmi Pemerintah Kabupaten Padang Pariaman. Surat elektronik yang ditujukan ke pihak-pihak di luar Pemerintah Kabupaten Padang Pariaman maka alamat penerima tidak ditampilkan (alamat penerima ditempatkan pada blind copy carbon (bcc)).	Surat elektronik yang dikirimkan harus menggunakan akun surat elektronik resmi Pemerintah Kabupaten Padang Pariaman hanya personil yang berwenang yang mempunyai akses. pengirim harus dengan hati- hati memeriksa siapa penerima e-mail. Dokumen atau data internal yang dikirimkan ditujukan hanya untuk sesama domain dalam Pemerintah Kabupaten Padang Pariaman . Surat elektronik yang ditujukan ke pihak-pihak diluar Pemerintah Kabupaten Padang Pariaman maka alamat penerimatidak ditampilkan (alamat penerima ditempatkan pada blind copy carbon (bcc)).	surat elektronik yang dikirimkan harus menggunakan akun surat elektronik resmi Pemerintah Kabupaten Padang Pariaman dan dilakukan oleh pegawai tertentusaja dalam Pemerintah Kabupaten Padang Pariaman. Dokumen atau data confidential yang ingin dikirimkan di luar Pemerintah Kabupaten Padang Pariaman harus berdasarkan persetujuan pemilik data/dokumen dan terdokumentasi siapa Penerima data/dokumen tersebut, kapan diterimanya, dan tujuan dari dibutuhkannya dokumen tersebut. Surat elektronik yang ditujukan ke pihak-pihak di luar Pemerintah Kabupaten Padang Pariaman maka alamat penerima tidak ditampilkan (alamat penerima ditempatkan pada blind copy carbon (bcc)).
Media penyimpan an elektronik	Media penyimpanan dan dokumen tidak diwajibkan dalam keadaan terenkripsi. dapat disimpan di berbagai jenis media tanpa diatur secara khusus keamanannya	hanya pegawai yang berwenang yang mempunyai akses. media atau dokumen harus dilindungi kata sandi. Jika dikirim keluar Pemerintah Kabupaten Padang Pariaman, media harus tercatat sebelum terkirim.	- media penyimpanan perangkat bergerak Portable Media(USB Flash Disk, External HDD, Laptop, dan Iainlain) harus disimpan ditempat yang terkunci. Mekanisme penyimpanan

		media hanya disimpan dalam ruangan dengan akses fisik dikendalikan. mekanisme penyimpanan informasi pada layanan penyimpanan daring Pemerintah Kabupaten Padang Pariaman dikendalikan oleh pemilik informasi. mekanisme penyimpanan informasi pada media perangkat bergerak (Portable Media), contoh: Flash Disk, External HDD, Laptop dan gawai lainnya dikendalikan olehpemilik informasi.	informasi pada layanan penyimpanan daring Pemerintah Kabupaten Padang Pariaman harus dilindungi kata sandi. perangkat bergerak (Portable Media), contoh: Flash Disk, External HDD, Laptop dan gawai lainnya harus dienkripsi dengan metode Full Disk Encryption. media penyimpanan CD, DVD dan read only media lainnya harus dilindungi dengan Kata sandi Protected File. Jika media dikirim ke luar Pemerintah Kabupaten Padang Pariaman, media harus dikirim dengan bukti tanda terima. hanya pemilik media Yang dapat menghancurkan medianya.

1.6 KENDALI AKSES

1. Pengendalian Hak Akses

    a. Hak akses terhadap aset-aset informasi harus diberikan sesuai dengan kebutuhan fungsi dan tugas pegawai dan diberikan sesuai kebutuhan pegawai dalam menjalankan tugasnya.

    b. Akses ke jaringan dan layanan jaringan milik Pemerintah Kabupaten Padang Pariaman diatur oleh unit kerja di Sekretariat Jenderal yang menyelenggarakan fungsi pengelolaan data, informasi, dan teknologi informasi.

2. Pendaftaran pengguna dan Pemberian Hak Akses Ketentuan pendaftaran akses pengguna:

    a. Identitas pengguna (User ID) harus unik, tidak diperbolehkan adanya Identitas pengguna yang sama.

b. Identitas pengguna beserta hak aksesnya hanya diberikan kepada pengguna setelah mendapat persetujuan dari pemilik informasi.

c. Hak akses yang diberikan kepada pengguna harus sesuai dengan kebutuhan tugas/operasional.

d. Hak akses yang diberikan kepada pengguna tidak boleh melanggar prinsip pemisahan tanggung jawab (segregation of duty).

e. Pengguna harus menyetujui pernyataan bahwa mereka memahami dan akan mentaati ketentuan mengenai penggunaan Identitas pengguna.

f. Daftar identitas pengguna untuk setiap aplikasi harus dimutakhirkan.

g. Hak akses pengguna yang telah berganti jabatan harus segera disesuaikan atau dihapus.

h. Identitas pengguna milik pegawai yang sudah berhenti bekerja dari Pemerintah Kabupaten Padang Pariaman harus segera dinonaktifkan.

3. Pengelolaan Hak Akses Khusus

a. Akses khusus seperti identitas pengguna root, administrator atau super user hanya diberikan dalam keadaan khusus untuk menjaga kelangsungan operasional atau tugas dan diberikan untuk jangka waktu sementara selama diperlukan berdasarkan penugasan yang diberikan oleh pejabat yang berwenang.

b. Penggunaan hak akses khusus perlu memperhatikan beberapa hal berikut:

c. Penggunaannya harus melalui proses otorisasi formal.

d. Pemberian hak akses khusus hanya dilakukan dalam keadaan mendesak untuk mendukung kebutuhan tugas atau operasional.

e. Penggunaan hak akses khusus harus memenuhi prinsip "segregation of duties" dan "dual control".

f. Aktivitas yang dilakukan dengan menggunakan hak akses khusus harus dicatat, didokumentasikan, dan ditinjau.

4. Peninjauan Ulang Hak Akses Pengguna

a. Peninjauan ulang terhadap hak akses sistem dan perangkat teknologi informasi dilaksanakan paling sedikit 1 (satu) bulan sekali dalam rangka memastikan pengguna masih berhak terhadap akses yang diberikan, dan melakukan penghapusan pengguna yang sudah tidak aktif.

b. Dilakukan pada saat pengguna yang bersangkutan mengalami perubahan jabatan (promosi, demosi, atau mutasi) oleh pimpinan yang bersangkutan berkoordinasi dengan pengelola sistem/aplikasi atau pemilik data/informasi.

5. Pengelolaan Kata Sandi

    a. Pengguna harus menerapkan kebiasaan keamanan yang baik ketika memilih dan menggunakan kata sandi:

        i. Kata sandi tidak boleh diketahui oleh orang lain, termasuk administrator.

        ii. Kata sandi yang dibuat oleh pengguna tidak boleh disebarkan melalui saluran apapun (melalui lisan, tertulis maupun secara elektronik dan lain- lain); kata sandi harus diganti apabila terdapat indikasi bahwa kata sandi atau sistem mungkin telah dibobol, dalam kasus tersebut, kejadian insiden keamanan ini harus segera dilaporkan.

        iii. Kata sandi yang kuat harus digunakan, dengan cara sebagai berikut:

            1. Menggunakan paling sedikit 8 (delapan) karakter.

            2. Menggunakan setidaknya satu karakter angka/numerik.

            3. Menggunakan setidaknya satu karakter huruf besar dan huruf kecil.

            4. Menggunakan setidaknya satu simbol.

        iv. Kata sandi harus diganti secara periodik setiap 3 (tiga) bulan dengan kata sandi yang berbeda.

        v. Kata sandi tidak boleh disimpan dalam sistem log-on otomatis kecuali yang sudah ditetapkan.

6. Pengendalian Akses Sistem Operasi dan Aplikasi

    a. Proses log-on ke dalam sistem operasi dan aplikasi harus dibuat untuk meminimalkan terjadinya akses tidak sah dengan tidak memunculkan informasi yang dapat membantu pengguna tidak sah untuk mengakses sistem operasi dan aplikasi.

    b. Kendali tambahan kontrol untuk mengendalikan akses kedalam sistem operasi dan aplikasi yaitu:

        i. Pada saat log-on terdapat peringatan bahwa komputer hanya dapat diakses oleh pengguna yang berhak.

        ii. Membatasi jumlah kesalahan dalam percobaan log-on dan sistem harus melakukan hal-hal berikut apabila jumlah kesalahan maksimal telah dilampaui:

            1. Mencatat setiap percobaan log-on baik yang gagal maupun berhasil.

            2. Memberikan jeda waktu sebelum log-on dapat dilakukan kembali atau menolak percobaan kembali setelah terjadi kesalahan dalam percobaan log-on.

            3. Memberikan pesan peringatan bahwa jumlah maksimal percobaan log-on telah terlampaui.

iii. Membatasi waktu minimal dan maksimal untuk proses log-on.

iv. Tidak menampilkan kata sandi yang dimasukkan pada saat log-on.

v. Tidak mentransmisikan kata sandi yang tidak dienkripsi dalam jaringan.

c. Identitas pengguna yang digunakan untuk mengakses sistem harus unik untuk setiap pengguna.

d. Akses kedalam sistem harus diautentikasi sekurang-kurangnya dengan menggunakan kata sandi. Untuk aplikasi harus ditambahkan autentikasi lainnya (two steps authentication).

e. Semua akses ke dalam sistem operasi beserta aktivitas yang dilakukan harus tercatat pada log.

f. Sistem harus dikonfigurasi agar pengelolaan kata sandi oleh sistem dapat memenuhi beberapa persyaratan di bawah ini:

i. Memungkinkan pengguna untuk memilih dan mengubah kata sandi sendiri.

ii. Memaksa pengguna menggunakan kata sandi yang kuat (tidak mudah ditebak atau diretas).

iii. Memastikan perubahan kata sandi secara berkala sesuai dengan ketentuan pengelola kata sandi.

iv. Memaksa pengguna mengganti kata sandi pada penggunaan pertama kali.

v. Mencegah penggunaan kembali kata sandi yang sudah pernah digunakan kecuali sudah melewati 2 (dua) kali siklus perubahan kata sandi yang diperbolehkan.

vi. Tidak menampikan kata sandi pada layar saat di-input.

vii. Penyimpanan dan pengiriman kata sandi harus menggunakan perlindungan khusus seperti enkripsi atau hash atau lainnya.

g. Penggunaan system utilities harus dibatasi dengan proses autentikasi.

h. System utilities harus terpisah dari aplikasi perangkat lunak.

i. Terdapat log untuk semua penggunaan system utilities.

j. System utilities yang tidak digunakan harus dihapus atau tidak diaktifkan.

k. Pembatasan akses ke informasi dan fungsi aplikasi didokumentasikan.

l. Pembatasan akses pada sistem aplikasi dan informasi dilakukan dengan pemberian hak akses baca (read), tulis (write), hapus (delete) dan eksekusi (execute).

m. Akses pada direktori, folder, atau file yang diberikan kepada semua pengguna harus dihapus. Semua akses harus diberikan secara manual.

7. Pengendalian Akses ke Kode Sumber (Source Code)

   a. Akses atas kode sumber harus dikendalikan untuk mencegah akses oleh pihak yang tidak berwenang.

   b. Pengendalian akses ke kode sumber dilakukan dengan cara:

      i. Penyimpanan kode sumber tidak dilakukan pada sistem produksi.

      ii. Akses terhadap kode sumber harus melalui proses otorisasi.

      iii. Daftar kode sumber perlu dibuat, dipelihara dan dijaga.

      iv. Setiap akses ke kode sumber perlu didokumentasikan, termasuk loguntuk akses tersebut.

8. Pemeliharaan kode sumber harus dilakukan melalui mekanisme Manajemen Perubahan.

1.7 KENDALI KRIPTOGRAFI

1. Apabila terdapat kebutuhan pengamanan data atau informasi sensitif pada sistem aplikasi yang dikembangkan, maka standar kriptografi atau enkripsi yang digunakan adalah:

   a. Enkripsi digunakan untuk melindungi informasi rahasia milik Pemerintah Kabupaten Padang Pariaman yang dikirimkan melalui jaringan komunikasi di luar Pemerintah Kabupaten Padang Pariaman.

   b. Enkripsi dilakukan berdasarkan kajian risiko untuk menentukan tingkat perlindungan yang dibutuhkan.

2. Kendali kriptografi di Pemerintah Kabupaten Padang Pariaman dikoordinasikan oleh unit kerja di Sekretariat Jenderal yang menyelenggarakan fungsi-fungsi pengelolaan data, informasi, dan teknologi informasi.

1.8 KEAMANAN FISIK DAN LINGKUNGAN

1. Area Aman (Secure Area)

   a. Pengamanan fisik sarana pemrosesan informasi

      Fasilitas pemrosesan informasi harus ditempatkan dalam area aman yaitu tempat atau ruangan yang dilengkapi dengan fasilitas pengamanan untuk mencegah akses secara fisik oleh pihak yang tidak berwenang serta perlindungan dari kerusakan dan gangguan dari lingkungan.

   b. Daftar area aman adalah segala tempat kerja bagi pegawai di Pemerintah Kabupaten Padang Pariaman termasuk di dalamnya:

      i. Ruang Pusat Data (Data Center atau DC),

ii. Ruang Pusat Pemulihan Bencana (Disaster Recovery Center atau DRC); dan

iii. Ruang Kerja Pegawai.

c. Kendali Akses Masuk

Akses ke area aman dilindungi dengan beberapa alat kendali, antara lain:

i. Kunci pintu akses.

ii. Kamera CCTV.

d. Pengendalian akses fisik

i. Seluruh pegawai, pihak eksternal, dan pengunjung yang memasuki area kerja Pemerintah Kabupaten Padang Pariaman harus membawa dan menggunakan kartu identitas yang diberikan oleh Pemerintah Kabupaten Padang Pariaman.

ii. Pengunjung memasuki area aman harus mencatat dalam buku tamu di resepsionis yang minimal berisi nama pengunjung, nama atau alamat instansi, keperluan berkunjung, pegawai yang akan ditemui dan tanggal, jam masuk dan jam keluar dan harus didampingi dengan pegawai yang bersangkutan.

iii. Seluruh pihak eksternal harus diberikan akses terbatas saat mengakses sumber informasi Pemerintah Kabupaten Padang Pariaman dan aktifitas mereka harus diawasi dan dikaji secara reguler.

2. Perlindungan terhadap risiko gangguan lingkungan

Fasilitas pemrosesan sistem informasi harus dilindungi dari risiko kerusakan yang disebabkan oleh faktor alam dan perbuatan manusia. Pengendalian terhadap risiko lingkungan:

a. Fisik Bangunan

i. Pengamanan fisik bangunan.

ii. Fisik bangunan DC dan DRC, seperti bahan yang tidak mudah terbakar, sistem saluran air dan udara yang baik, kekuatan bangunan dalam menahan beban perangkat DC/DRC dan peralatan peralatan berat lainnya;

iii. Ketersediaan pengendalian hama (pest control) untuk menanggulangi gangguan dari tikus dan hewan pengganggu lainnya.

iv. Ketersediaan sistem penangkal petir.

v. Ketersediaan pasokan air ke dalam gedung.

vi. Ketersediaan dan lokasi saluran udara di dalam gedung.

vii. Ketersediaan lapisan anti bocor.

b. Pengendali Suhu dan Kelembaban Ruangan DC dan DRC

   i. Pengendalian menggunakan AC presisi atau biasa disingkat PAC (Precision Air Conditioning) adalah salah satu sistem pendingin yang dibuat untuk menjaga secara konstan suhu (temperature) 18 s.d 24 derajat celcius; dan

   ii. kelembaban (RH: Relative Humidity 50% dengan toleransi ± 5%) pada suatu ruangan tertutup yang didalamnya terdapat perangkat yang membutuhkan pendingin secara kontinyu.

c. Pencegahan Kebakaran

   i. Larangan merokok di area DC dan DRC;

   ii. Larangan terhadap keberadaan bahan-bahan kimia serta bahan yang mudah terbakar lainnya dalam area DC dan DRC;

   iii. Pengecekan secara berkala terhadap mekanisme serta sistem pemadaman kebakaran;

   iv. Secara fisik dilakukan pemisahan permanen antara area DC dan DRC terutama untuk Ruang server dan Ruang Telekomunikasi dengan area lainnya;

   v. Akses yang mudah serta kejelasan dalam pengoperasian alat-alat pemadam kebakaran.

d. Pemasangan Sistem Deteksi Api

   i. Pemasangan deteksi asap (smoke) dan panas (heat) di bawah raised floor, di langit-langit dan di atas plafon;

   ii. Instalasi pull stations alarm yang berguna untuk memperingatkan seluruh penghuni gedung akan adanya kejadian kebakaran;

   iii. Instalasi signaling devices, baik menggunakan sinyal suara maupun cahaya untuk memperingatkan seluruh penghuni gedung akan adanya kejadian kebakaran.

e. Sistem Pemadam Kebakaran

   i. Instalasi sistem pemadam kebakaran otomatis yang menggunakan gas (fire Suppression system), yang tidak merusak perangkat keras dan tidak berakibat berisiko terhadap manusia, direkomendasikan menggunakan gas nn100 atau jenis lainnya;

   ii. Instalasi dilakukan pada Ruang server, Ruang Telekomunikasi, Ruang Data serta Ruang UPS;

   iii. Penempatan tabung gas yang terpisah secara fisik dengan Ruang server dan Ruang Telekomunikasi;

iv. Kemampuan dalam mendeteksi ada tidaknya operator yang masih berada di dalam ruang sebelum gas pemadam kebakaran dilepaskan;

v. Alat pemadam kebakaran manual, alat pemadam api ringan (APAR) atau portable tersedia dalam jumlah yang memadai dan diletakkan pada lokasi-lokasi yang mudah dijangkau dan strategis. Pemasangan tanda-tanda letak alat pemadam serta panduan penggunaan yang jelas, biasanya berupa gambar cara pengoperasian.

f. Pendeteksi Kebocoran Air

Pemasangan deteksi kebocoran air (water leak detector) yang biasanya dipasang di bawah raised floor dekat dengan PAC dan biasanya diintegrasikan juga dengan kontrol yang ada di PAC.

g. Bekerja dalam area aman

i. Seluruh aktifitas atau pekerjaan pihak eksternal harus disetujui oleh pimpinan unit organisasi, unit kerja, atau unit pelaksana teknis dan diawasi oleh pegawai yang ditugaskan;

ii. Tidak diperkenankan untuk membawa makanan, minuman, dan tidak diperbolehkan merokok sesuai ketentuan masing- masing ruangan;

iii. Segala peralatan perekam (audio maupun video) tidak boleh dibawa masuk ke dalam area aman tanpa persetujuan dari pejabat yang berwenang.

3. Pengamanan Peralatan (Equipment)

a. Penempatan dan perlindungan peralatan pengendalian

i. Peralatan harus ditempatkan di lokasi sesuai dengan tingkat kekritisan dan klasifikasi yang mengacu kepada Manajemen Aset.

ii. Seluruh peralatan harus memiliki rencana pemeliharaan yang memadai atau asuransi berdasarkan nilai peralatan.

iii. Peralatan tidak boleh dipindahlokasikan kecuali telah diizinkan oleh pemilik peralatan.

b. Sarana pendukung

i. Peralatan dan fasilitas sistem informasi yang kritikal bagi kelangsungan tugas Pemerintah Kabupaten Padang Pariaman harus dilengkapi dengan Uninterrupted Power Supply (UPS).

ii. Sumber daya listrik cadangan termasuk UPS, pembangkit listrik cadangan, dan lain-lain harus dilakukan pemeliharaan dan pengujian secara berkala untuk memastikan sarana pendukung tersebut dapat berfungsi setiap saat bila diperlukan.

c. Pemeliharaan peralatan

i. Perangkat komputer, komunikasi data dan perangkat sistem informasi lainnya dilakukan perawatan preventif secara berkala harus sesuai spesifikasi dari pabrik pembuat untuk meminimalkan risiko terjadinya kerusakan pada perangkat tersebut.

ii. Pemeliharaan peralatan hanya boleh dilakukan oleh personil yang berwenang dan kompeten.

iii. Pemeliharaan peralatan harus menjaga kerahasiaan informasi yang terdapat di dalam peralatan tersebut. Apabila peralatan harus dikirim keluar lokasi Pemerintah Kabupaten Padang Pariaman, maka media penyimpanan data (storage) di dalamnya harus dilepas dari posisinya terlebih dahulu.

d. Pengamanan kabel

i. Kabel listrik dan komunikasi data yang digunakan untuk fasilitas pemrosesan informasi harus terlindung secara fisik dengan baik, misalnya menggunakan rumah kabel (wiring duct).

ii. Semua kabel listrik harus dipasang dan dipelihara sesuai dengan ketentuan yang ditetapkan oleh perusahaan penyedia listrik.

iii. Jalur kabel data harus terlindungi dari intersepsi dan harus dipasang secara terpisah dari kabel listrik, untuk menghindari terjadinya induksi.

iv. Semua kabel data harus diberi label dan instalasi jalur kabel harus didokumentasikan.

e. Pengamanan peralatan di luar area Pemerintah Kabupaten Padang Pariaman

i. Jika aset berada di luar lokasi Pemerintah Kabupaten Padang Pariaman , aset tersebut harus dikendalikan oleh pegawai yang diberikan izin.

ii. Prosedur pengamanan peralatan di luar Pemerintah Kabupaten Padang Pariaman termasuk pemusnahan dan penggunaan kembali perangkat informasi harus mengacu pada Penggunaan Aset Informasi.

f. Pemusnahan dan Penggunaan Kembali Perangkat Informasi

i. Berdasarkan Klasifikasi Informasi, data harus dihapus dengan beberapa cara, seperti Format, Secure Erase (wipe), dan Factory Reset untuk perangkat penyimpanan bergerak. Namun jika proses penghapusan tersebut kurang cukup aman berdasarkan sensitivitas data, maka media penyimpanan harus dimusnahkan.

ii. Penyimpanan dan pemusnahan dokumen dilakukan sesuai dengan ketentuan perundang-undangan.

g. Pemindahan informasi

i. Peralatan sistem informasi milik Pemerintah Kabupaten Padang Pariamanhanya boleh dibawa keluar area Pemerintah Kabupaten Padang Pariaman setelah disetujui oleh pihak yang berwenang.

ii. Pemindahan peralatan harus didokumentasikan dan diawasi.

h. Tambahkan terkait alat pemadam kebakaran, kebocoran, hama tikus.

4. Pengosongan Meja dan Layar

a. Pengosongan meja

i. Jika personil yang berwenang sedang tidak berada di tempat kerja, seluruh dokumen kertas, termasuk media penyimpanan data yang bersifat rahasia, tidak diletakkan di atas meja secara sembarangan dan harus dipindahkan dari meja atau tempat lain (printer, mesin fax, mesin fotokopi, dan lain-lain) untuk mencegah akses tidak sah terhadap dokumen tersebut.

ii. Setelah selesai menggunakan papan tulis (whiteboard), informasi yang bersifat rahasia pada papan tulis harus segera dihapus untuk mencegah terbacanya informasi rahasia.

iii. Dokumen dan media harus disimpan ditempat dan dengan cara yang aman.

b. Pengosongan layar

i. Jika personil yang berwenang sedang tidak berada di tempat kerja, seluruh informasi yang bersifat rahasia harus dihapus dari layar, dan layar harus ditinggalkan dalam keadaan terlindungi dengan kata sandi.

ii. Apabila personil yang berwenang meninggalkan tempat kerja, maka komputer harus dalam keadaan terkunci.

c. Perlindungan terhadap fasilitas Bersama

i. Dokumen yang mengandung informasi sensitif harus segera disingkirkan dari printer, fax, mesin fotokopi, dan seluruh area yang bukan tempat kerja

pegawai yang bersangkutan. Dokumen terkait harus terlindungi dari orang- orang yang tidak berkepentingan.

ii. Untuk pengiriman dan penerimaan surat atau dokumen yang bersifat rahasia, harus tercatat di Tata Usaha. Ketika penerima surat atau dokumen tidak hadir, maka surat tersebut disimpan di Tata Usaha masing-masing bagian sampai penerima sudah hadir.

iii. Akses tidak sah untuk penggunaan printer, mesin fotokopi, mesin pemindai, dan peralatan lain yang berada di seluruh area kerja Pemerintah Kabupaten Padang Pariaman harus dicegah dengan cara memberikan akses kontrol berupa PIN atau kata sandi.

1.9 KEAMANAN OPERASIONAL

1. Prosedur dan Tanggung Jawab Operasional

   Prosedur operasional sistem informasi harus dibuat meliputi sekurang-kurangnya:

   a. Job Scheduling;

   b. Pencadangan dan restore;

   c. Penanganan dan eskalasi permasalahan;

   d. Prosedur restart dan recovery sistem;

   e. Pendistribusian output; dan

   f. Pengaktifan dan pengelolaan log.

2. Manajemen Perubahan

   a. Seluruh perubahan terhadap fasilitas pengolah dan pengelola informasi harus dikendalikan dan terdokumentasi untuk menjamin perubahan pada sistem informasi terkelola dan terkendali dengan benar.

   b. Setiap perubahan yang dilakukan pada sistem operasional atau sistem produksi harus dilakukan dengan cara berikut:

      i. Pengajuan perubahan dapat diajukan oleh seluruh unit organisasi;

      ii. Perubahan harus disetujui oleh pemilik sistem/aplikasi;

      iii. Perubahan harus diimplementasikan oleh personil yang berwenang;

      iv. Pemilik sistem/aplikasi bertanggung jawab untuk memeriksa bahwa perubahan yang dilakukan telah memenuhi permintaan perubahan;

      v. Pemilik Sistem/Aplikasi bertanggung jawab untuk menguji dan memeriksa stabilitas sistem. Sistem tidak boleh dipasang ke dalam

         sistem produksi sebelum pengujian secara keseluruhan benar-benar dilakukan;

      vi. Konfigurasi sistem pengembangan, pengujian dan produksi harus dipelihara dan dimutakhirkan atas setiap perubahan yang dilakukan.

   c. Setelah implementasi perubahan akan dilakukan sosialisasi ke pihak terkait.

3. Prinsip Pemisahan Tugas dan Tanggung Jawab (Segregation of Duties) dan Dual Control

   a. Pemisahan tugas dan tanggung jawab dilaksanakan untuk mencegah adanya pihak atau personil yang dapat melakukan kesalahan atau pelanggaran baik disengaja atau tidak disengaja, tanpa diketahui atau tanpa terdeteksi.

b. Harus ada pemisahan tugas dan tanggung jawab diantara fungsi yang disebut di bawah ini:
    i. Pengembangan Teknologi Informasi
    ii. Operasional Teknologi Informasi
    iii. Strategi, Perencanaan, dan Keamanan Teknologi Informasi
c. Aktifitas yang memiliki risiko tinggi harus dikerjakan dan diperiksa oleh personil yang berbeda.
d. Sistem dan prosedur harus dirancang untuk tidak memungkinkannya seorang personil dapat menjalankan suatu proses atau transaksi yang berisiko tinggi, tanpa adanya kendali dari personil lainnya.
e. Prinsip dual control harus dilaksanakan untuk memastikan terlaksananya fungsi check and balance. Dual Control harus dilaksanakan untuk fungsi- fungsi berikut ini:
    i. Konfigurasi Keamanan Informasi;
    ii. Instalasi dan pemeliharaan sistem pengendalian akses;
    iii. Perubahan parameter pada Operating Sistem;
    iv. Pemeliharaan firewall rule;
    v. Pelaksanaan Prosedur Darurat (emergency procedure);
    vi. Penggunaan Super Pengguna (super user);
    vii. Pengelolaan kunci kriptografi;
    viii. Fungsi-fungsi lainnya yang dapat menimbulkan kerugian apabila dilaksanakan dengan cara yang salah atau dilakukan secara tidak sah.
f. Jika terjadi kendala dalam menjalankan prinsip dual control maka harus dilakukan bentuk pengawasan lain (compensating control) seperti proses monitoring, audit log review dan pengawasan dari pimpinan di atasnya.

4. Pemisahan Aktivitas Pengembangan, Pengujian, dan Operasional
    a. Fasilitas pengembangan aplikasi dan pengujian aplikasi harus berada pada sistem yang terpisah dari lingkungan produksi.
    b. Lingkungan pengujian aplikasi harus memiliki kesamaan konfigurasi dan spesifikasi dengan lingkungan produksi aplikasi.
    c. Prosedur pemindahan aplikasi dari pengembangan ke produksi harus ditetapkan secara formal.
    d. Compiler, editor, dan tools pengembangan lain tidak diperbolehkan untuk digunakan pada sistem produksi kecuali saat emergency.
    e. Konfigurasi sistem pengembangan, pengujian dan produksi harus dipelihara.

5. Pengelolaan Layanan Pihak Eksternal

    a. Layanan oleh pihak eksternal harus dipastikan memenuhi tingkat layanan yang sesuai dengan Service Level Agreement (SLA) dan persyaratan keamanan informasi yang sudah ditentukan.

    b. Pihak eksternal harus memiliki kemampuan dan perencanaan untuk menghadapi kegagalan atau bencana, sehingga pihak eksternal yang bersangkutan dapat memelihara tingkat layanan yang sudah disepakati.

    c. Pengawasan terhadap kinerja pihak eksternal harus dilakukan untuk menjamin:

        i. Kinerja atau service level pihak eksternal sudah sesuai dengan perjanjian.

        ii. Kebenaran laporan layanan tahunan yang disusun oleh pihak eksternal.

        iii. Bila terjadi insiden keamanan informasi, maka dapat dilakukan penanganan sesuai dengan prosedur penanganan insiden keamanan informasi yang berlaku.

    d. Pemilik informasi/sistem harus memiliki kontrol atas keamanan informasi rahasia yang diakses, diproses atau dikelola oleh pihak eksternal.

    e. Pemilik informasi/sistem harus memastikan pihak eksternal melaksanakan pengamanan informasi, identifikasi atas kelemahan sistem informasi dan penanganan insiden keamanan informasi.

    f. Perubahan sistem pada layanan TI oleh pihak eksternal harus ditinjau ulang dan disetujui oleh pemilik informasi/sistem sebelum perubahan diimplementasikan.

6. Perencanaan dan Pemantauan Kapasitas

    a. Semua aktivitas atau proses pada sistem informasi baik yang sedang berjalan maupun yang akan diimplementasikan harus memperhitungkan kebutuhan kapasitas sumber daya sistem.

    b. Proses monitoring sistem dan tuning system harus dilakukan untuk memastikan dan meningkatkan kinerja, ketersediaan dan efisiensi sistem.

    c. Perkiraan/proyeksi kebutuhan kapasitas sistem untuk masa yang akan datang harus diperhitungkan dengan memperhatikan tren pertumbuhan penggunaan sumber daya sistem dan perkembangan kebutuhan.

    d. Perencanaan kapasitas harus dimutakhirkan agar sesuai dengan perubahan yang ada.

    e. Semua sistem baru atau sistem hasil pengembangan harus melalui proses pengujian formal sebelum digunakan.

    f. Proses pengujian sistem agar mengacu pada Pedoman Manajemen Layanan SPBE.

7. Perlindungan Malware dan Pengelolaan Patch

    a. Semua server atau perangkat Pemerintah Kabupaten Padang Pariaman yang kritikal/penting harus menerapkan perlindungan malware. Termasuk di dalamnya adalah pengelolaan patch untuk meminimalkan potensi celah keamanan pada sistem informasi. Kendali deteksi, pencegahan dan pemulihan untuk melindungi terhadap malware harus diimplementasikan.

    b. Sebelum diterapkan di lingkungan operasional, risiko penerapan security patch perlu dikaji dan dilakukan pengujian di fasilitas pengembangan (development) yang tersedia untuk memastikan agar penerapannya tidak menyebabkan gangguan terhadap operasional layanan TI.

    c. Penerapan security patch harus dilakukan dengan mengikuti prosedur manajemen perubahan.

    d. Bukti penerapan security patch harus didokumentasikan dan disimpan.

8. Pencadangan (Backup)

    a. Pencadangan informasi/data dan perangkat lunak yang kritikal harus dibuat untuk dapat memenuhi kebutuhan pemulihan bila terjadi permasalahan atau bencana.

    b. Media pencadangan harus ditempatkan pada lokasi yang aman dan terlindung dari pengaruh lingkungan.

    c. Frekuensi pencadangan disesuaikan dengan masing-masing kebutuhan.

    d. Masa retensi dari pencadangan informasi perlu ditentukan berdasarkan masing-masing kebutuhan, sesuai dengan ketentuan peraturan perundang- undangan, dan kewajiban kontrak.

    e. Media pencadangan yang disimpan di luar (off-site) harus disimpan pada lokasi dengan jarak yang aman dari lokasi pencadangan di kantor (on-site backup).

    f. Media pencadangan harus dilengkapi dengan label.

    g. Hasil pelaksanaan pencadangan harus didokumentasikan.

    h. Media pencadangan data harus diuji secara berkala. Pengujian media pencadangan data dapat dilakukan pada saat pengujian Rencana Pemulihan Bencana atau pada saat adanya permintaan restore data.

9. Pencatatan (Logging) dan Pemantauan

    a. Akses terhadap log harus dibatasi hanya bagi personil dengan tugas dan tanggung-jawab memerlukan akses ke dalam log.

    b. Semua log harus dilindungi dari upaya perubahan, penghapusan, atau penambahan.

c. Kapasitas penyimpanan dokumen log harus dijaga agar tidak menyebabkan terhentinya sistem logging untuk mencatat events atau overwriting pada event log sebelumnya.

d. Log dan log reports dapat mengandung informasi yang bersifat rahasia sehingga harus diklasifikasikan sebagai informasi rahasia dan ditangani sesuai prosedur penanganan informasi rahasia.

e. Logging yang sudah ditetapkan untuk diaktifkan, tidak boleh dinonaktifkan.

f. Log monitoring sistem harus ditempatkan pada jaringan yang terpisah (segregated) dan dilindungi oleh firewall.

g. Log dari server, firewall, dan router harus dicadangkan ke suatu internal log server atau media penyimpan data yang aman dari upaya modifikasi.

h. Masa retensi penyimpanan log harus ditetapkan sesuai dengan kebutuhan dan ketentuan peraturan perundang-undangan.

i. Pencatatan log untuk mencatat aktivitas administrator dan aktivitas operasional pada server atau perangkat sistem lainnya harus meliputi:

   i. Identitas dari administrator atau operator yang digunakan.

   ii. Tanggal dan jam dari kejadian (event) yang berhasil maupun yang gagal.

   iii. Informasi mengenai kejadian (event) atau kegagalan yang terjadi.

j. Administrator dilarang menghapus atau menonaktifkan log dari aktivitas siapapun termasuk diri sendiri.

k. Setiap kegagalan atau kesalahan pada sistem harus dicatat, dilaporkan dan dianalisis serta dilakukan tindakan perbaikan yang sesuai.

l. Error logging pada sistem/aplikasi bila tersedia, harus selalu diaktifkan.

m. Logging dapat berpengaruh terhadap kinerja sistem, oleh sebab itu pengaktifan log harus dilakukan hanya pada error/fault log tertentu sesuai kebutuhan dan dilakukan oleh personil yang kompeten.

n. Jam (clock) dari semua server, komputer, dan perangkat pemroses informasi lainnya harus disinkronisasi sehingga menunjukkan waktu yang sama dengan menggunakan Network Time Protocol (NTP).

10. Kendali Perangkat Lunak Operasional

11. Perangkat lunak yang digunakan untuk kegiatan operasional harus berlisensi atau open source yang sudah disetujui oleh unit kerja di Sekretariat Jenderal yang menyelenggarakan fungsi-fungsi pengelolaan data, informasi, dan teknologi informasi dalam rangka memastikan integritas sistem operasional.

12. Pengelolaan Kerentanan Teknis

    a. Vulnerability Assessment pada sistem operasi, jaringan, basis data maupun aplikasi harus dilakukan secara berkala, misalnya dengan menggunakan penetration testing yang dilakukan setiap 1 (satu) tahun sekali.

    b. Unit kerja yang bertanggung-jawab untuk melakukan vulnerability assessment harus mendapatkan informasi terkini mengenai sistem vulnerabilities dari forum atau melalui keikutsertaan special interest group lainnya.

1.10 KEAMANAN KOMUNIKASI

1. Manajemen Keamanan Jaringan dan Layanan Jaringan
   Pengendalian keamanan pada jaringan harus dikelola dan dikendalikan untuk melindungi informasi yang dikirimkan dan sistem informasi yang menggunakan jaringan tersebut. Dalam hal penyelenggaraan jaringan bekerja sama dengan pihak eksternal (service provider), tingkat layanan (service level), fitur keamanan, dan semua kebutuhan layanan jaringan harus tercakup di dalam kontrak.
2. Perpindahan Informasi
    a. Proses perpindahan informasi dengan pihak eksternal melalui jaringan atau media komunikasi elektronik harus memperhatikan hal-hal berikut ini:
        i. Pengamanan pertukaran informasi dari risiko intersepsi, modifikasi, dan pengalihan kepada penerima yang tidak berhak (misrouting).
        ii. Kriptografi harus digunakan untuk melindungi keamanan informasi rahasia yang dipertukarkan melalui jaringan eksternal, termasuk data yang dipertukarkan melalui lampiran surat elektronik.
        iii. Tidak diperkenankan untuk melakukan meneruskan (forwarding) informasi rahasia dari surat elektronik Pemerintah Kabupaten Padang Pariaman ke surat elektronik pribadi.
        iv. Informasi harus dilindungi dari malicious code pada saat dikirimkan melalui media komunikasi elektronik.
    b. Media komunikasi fisik seperti laptop dan telepon genggam harus dilindungi dengan pengamanan yang cukup, namun tidak terbatas pada kata sandi, PIN, atau kunci sidik jari.
3. Perjanjian Perpindahan Informasi
    a. Sebelum bertukar informasi dan/atau perangkat lunak dengan pihak eksternal, sebuah perjanjian menjaga kerahasiaan harus ditandatangani, yang merupakan tanggung jawab pejabat yang berwenang.
    b. Perjanjian tersebut dapat berupa kertas atau elektronik dan harus berisi klausul yang sesuai dengan ketentuan, termasuk setidaknya otorisasi untuk mengakses informasi, standar teknis untuk transfer data, respon insiden, penanganan informasi rahasia, dan hak cipta.

c. Perjanjian perpindahan informasi untuk pertukaran informasi dengan pihak lain harus memperhatikan aspek keamanan informasi sebagai berikut:
   i. Pengaturan notifikasi atas pengiriman dan penerimaan data.
   ii. Pertukaran informasi yang harus dapat ditelusuri (traceable) dan memenuhi persyaratan kenirsangkalan (non repudiation).
   iii. Tugas dan tanggung jawab apabila terjadi insiden keamanan informasi.
   iv. Perlindungan data seperti penggunaan kriptografi untuk informasi yang rahasia.
   v. Pelabelan informasi yang rahasia.

4. Pesan Elektronik

   Pengiriman informasi milik Pemerintah Kabupaten Padang Pariaman yang menggunakan pesan elektronik (electronic messaging) harus dilindungi dalam rangka pengamanan terhadap aset informasi milik Pemerintah Kabupaten Padang Pariaman dan mitra kerja Pemerintah Kabupaten Padang Pariaman.

1.11 PENGEMBANGAN DAN PEMELIHARAAN SISTEM INFORMASI

1. Persyaratan Keamanan Informasi

   Persyaratan yang terkait keamanan informasi harus termasuk dalam persyaratan untuk sistem informasi baru atau pengembangan sistem informasi yang ada dan didokumentasikan.

   Persyaratan keamanan antara lain, tidak terbatas pada:

   a. Pendefinisian hak akses dan prosedur autentikasinya.

   b. Perlindungan data pengguna dan kata sandi atau data rahasia lainnya di dalam basis data harus dienkripsi atau disamarkan (masking).

   c. Merekam log transaksi (siapa melakukan apa dan kapan) di dalam log untuk keperluan pelacakan (audit trail).

2. Lingkungan Pengembangan yang Aman

   Pemilik sistem informasi harus menyiapkan lingkungan pengembangan yang aman mencakup seluruh daur hidup pengembangan sistem informasi.

3. Pengembangan oleh Alihdaya atau Pihak Eksternal

   Pemilik sistem informasi harus mengawasi dan memantau aktivitas pengembangan sistem yang dialihdayakan.

4. Data Uji

   a. Data yang digunakan dalam pengujian sistem harus dilindungi dari kemungkinan rusak, hilang, atau perubahan yang dilakukan tanpa izin.

b. Beberapa pengendalian berikut dapat dipertimbangkan untuk melindungi data produksi yang digunakan untuk pengujian sistem di lingkungan pengujian (testing) atau pengembangan (development):

   i. Informasi pegawai/pribadi (seperti nama, alamat, nomor telepon dan sebagainya) agar disamarkan.

   ii. Setelah proses pengujian selesai, dan data produksi yang bersangkutan tidak diperlukan lagi, maka harus segera dihapus.

   iii. Penggunaan data produksi untuk pengujian harus didokumentasikan.

1.12 PENGELOLAAN PIHAK EKSTERNAL

1. Keamanan Akses Pihak Eksternal

   a. Sebelum memberikan akses kepada mitra dan pihak eksternal, pemilik sistem wajib mendeteksi dan mengevaluasi risiko-risiko yang mungkin muncul sehubungan dengan pemberian akses dan menerapkan kontrol yang memadai untuk mengurangi dampak atau mencegah terjadiny a risiko-risiko tersebut.

   b. Evaluasi dilakukan dengan memperhatikan aspek-aspek berikut

      i. Jenis akses yang diperlukan seperti akses fisik ke kantor, ruang kerja, atau ruang server, akses non fisik ke dalam jaringan, basis data dan sistem informasi.

      ii. Alasan kebutuhan akses seperti untuk memberi dukungan perangkat keras dan perangkat lunak, audit keamanan informasi dan pengembangan aplikasi dan/atau sistem informasi.

   c. Pengendalian risiko pemberian akses pada pihak eksternal dilakukan antara lain melalui klausul-klausul dalam kontrak dan melalui Pernyataan Menjaga Kerahasiaan (Non-Disclosure Agreement).

2. Kontrak

   Dalam perjanjian kontrak dengan pihak eksternal dicantumkan antara lain:

   a. Kewajiban pihak eksternal mematuhi kebijakan keamanan informasi yang berlaku di Pemerintah Kabupaten Padang Pariaman.

   b. Persetujuan untuk turut melindungi keamanan sumber daya informasi Pemerintah Kabupaten Padang Pariaman terkait dengan akses yang diberikan.

   c. Jenis akses yang diberikan dan tata cara penggunaan akses tersebut.

d. Identitas pegawai/personil pihak eksternal yang menggunakan akses tersebut.

e. Pembatasan lokasi dari mana akses dapat dilakukan dan waktu penggunaan akses.

f. Persetujuan atas hak pantau dan pengawasan yang dilakukan pemilik sistem terhadap penggunaan akses.

g. Setiap aset yang diberikan kepada pihak eksternal wajib dikembalikan saat perjanjian kerja berakhir.

3. Evaluasi dan Peninjauan

a. Pemilik sistem harus secara teratur memeriksa dan memantau tingkat layanan dan pemenuhan klausul keamanan dengan pihak eksternal, laporan dan catatan yang dibuat oleh pihak eksternal, serta audit pihak eksternal setidaknya 1 (satu) tahun sekali.

b. Setiap insiden keamanan yang terkait dengan pihak eksternal harus dilaporkan secepat mungkin kepada Kepala unit kerja di Sekretariat Jenderal yang menyelenggarakan fungsi pengelolaan data, informasi, dan teknologi informasi dan dilakukan penanganan sesuai dengan penanganan insiden keamanan informasi.

c. Layanan oleh pihak eksternal harus dipastikan memenuhi tingkat layanan yang sesuai dengan Service Level Agreement dan persyaratan keamanan informasi yang sudah ditentukan.

d. Harus memastikan bahwa pihak eksternal memiliki kemampuan dan perencanaan untuk menghadapi kegagalan atau bencana, sehingga pihak eksternal yang bersangkutan dapat memelihara tingkat layanan yang sudah disepakati.

e. Melakukan kontrol atas keamanan informasi rahasia yang diakses, diproses atau dikelola oleh pihak eksternal.

f. Pihak eksternal harus melaksanakan pengamanan informasi, identifikasi atas kelemahan sistem informasi dan penanganan insiden keamanan informasi yang dikelolanya.

4. Manajemen Perubahan Pada Layanan TI oleh Pihak Eksternal

Perubahan sistem pada layanan TI oleh pihak eksternal (penyedia layanan TI) harus direviu dan disetujui oleh pemilik sistem sebelum perubahan diimplementasikan.

5. Penghapusan Hak Akses

Ketika terjadi perubahan atau penghentian kontrak:

a. Hak akses bagi pegawai/personil dari pihak eksternal harus dihapus sesuai dengan kebijakan yang berlaku.

b. Pemilik sistem harus memastikan semua peralatan, perangkat lunak, atau informasi dalam bentuk elektronik atau dokumen harus dikembalikan.

1.13 MANAJEMEN INSIDEN KEAMANAN INFORMASI

Prosedur Penanganan Insiden Keamanan Informasi

1. Helpdesk, sebagai Single Point of Contact (SPOC), merupakan kontak pertama dari pengguna jika terjadi insiden/gangguan dengan layanan teknologi informasi. Aktivitas penanganan insiden keamanan informasi adalah:
    a. Pencatatan insiden (incident logging)
    b. Pengkategorisasian insiden (incident categorization)
    c. Prioritas insiden (incident prioritization)
    d. Diagnosa Awal (initial diagnosis).
    e. Eskalasi insiden (incident escalation)
    f. Investigasi (investigation and diagnosis)
    g. Resolusi (resolution dan recovery)
    h. Penutup (incident closure)
    i. Pelaporan penanganan insiden
2. Penanganan insiden/gangguan harus dilaksanakan segera mungkin agar dapat mengembalikan fungsi layanan operasional TI, dengan melaksanakan solusi baik yang bersifat sementara maupun permanen, agar kelangsungan layanan operasional Pemerintah Kabupaten Padang Pariaman tetap berjalan.
3. Penanganan insiden/gangguan harus dilakukan berdasarkan klasifikasi prioritas. Prioritas penanganan dilihat dari sisi urgensi dan dampaknya terhadap operasional dan layanan Pemerintah Kabupaten Padang Pariaman .

1.14 ASPEK KEAMANAN INFORMASI DARI MANAJEMEN KEBERLANGSUNGAN LAYANAN SPBE

Keberlangsungan keamanan informasi harus diintegrasikan ke dalam sistem manajemen keberlangsungan Layanan SPBE Pemerintah Kabupaten Padang Pariaman dengan:

1. Pemilik sistem/aplikasi melakukan pencadangan secara teratur terhadap data dan aplikasi yang digunakan dalam pelayanan teknologi informasi.
2. Dalam hal terjadi ketidaktersediaan Layanan SPBE maka layanan terhadap pengguna dan publik dapat dilakukan secara manual jika memungkinkan sesuai dengan ketentuan peraturan perundang- undangan.
3. Unit kerja di Sekretariat Jenderal yang menyelenggarakan fungsi pengelolaan data, informasi, dan teknologi informasi menetapkan Rencana Pemulihan Bencana (Disaster Recovery Plan atau DRP) bagi seluruh proses Layanan SPBE yang vital.

4. Rencana Pemulihan Bencana dilakukan dengan mempertimbangkan hal-hal sebagai berikut:
    a. Dilakukannya identifikasi aset-aset informasi yang vital dan sensitif, khususnya yang berklasifikasi rahasia.
    b. Dilakukannya identifikasi kejadian-kejadian yang menyebabkan gangguan terhadap aset informasi yang vital dan sensitif.
    c. Ditindaklanjutinya hasil-hasil kajian risiko keamanan informasi.
5. Untuk menjamin agar pengelolaan kelangsungan Layanan SPBE tetap relevan dan efektif, maka pengelolaan kelangsungan Layanan SPBE harus diuji secara rutin, minimal sekali setahun.
6. Hasil pengujian pengelolaan kelangsungan Layanan SPBE dan tindakan perbaikan yang perlu dilakukan harus dilaporkan ke pimpinan unit kerja di Sekretariat Jenderal yang menyelenggarakan fungsi pengelolaan data, informasi, dan teknologi informasi dan pimpinan unit kerja Penyelenggara Layanan SPBE.

1.15 KEPATUHAN

1. Identifikasi Terhadap Hukum dan Peraturan Perundang-undangan
    a. Seluruh pengguna sistem informasi milik Pemerintah Kabupaten Padang Pariaman termasuk pihak eksternal lainnya harus mematuhi kebijakan keamanan informasi Pemerintah Kabupaten Padang Pariaman, dan mentaati ketentuan hukum dan peraturan perundang-undangan yang terkait serta perjanjian tentang lisensi, termasuk persyaratan-persyaratan kontrak yang telah disepakati.
    b. Semua ketentuan tersebut harus dikomunikasikan kepada seluruh unit organisasi, unit kerja, dan unit pelaksana teknis di Pemerintah Kabupaten

       Padang Pariaman yang terkait agar mengetahui kewajibannya untuk mematuhi semua ketentuan tersebut.
2. Hak Atas Kekayaan Intelektual
    a. Seluruh unit organisasi, unit kerja, dan unit pelaksana teknis di Pemerintah Kabupaten Padang Pariaman harus mematuhi ketentuan perlindungan hak atas kekayaan intelektual (HAKI) yang mencakup penggunaan perangkat lunak berlisensi.
    b. Daftar aset yang memiliki hak atas kekayaan intelektual harus dipelihara dengan baik.
    c. Setiap penemuan, kegiatan, atau gagasan-gagasan praktis yang diperoleh pegawai, pihak eksternal, dan mitra kerja selama bekerja atau dibiayai Pemerintah Kabupaten Padang Pariaman adalah menjadi hak milik Pemerintah Kabupaten Padang Pariaman.

d. Lisensi perangkat lunak yang disediakan Pemerintah Kabupaten Padang Pariaman tidak boleh digunakan atau dipasang di peralatan komputer selain milik Pemerintah Kabupaten Padang Pariaman.

3. Perlindungan Terhadap Dokumen Pemerintah Kabupaten Padang Pariaman

a. Dokumen penting milik Pemerintah Kabupaten Padang Pariaman dan/atau yang digunakan dan dihasilkan oleh sistem informasi atau aset informasi yang dikelola Pemerintah Kabupaten Padang Pariaman seperti basis data, audit log, dan transaction log harus dilindungi dari kehilangan, kerusakan, atau penyalahgunaan.

b. Prosedur mengenai retensi, penyimpanan, penanganan, dan pemusnahan dokumen Pemerintah Kabupaten Padang Pariaman sesuai dengan ketentuan peraturan perundang-undangan.

4. Perlindungan Data dan Informasi Pribadi

Seluruh unit organisasi, unit kerja, dan unit pelaksana teknis di Pemerintah Kabupaten Padang Pariaman harus melindungi kepemilikan dan kerahasiaan data pribadi pegawai, mitra kerja dan pihak eksternal yang bekerja sama dengan Pemerintah Kabupaten Padang Pariaman. Data pribadi tersebut hanya boleh digunakan untuk kepentingan yang diperbolehkan oleh ketentuan peraturan perundang- undangan.

5. Kepatuhan Terhadap Kebijakan dan Pedoman Keamanan Informasi

a. Untuk menjamin dipatuhinya kebijakan dan pedoman keamanan informasi oleh seluruh pegawai, unit organisasi, unit kerja, dan unit

pelaksana teknis di Pemerintah Kabupaten Padang Pariaman harus melakukan hal-hal sebagai berikut :

i. Mengkomunikasikan kebijakan dan pedoman keamanan informasi.

ii. Meningkatkan pengetahuan dan keterampilan pegawai dalam pengelolaan keamanan informasi sesuai dengan bidang tugasnya.

iii. Memeriksa dan mengevaluasi tingkat kepatuhan atau kesesuaian pegawai terhadap pelaksanaan kebijakan ini secara berkala.

b. Setiap ketidakpatuhan terhadap kebijakan dan pedoman keamanan informasi, kepala unit organisasi, unit kerja, dan/atau unit pelaksana teknis harus :

i. Menentukan penyebab dari ketidakpatuhan.

ii. Menentukan dan menerapkan tindakan perbaikan yang sesuai.

iii. Menentukan tindakan yang diperlukan untuk mencegah terjadiny a kembali ketidakpatuhan tersebut.

iv. Meninjau efektifitas tindakan perbaikan yang telah dilakukan.

c. Pemeriksaan kesesuaian teknis, seperti tes penetrasi (penetration test), pemindaian jaringan (scanning), atau teknik pencarian kelemahan keamanan informasi lainnya (vulnerability assessment), akan dilakukan secara berkala oleh pegawai yang kompeten baik dari internal Pemerintah Kabupaten Padang Pariaman ataupun menggunakan jasa ahli independen dari luar Pemerintah Kabupaten Padang Pariaman sesuai dengan spesifikasi atau standar yang berlaku.

d. Rencana pemeriksaan kesesuaian teknis harus didokumentasikan, dikomunikasikan, dan disetujui pimpinan unit kerja di Sekretariat Jenderal yang menyelenggarakan fungsi- fungsi pengelolaan data, informasi, dan teknologi informasi.

e. Setiap pemeriksaan teknis harus dicatat dan dilaporkan sebagai masukan bagi evaluasi manajemen keamanan informasi.

6. Pertimbangan Audit Sistem Informasi

a. Kegiatan audit sistem informasi secara berkala dilakukan untuk memaksimalkan efektivitas audit dan meminimalkan gangguan

b. terhadap proses operasional terkait dengan pelaksanaan audit pada sistem informasi.

c. Aktivitas ini harus direncanakan dan disetujui untuk meminimalkan dampak dari gangguan terhadap Layanan SPBE Pemerintah Kabupaten Padang Pariaman.

d. Persyaratan dan aktivitas audit ini harus direncanakan secara hati-hati untuk memperkecil gangguan Layanan SPBE.

e. Akses pada pemeriksaan audit terhadap data dan aplikasi perlu dibatasi dengan akses read only.

f. Hak akses selain read only hanya dibolehkan untuk salinan atau copy dari sistem files yang terbatas dan terisolasi. Salinan atau copy tersebut perlu segera dihapus setelah proses audit selesai atau diberikan perlindungan yang memadai apabila terdapat kebutuhan untuk mendokumentasikan salinan dari sistem files tersebut.

g. Seluruh proses audit sistem informasi harus didokumentasikan secara formal.

- 38 -

7. Perlindungan Terhadap Perangkat Lunak Audit/Audit Tools

   a. Perangkat lunak yang mendukung kegiatan audit harus dikendalikan untuk mencegah kemungkinan penyalahgunaan yang berpotensi tidak akuratnya hasil audit yang dilakukan oleh perangkat tersebut.

Apabila audit dilakukan dengan atau oleh melibatkan pihak eksternal, perangkat lunak audit atau audit tools dan data yang diperiksa harus dijaga dari risiko penyalahgunaan oleh pihak eksternal tersebut.

BUPATI PADANG PARIAMAN,

SUHATRI BUR