SALINAN

PERATURAN WALI KOTA PONTIANAK
NOMOR 25 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA PONTIANAK,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 19 ayat (5) Peraturan Daerah Kota Pontianak Nomor 9 Tahun 2022 tentang Penyelenggaraan Pontianak *Smart City*, perlu menetapkan Peraturan Wali Kota tentang Sistem Manajemen Keamanan Informasi;

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 27 Tahun 1959 tentang Penetapan Undang-Undang Darurat Nomor 3 Tahun 1953 tentang Perpanjangan Pembentukan Daerah Tingkat II di Kalimantan (Lembaran Negara Republik Indonesia Tahun 1953 Nomor 9) Sebagai Undang-Undang sebagaimana telah diubah dengan Undang-Undang Nomor 8 Tahun 1965 tentang Pembentukan Daerah Tingkat II Tanah Laut, Daerah Tingkat II Tapin dan Daerah Tingkat II Tabalong dengan Mengubah Undang-Undang Nomor 27 Tahun 1959 tentang Penetapan Undang-Undang Darurat Nomor 3 Tahun 1953 tentang Pembentukan Daerah Tingkat II di Kalimantan (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 51, Tambahan Lembaran Negara Republik Indonesia Nomor 2756);
3. 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);
4. 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);

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 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Penganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
6. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
7. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 538);
8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Menteri Komunikasi dan Informatika Nomor 41/PER/MEN.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional;
10. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
11. Peraturan Menteri Dalam Negeri Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Berita Negara Tahun 2016 Nomor 1829);
12. Peraturan Menteri Pendayagunaan Aparatur Negara dan reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Resiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
13. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
14 Peraturan Daerah Nomor 9 Tahun 2022 tentang Penyelenggaraan Pontianak *Smart City* (Lembaran Daerah Kota Pontianak Tahun 2022 Nomor 9, Tambahan Lembaran Daerah Kota Pontianak Nomor 216);
15. Peraturan Wali Kota Nomor 20 Tahun 2020 tentang Rencana Induk Sistem Pemerintahan Berbasis Elektronik Kota Pontianak Tahun 2020-2029 (Berita Daerah Kota Pontianak Tahun 2020 Nomor 20);

MEMUTUSKAN:

Menetapkan : PERATURAN WALI KOTA TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:
1. Daerah adalah Kota Pontianak.
2. Pemerintah Daerah adalah Wali Kota sebagai unsur Penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan Pemerintahan yang menjadi kewenangan Pemerintah Kota Pontianak.
3. Wali Kota adalah Wali Kota Pontianak.
4. Sistem adalah suatu kesatuan yang terdiri elemen yang dihubungkan bersama untuk memudahkan aliran data, informasi, atau materi untuk mencapai suatu tujuan.
5. Perangkat Daerah adalah unsur pembantu Wali Kota dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
6. Data adalah catatan atas kumpulan fakta yang belum diolah dan apa adanya.
7. Informasi adalah keterangan, pernyataan, gagasan dan tanda-tanda yang mengandung data, fakta, pesan, yang memiliki nilai dan makna dimana penjelasannya dapat dilihat, didengar dan dibaca yang disajikan dalam berbagai format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik maupun non elektronik.
8. Teknologi Informasi dan Komunikasi adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
9. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk meningkatkan efisiensi, efektifitas, transparansi dan akuntabilitas layanan pemerintahan.
10. Keamanan informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi.
11. Keamanan Informasi SPBE adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan keamanan informasi berdasarkan pendekatan risiko.
12. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan Informasi Elektronik.
13. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer dan/atau media elektronik lainnya.
14. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
15. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik.

16. Dokumen Digital adalah setiap data dan informasi digital yang dibuat, diteruskan, dikirimkan, diterima atau disimpan serta dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, atau simbol yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
17. Risiko adalah peluang terjadinya suatu peristiwa yang akan mempengaruhi keberhasilan terhadap pencapaian tujuan.
18. Manajemen Risiko adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur, dan budaya untuk menentukan tindakan terbaik terkait risiko.
19. Tim Respon Insiden Keamanan Informasi (*Computer Security Incident Response Team*) yang selanjutnya disingat CSIRT adalah tim yang bertanggung jawab untuk memonitor, mengevaluasi, mencegah, menerima, meninjau dan menanggapi laporan dan aktifitas insiden keamanan teknologi informasi.
20. Insiden Siber adalah kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik dan/atau pelanggaran kepatuhan terhadap kebijakan keamanan siber.
21. Aset Informasi adalah unit informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.
22. Aset Pengolahan Informasi adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting informasi.
23. Penyimpanan Informasi adalah suatu proses menyimpan informasi dengan menggunakan media baik elektronik maupun non-elektronik.
24. *Data Center* adalah suatu fasilitas fisik (on-premise) untuk menempatkan sistem komputer dan perangkat-perangkat terkait, seperti sistem komunikasi data dan penyimpanan data.
25. *Cloud* atau dikenal *Cloud Computing* (komputasi awan) adalah sistem komputasi off-premise (non-fisik) yang berfungsi sebagai penyimpanan, pengelolaan, pemrosesan data pada server melalui internet sebagai medianya.
26. Basis Data (*database*) adalah suatu sistem yang menyimpan data dalam jumlah besar dengan mekanisme sistematis dan terstruktur.
27. *File* adalah kumpulan berbagai macam informasi atau data yang tersimpan pada storage komputer atau gadget.
28. *Server* adalah sistem komputer yang menyediakan sumber daya penyimpanan data.
29. *Hard disk* adalah komponen perangkat keras yang menyimpan semua data/dokumen digital.
30. *Flash disk* adalah salah satu media penyimpanan data portabel yang dapat dihubungkan melalui *port USB* suatu komputer.
31. Kartu memori adalah penyimpanan bebasis *flash* dalam bentuk yang ramping dan ringan.
32. *Website* adalah situs atau daerah lokasi jelajah dalam internet.
33. Domain adalah nama unik yang diberikan untuk mengidentifikasi nama server komputer seperti *web server* atau *email server* di jaringan internet.
34. Sub Domain adalah Domain yang merupakan bagian dari domain yang lebih besar sebagai komponen yang lebih rendah tingkatannya dari domain di atasnya.
35. *Back end* adalah bagian belakang layar dari sebuah *website* yang berfungsi untuk mengatur tampilan website yang dilihat oleh pengguna.

BAB II
MAKSUD, TUJUAN DAN RUANG LINGKUP
Pasal 2

Maksud disusunnya Peraturan Wali Kota ini adalah sebagai pedoman bagi Pemerintah Daerah dalam melaksanakan kebijakan, program dan kegiatan terkait manajemen Keamanan Informasi SPBE.

Pasal 3

Tujuan disusunnya Peraturan Wali Kota ini untuk melaksanakan pengelolaan Keamanan Informasi SPBE yang meliputi infrastruktur komputer, jaringan, sistem informasi/aplikasi, dan sumber daya manusia SPBE secara terpadu untuk menjamin kerahasiaan, keutuhan, keaslian, kenirsangkalan serta pengamanannya.

Pasal 4

(1) Ruang Lingkup Peraturan Wali Kota ini mengatur tentang manajemen keamanan informasi dalam penyelnggaraan SPBE di Lingkungan Pemerintah Daerah.
(2) Cakupan pengaturan manajemen keamanan informasi sebagaimana dimaksud pada ayat (1) meliputi:
    a. pengelolaan kebijakan keamanan informasi;
    b. pengelolaan aset informasi;
    c. keamanan jaringan dan sistem;
    d. pengelolaan insiden keamanan informasi;
    e. kepatuhan audit keamanan informasi; dan
    f. peningkatan kesadaran dan pelatihan keamanan informasi.

BAB III
PENGAMANAN INFORMASI
Pasal 5

(1) Pengamanan Informasi merupakan upaya penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, kenirsangkalan serta pengamanan terkait data dan informasi Pemerintah Daerah.
(2) Penjaminan kerahasiaan sebagaimana dimaksud pada ayat (1) dilakukan melalui penetapan klasifikasi keamanan, pembatasan akses, menjaga kerahasiaan data dan informasi dari pihak yang tidak berwenang dan pengendalian keamanan lainnya.
(3) Penjaminan keutuhan sebagaimana dimaksud pada ayat (1) dilakukan melalui penerapan otentifikasi dan pendeteksian modifikasi.
(4) Penjaminan ketersediaan sebagaimana dimaksud pada ayat (1) dilakukan melalui penyediaan cadangan dan pemulihan serta jaminan ketersediaan akses data dan informasi untuk pihak yang berwenang.
(5) Penjaminan keaslian sebagaimana dimaksud pada ayat (1) dilakukan melalui penyediaan mekanisme verifikasi dan validasi.
(6) Penjaminan kenirsangkalan sebagaimana dimaksud pada ayat (1) dilakukan melalui penerapan tanda tangan elektronik dan jaminan pihak ketiga terpercaya melalui penggunaan Sertifikat Elektronik.

Pasal 6

(1) Setiap orang yang bekerja di lingkungan Pemerintah Daerah wajib mengamankan dan melindungi informasi Pemerintah Daerah.
(2) Perlindungan keamanan, kerahasiaan, kekinian, akurasi serta keutuhan data dan informasi menjadi tanggung jawab setiap Perangkat Daerah sesuai dengan kewenangannya dengan memperhatikan tugas dan fungsi masing-masing Perangkat Daerah.
(3) Pelaksanaan perlindungan sebagaimana dimaksud pada ayat (2) dilakukan dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 7

Pengamanan informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) meliputi:
a. aset informasi;
b. aset pengolahan informasi; dan
c. penyimpanan informasi.

Pasal 8

(1) Aset Informasi sebagaimana dimaksud dalam Pasal 7 huruf a meliputi informasi yang tercetak, tertulis, dan tersimpan dalam bentuk fisik dan elektronik.
(2) Aset Informasi yang tercetak dan tertulis dalam bentuk fisik sebagaimana dimaksud pada ayat (1) adalah informasi yang tertuang pada kertas, papan tulis, spanduk, buku atau dokumen.
(3) Aset Informasi yang tersimpan dalam bentuk elektronik sebagaimana dimaksud pada ayat (1) meliputi antara lain: *database* dan *file* di dalam komputer, informasi yang ditampilkan pada *website*, layar komputer, informasi yang dikirimkan melalui sensor pemindai dan peranti lain melalui jaringan telekomunikasi.

Pasal 9

Aset Pengolahan Informasi sebagaimana dimaksud dalam Pasal 7 huruf b berupa:
a. peralatan mekanik yang digerakkan dengan tangan secara manual; dan
b. peralatan elektronik digital yang bekerja secara penuh.

Pasal 10

(1) Penyimpanan Informasi sebagaimana dimaksud dalam Pasal 7 huruf c menggunakan media elektronik dan non elektronik.
(2) Penyimpanan Informasi menggunakan media elektronik sebagaimana dimaksud pada ayat (1) meliputi antara lain:
    a. *data storage*, seperti *server*, *hard disk*, *flash disk*, kartu memori; dan
    b. penyimpanan *cloud*.
(3) Penyimpanan Informasi menggunakan media non elektronik sebagaimana dimaksud pada ayat (1) meliputi antara lain lemari, rak, laci, *filling cabinet*.

BAB IV
SUMBER DAYA
Pasal 11

(1) Kepala Perangkat Daerah menyediakan sumber daya yang dibutuhkan untuk membentuk, mengimplementasikan, memelihara, dan meningkatkan penerapan Keamanan Informasi SPBE secara berkesinambungan.
(2) Perangkat Daerah penyelenggara layanan elektronik wajib menyediakan, mendidik dan melatih sumber daya manusia yang bertugas dan bertanggung jawab terhadap pengamanan dan perlindungan Sistem Elektrtonik mengacu pada Keamanan Informasi SPBE.
(3) Uraian mengenai keamanan sumber daya manusia sebagaimana dimaksud pada ayat (1) dan ayat (2) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Wali Kota ini.

BAB V
MANAJEMEN RISIKO
Pasal 12

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 4 huruf c dilakukan oleh setiap Perangkat Daerah untuk menjamin keberlangsungan SPBE dengan minimalkan dampak risiko dalam SPBE.
(2) Setiap perangkat daerah harus menerapkan prosedur pelaksanaan manajemen risiko meliputi:
    a. komunikasi dan konsultasi;
    b. penetapan konteks risiko SPBE:
        1. inventarisasi informasi umum;
        2. identifikasi sasaran SPBE;
        3. penentuan struktur pelaksanaan manajemen risiko SPBE;
        4. identifikasi pemangku kepentingan;
        5. Identifkasi peraturan perundang-undangan;
        6. Penetapan kategori risiko SPBE;
        7. Penetapan area dampak risiko SPBE;
        8. penetapan kriteria risiko SPBE;
        9. matriks analisis risiko SPBE dan level risiko SPBE; dan
        10. Selera risiko SPBE.
    c. penilaian risiko SPBE;
        1. prioritas risiko;
        2. analisis risiko SPBE; dan
        3. evaluasi risiko SPBE.
    d. penanganan risiko SPBE:
        1. prioritas risiko;
        2. Rencana penanganan risiko SPBE; dan
        3. risiko residual.
    e. pemantauan dan review;
    f. pencatatan dan pelaporan;
    g. dokumen manajemen risiko SPBE:
        1. pakta integritas manajemen risiko SPBE;
        2. dokumen proses risiko SPBE; dan
        3. dokumen proses pengendalian risiko SPBE.
(3) Perangkat Daerah dalam melaksanakan penyusunan dokumen manajemen risiko di lingkungan kerjanya masing-masing dapat berkoordinasi dengan pelaksana teknis keamanan informasi.

BAB VI
MEKANISME PENYELENGGARAAN KEAMANAN
Pasal 13

(1) Setiap Perangkat Daerah penyelenggara Sistem Elektronik memiliki tanggung jawab dalam pengamanan informasi elektronik dengan berkoordinasi dengan Perangkat Daerah yang menyelenggarakan tugas dan fungsi di bidang Teknologi Informasi dan Komunikasi.
(2) Setiap Perangkat Daerah penyelenggara Layanan Elektronik harus memastikan ketersediaan data/informasi dan Sistem Elektronik dalam rangka menjaga kelangsungan teknologi informasi melalui penyelenggaraan fasilitas *Data Center* baik dikelola oleh internal atau pihak penyedia jasa.
(3) Setiap aktivitas pada fasilitas di *Data Center* harus dapat terpantau untuk menghindari kesalahan proses pada sistem dengan memperhatikan aspek perlindungan terhadap data yang diproses dan lingkungan fisik.

Pasal 14

(1) Setiap Perangkat Daerah pengelola Sistem Elektronik harus memperhatikan jaminan kerahasiaan, ketersediaan, kekinian, akurasi, keaslian dan kenirsangkalan data dan informasi yang termuat dalam Sistem Elektronik.
(2) Jaminan kerahasiaan sebagaimana dimaksud pada ayat (1) dilakukan melalui pembatasan akses menuju kontrol panel Sistem Elektronik (*back end*), pengaturan otorisasi, penggantian kode akses (*password*) kontrol panel Sistem Elektronik (*back end*) secara berkala dan pengendalian keamanan lainnya.
(3) Jaminan ketersediaan sebagaimana dimaksud pada ayat (1) adalah Sistem Elektronik harus beroperasi terus menerus selama 24 (dua puluh empat) jam sehari dan 7 (tujuh) hari seminggu serta memiliki penyediaan cadangan dan pemulihan data/informasi.
(4) Jaminan kekinian sebagaimana dimaksud pada ayat (1) adalah sistem elektronik harus terus terbarui, menampilkan data dan informasi terkini.
(5) Jaminan akurasi sebagaimana dimaksud pada ayat (1) adalah kepastian bahwa data dan informasi yang ditampilkan dalam Sistem Elektronik adalah akurat sesuai fakta.
(6) Jaminan keaslian sebagaimana dimaksud pada ayat (1) dilakukan melalui pelaksanaan mekanisme verifikasi dan validasi data/informasi dari pengelola Sistem Elektronik
(7) Jaminan kenirsangkalan sebagaimana dimaksud pada ayat (1) dilakukan melalui penerapan tanda tangan elektronik dan jaminan pihak ketiga terpercaya melalui penggunaan Sertifikat Elektronik.

Pasal 15

(1) Kebijakan penggunaan Sertifikat Elektronik sebagaimana dimaksud dalam Pasal 14 ayat (6) diatur oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Teknologi Informasi dan Komunikasi sesuai dengan ketentuan peraturan perundang-undangan.
(2) Setiap pelaksanaan transaksi elektronik dalam layanan publik menggunakan Sertifikat Elektronik.
(3) Setiap pejabat yang mempunyai kewenangan dalam pelaksanaan Transaksi Elektronik di Perangkat Daerah harus memiliki Sertifikat Elektronik.

(4) Perangkat Daerah yang menyelenggarakan tugas dan fungsi di bidang Teknologi Informasi dan Komunikasi memfasilitasi penyediaan Sertifikat Elektronik serta memonitor penggunaannya pada setiap Perangkat Daerah.

Pasal 16

(1) Perangkat Daerah melaksanakan penerapan Dokumen Digital untuk melakukan penyiapan, pengiriman, penerimaan, penyimpanan, pemeliharaan dan penggunaan data, informasi, dan arsip.
(2) Pengiriman Dokumen Digital antar Perangkat Daerah dan/atau pihak lain harus memuat Tanda Tangan Elektronik yang diverifikasi oleh pejabat yang berwenang.
(3) Pihak lain baik individu, masyarakat dan pelaku usaha dapat mengirim Dokumen Digital kepada pejabat Perangkat Daerah dengan memuat Tanda Tangan Elektronik.
(4) Identitas pengirim dengan Tanda Tangan Elektronik harus dapat dikenal dan diverifikasi.
(5) Penerapan Dokumen Digital dan Tanda Tangan Elektronik sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 17

(1) Dalam rangka pelaksanaan Manajemen Keamanan Informasi SPBE Pemerintah Daerah dan Manajemen Keamanan Informasi SPBE Perangkat Daerah membentuk tim keamanan informasi Manajemen Keamanan Informasi SPBE pemerintah daerah dan tim keamanan informasi Manajemen Keamanan Informasi SPBE Perangkat Daerah yang ditetapkan dengan Keputusan Sekretaris Daerah.
(2) Tim sebagaimana dimaksud pada ayat (1) mempunyai struktur, tugas dan tanggung jawab sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Wali Kota ini.

Pasal 18

(1) Untuk mendukung tugas pengamanan informasi sebagaimana dimaksud dalam Pasal 5 ayat (1), Pemerintah Daerah membentuk CSIRT.
(2) CSIRT sebagaimana dimaksud pada ayat (1) diketuai oleh kepala Perangkat Daerah yang menyelenggarakan tugas dan fungsi di bidang Teknologi Informasi dan Komunikasi, dan beranggotakan pejabat struktural dan fungsional atau petugas yang menyelenggarakan fungsi Teknologi Informasi.
(3) CSIRT sebagaimana dimaksud pada ayat (1) bertanggungjawab memastikan Teknologi Informasi yang digunakan oleh seluruh Perangkat Daerah memenuhi standar dan ketentuan tata kelola keamanan informasi SPBE.
(4) CSIRT memiliki tugas dan wewenang:
    a. melakukan pencegahan terjadinya insiden siber dengan cara terlibat aktif pada penilaian dan deteksi ancaman, perencanaan mitigasi, penyusunan pedoman keamanan Sistem Elektronik dan data elektronik serta pemberian peringatan terkait keamanan siber;
    b. memantau dan memonitor keamanan serta melindungi seluruh Sistem Elektronik atau data elektronik;
    c. menanggapi, menyelidiki dan menangani secara komprehensif serta melakukan pemulihan atas insiden keamanan siber yang menimpa Sistem Elektronik;

d. melakukan evaluasi internal kinerja penyelenggaraan Teknologi Informasi; dan
e. melakukan edukasi dan pelatihan keamanan siber bagi Aparatur Sipil Negara di lingkungan Pemerintah Daerah.

BAB VII
STANDAR DAN PROSEDUR PENGENDALIAN

Pasal 19

(1) Setiap Perangkat Daerah wajib menyelenggarakan Keamanan Informasi SPBE yang mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan dan kerugian.
(2) Setiap Perangkat Daerah harus menyusun standar dan prosedur pengendalian kegiatan teknologi informasi yang memenuhi prasyarat keamanan informasi mengacu kepada Keamanan Informasi SPBE.
(3) Prasyarat keamanan informasi sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan tindakan dalam mengelola risiko yang meliputi aspek sebagai berikut:
    a. organisasi keamanan informasi;
    b. keamanan sumber daya manusia;
    c. pengelolaan aset;
    d. pengendalian akses;
    e. kriptografi;
    f. keamanan fisik dan lingkungan;
    g. keamanan operasional;
    h. keamanan komunikasi;
    i. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
    j. hubungan kerja dengan pemasok (*supplier*);
    k. penanganan insiden keamanan informasi;
    l. kelangsungan usaha; dan
    m. kepatuhan.
    n. perlindungan data pribadi; dan/atau
    o. prosedur pengendalian keamanan SPBE lainnya.
(4) Dalam hal terjadi insiden siber dan/atau kegagalan atau gangguan sistem yang berdampak serius sebagai akibat perbuatan dari pihak lain terhadap Sistem Elektronik, sebagaimana dimaksud pada ayat (1), Perangkat Daerah penyelenggara layanan elektronik wajib mengamankan data dan segera melaporkan dalam kesempatan pertama kepada CSIRT melalui portal layanan CSIRT pada alamat *https://csirt.pontianak.go.id/* serta memberitahukan secara tertulis kepada Wali Kota.
(5) Untuk mengendalikan dan mengevaluasi penerapan Keamanan Informasi SPBE, Perangkat Daerah yang menyelenggarakan urusan di bidang Teknologi Informasi dan Komunikasi dapat melakukan audit keamanan informasi yang dilaksanakan oleh tenaga ahli yang berkompeten terhadap keseluruhan Sistem Elektronik yang diselenggarakan Perangkat Daerah.

Pasal 20

(1) Setiap Perangkat Daerah bertanggung jawab dalam memastikan operasional teknologi informasi yang diselenggarakannya selalu dalam kondisi stabil dan aman.

(2) Penyelenggaraan pemrosesan transaksi pada operasional teknologi informasi harus memenuhi prinsip kehati-hatian.
(3) Setiap Perangkat Daerah penyelenggara teknologi informasi wajib mengidentifikasi dan memantau aktivitas operasional Teknologi Informasi untuk memastikan efektivitas, efisiensi, dan keamanan dari aktivitas tersebut antara lain dengan cara:
   a. menerapkan perimeter fisik dan lingkungan di area kerja dan *Data Center*;
   b. mengendalikan hak akses secara memadai sesuai kewenangan yang ditetapkan;
   c. menerapkan pengendalian terhadap informasi yang diproses;
   d. memastikan ketersediaan dan kecukupan kapasitas layanan jaringan komunikasi baik yang dikelola secara internal maupun oleh pihak lain penyedia jasa;
   e. melakukan pemantauan kegiatan operasional Teknologi Informasi termasuk *audit trail*/riwayat; dan
   f. melakukan pemantauan terhadap aplikasi yang digunakan oleh Perangkat Daerah maupun pengguna.

Pasal 21

(1) Setiap Perangkat Daerah harus melakukan pengendalian terhadap aktivitas teknologi informasi melalui evaluasi dan pemantauan secara berkala.
(2) Setiap Perangkat Daerah wajib melakukan kegiatan pemantauan dan tindakan koreksi penyimpangan terhadap kontrol keamanan informasi yang berada di bawah tanggung jawabnya meliputi:
   a. kegiatan pemantauan secara terus menerus; dan
   b. pelaksanaan fungsi pemeriksaan internal yang efektif dan menyeluruh.
(3) Perangkat Daerah penyelenggara teknologi informasi berdasarkan hasil audit, umpan balik dan evaluasi terhadap pengendalian keamanan informasi yang dilakukan, wajib meningkatkan efektivitas Keamanan Informasi SPBE secara berkesinambungan melalui perbaikan terhadap akibat penyimpangan kegiatan teknologi informasi.
(4) Hasil dari tindakan perbaikan dan peningkatan sebagaimana dimaksud pada ayat (3) harus dilaporkan kepada Kepala Perangkat Daerah dan didokumentasikan.

Pasal 22

(1) Apabila terdapat indikasi kebocoran dan hilangnya data/informasi mempunyai dampak luas pada Perangkat Daerah, maka Pemerintah Daerah dapat menunjuk auditor independen untuk melakukan investigasi yang diperlukan.
(2) Perangkat Daerah penyelenggara teknologi informasi wajib menyediakan akses kepada auditor independen sebagaimana dimaksud pada ayat (1) untuk melakukan Pemeriksaan seluruh aspek terkait penyelenggaraan Teknologi Informasi.

BAB VIII
PEMBINAAN, PENGAWASAN DAN EVALUASI

Pasal 23

(1) Pembinaan penyelenggaraan Manajemen Keamaman Informasi SPBE dilakukan oleh Wali Kota.

(2) Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Teknologi Informasi dan Komunikasi bertugas melakukan pengawasan dan evaluasi terhadap implementasi Manajemen Keamaman Informasi SPBE di lingkungan Pemerintah Daerah.
(3) Pelaksanaan pengawasan dan evaluasi sebagaimana dimaksud pada ayat (2) dilaksanakan paling sedikit 1 (satu) kali dalam 2 (dua) tahun.
(4) Hasil pengawasan dan evaluasi Manajemen Keamanan Informasi SPBE dilaporkan kepada Wali Kota.

BAB IX
PEMBIAYAAN
Pasal 24

Pembiayaan Penyelenggaraan Manajemen Keamanan Informasi SPBE bersumber dari:
a. Anggaran Pendapatan dan Belanja Daerah; dan/atau
b. sumber pembiayaan lainnya yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB X
KETENTUAN PENUTUP
Pasal 25

Peraturan Wali Kota ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Wali Kota ini dengan penempatannya dalam Berita Daerah Kota Pontianak.

Ditetapkan di Pontianak
pada tanggal 30 Agustus 2024

Pj WALI KOTA PONTIANAK,

ttd

ANI SOFIAN

Diundangkan di Pontianak
pada tanggal 30 Agustus 2024

SEKRETARIS DAERAH KOTA PONTIANAK,

ttd

AMIRULLAH

BERITA DAERAH KOTA PONTIANAK TAHUN 2024 NOMOR 25

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM

PEMERINTAH KOTA PONTIANAK SEKRETARIAT DAERAH

FERRY ABDI, S.H., M.H.
Pembina Tk.I
NIP. 19770211 200212 1 002

LAMPIRAN
PERATURAN WALI KOTA PONTIANAK
NOMOR 25 TAHUN 2024
TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

KEBIJAKAN DAN MANAJEMEN KEAMANAN INFORMASI SPBE
PEMERINTAH KOTA PONTIANAK

# BAB I
# PENDAHULAN

## I.1. LATAR BELAKANG

Informasi adalah aset yang sangat penting bagi Instansi Pemerintah Daerah, baik informasi yang terkait dengan data, keuangan, laporan maupun informasi lainnya. Kebocoran, kerusakan, ketidakakuratan, ketidaktersediaan atau gangguan lain terhadap informasi tersebut dapat menimbulkan dampak yang merugikan baik seara finansial maupun non finansial bagi layanan Pemerintah Daerah. Dampak yang dimaksud tidak hanya terbatas ruang lingkup layanan pemerintah, namun juga kepada masyarakat umum, lembaga lain dan bahkan terhadap Sistem Pemerintahan Berbasis Elektronik di lingkup Pemerintahn Daerah.

Mengingat pentingnya informasi, maka informasi harus dilindungi atau diamankan oleh seluruh Pegawai Pemerintah Daerah. Pengamanan informasi sangat bergantung pada pengamanan terhadap semua aspek dan komponen TIK terkait, seperti perangkat lunak, perangkat keras, jaringan, peralatan pendukung (misalnya sumber daya listrik, AC) dan sumber daya manusia (termasuk kualifikasi dan keterampilan).

Pemerintah Daerah beroperasi pada lingkungan bisnis dimana terdapat ketergantungan yang tinggi pada Sistem Informasi dan jaringan komputer yang saling berhubungan. Dalam lingkungan seperti ini, terdapat berbagai risiko yang mengancam terjaganya kerahasiaan, integritas dan ketersediaan informasi. Ancaman dapat berupa kebocoran data, sabotase, vandalisme, virus, *malware* dan *phishing*, *hacking*, *spoofing, ransomware* dan sebagainya.

Saat ini, ancaman-ancaman tersebut semakin meningkat, seiring dengan berkembangnya layanan-layanan berbasis elektronik dan *online*. Oleh karena itu aset-aset informasi yang penting milik Pemerintah Daerah harus dipastikan terlindungi dengan baik. Manajemen Keamanan Informasi SPBE digunakan sebagai acuan dalam rangka melindungi Aset Informasi Pemerintah Daerah dari berbagai bentuk ancaman baik dari dalam maupun dari luar, yang dilakukan secara sengaja maupun tidak sengaja. Pengamanan dan perlindungan ini diberikan untuk menjamin keamanan informasi secara optimal.

I.2. TUJUAN

Tujuan penerapan Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Kota Pontianak adalah:

a. Memastikan ketersediaan, terpeliharanya kerahasiaan dan integritas informasi Pemerintah Daerah, serta seluruh sumber daya informasi.
b. Membangun sistem pengamanan untuk melindungi aset informasi milik Pemerintah Daerah dari ancaman pencurian, penyalahgunaan, atau kerusakan.
c. Memastikan terlaksananya prinsip *non-repudiation* atas pihak-pihak yang terlibat dalam proses bisnis Pemerintah Daerah.
d. Memastikan kapabilitas Pemerintah Daerah untuk melanjutkan operasional/layanannya apabila terjadi insiden keamanan informasi.
e. Mendorong Perangkat Daerah dan seluruh ASN Pemerinta Daerah untuk memiliki tingkat kesadaran (*awareness*), pengetahuan dan keterampilan yang memadai agar dapat memenuhi kewajiban mereka dalam menjaga keamanan aset informasi.
f. Memastikan kepatuhan terhadap hukum, undang-undang dan peraturan yang berlaku.

I.3. PRINSIP

Penyelengaraan Manajemen Keamanan Informasi SPBE dilaksanakan dengan prinsip sebagai berikut:

a. Prinsip Kerahasiaan
   Kemampuan akses dan modifikasi informasi diberikan hanya kepada pihak yang berwenang untuk tujuan yang jelas.
b. Prinsip Keutuhan Integritas
   Informasi yang digunakan pengguna bisa dipercaya kebenarannya merefleksikan realitas sebenarnya, terutama informasi strategis.
c. Perinsip Ketersediaan
   Informasi tersedia untuk mendukung organisasi dalam rentang waktu yangdisepakati bersama dan sesuai dengan peraturan yang ada sesuai tujuan organisasi
d. Prinsip Akuntabilitas
   Tanggung jawab pemilik, penyedia dan pengguna sistem informasi dan pihak lain yang terkait dengan keamanan informasi harus dideskripsikan dengan jelas
e. Prinsip Integrasi
   Kebijakan, pedoman, prosedur, ukuran dan praktek untuk keamanan informasi harus dikoordinasikan dan diintegrasikan antara satu dengan yang lain.
f. Prinsip Kesadaran
   Pemilik, penyedia, pengguna sistem informasi dan pihak lain yang terkait memiliki pemahaman dan informasi yang cukup mengenai kebijakan, pedoman, prosedur, ukuran, praktek keamanan informasi.
g. Prinsip Berkelanjutan
   Keamanan informasi harus diterapkan dan diperbaiki terus menerus sesuai dengan perkembangan kebutuhan organisasi, risiko dan teknologi.

I.4. RUANG LINGKUP

Sistem Manajemen Keamanan Informasi SPBE memuat kebijakan dan standar keamanan informasi yang akan menjadi acuan dalam kebijakan spesifik, pedoman, prosedur, *risk assessment* maupun proses keamanan informasi lainnya.

Kebijakan spesifik akan digunakan oleh bagian teknis dalam menyelesaikan tanggung jawab keamanan informasi. Pedoman dan prosedur digunakan untuk mengimplementasikan kebijakan yang telah ditetapkan dan sifatnya anjuran, berbeda dengan kebijakan yang sifatnya keharusan.

Kebijakan dan Standar Manajemen Keamanan Informasi SPBE ini memiliki kesamaan tingkat dengan kebijakan di Pemerintah Kota Pontianak lainnya dan harus dipatuhi oleh seluruh Pegawai Pemerintah Daerah dan pegawai pihak ketiga (pegawai dari pihak vendor, konsultan atau tenaga kerja kontrak yang berhubungan dengan Pemerintah Daerah)) untuk pengelolaan pengamanan seluruh Aset Informasi Pemerintah Daerah dan dilaksanakan oleh pegawai Pemerintah Daerah dan seluruh pihak yang terikat kontrak kerja sama dengan Pemerintah Daerah meliputi:

a. Organisasi dan lokasi: meliputi seluruh unit kerja Pemerintah Daerah serta pihak eksternal lainnya yang menyediakan dan atau mendukung layanan Teknologi Informasi Pemerintah Daerah.
b. Informasi: mencakup semua jenis informasi yang dihasilkan atau diterima Pemerintah Daerah, tersimpan dalam media elektronik yang dikelola dengan Teknologi Informasi, dan informasi lainnya yang berhubungan dengan Sistem Informasi yang digunakan oleh Pemerintah Daerah, termasuk namun tidak terbatas pada dokumen mengenai topologi jaringan, data pegawai, surat-surat internal, laporan-laporan internal dan lain-lain.
c. Bisnis Proses: mencakup bisnis proses Keamanan TI, Perencanaan TI, Penanganan Keluhan TI, Pengembangan Aplikasi Inti, Pengembangan Aplikasi Pendukung, Pengembanan Data Manajemen, Quality Assurance, Manajemen Basis Data, Layanan TI, DC, Jaringan dan Infrastruktur.

Adapun Ruang lingkup Kebijakan dan Standar Manajemen Keamanan Informasi SPBE mencakup aspek-aspek sebagai berikut:

1. Pengendalian Umum
2. Pengendalian Organisasi Keamanan Informasi
3. Keamanan Sumber Daya Manusia
4. Pengendalian Pengelolaan Aset Informasi
5. Pengendalian Akses
6. Pengendalian Terhadap Penerapan Kriptografi
7. Pengendalian Pengelolaan Keamanan Fisik dan Lingkungan
8. Pengendalian Pengelolaan Keamanan Operasional
9. Pengendalian Keamanan Komunikasi
10. Pengendalian Keamanan Informasi dalam Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi
11. Pengendalian Hubungan Dengan Pihak Ketiga atau Penyedia Jasa/Barang
12. Pengendalian Pengelolaan Gangguan Keamanan Informasi
13. Pengendalian Aspek Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan
14. Pengendalian Kepatuhan

I.5. REFERENSI

Kebijakan dan Standar Sistem Manajemen Keamanan Informasi ini mengacu pada dokumen/regulasi berikut:

1. ISO/IEC 27001:2013 - *Information security management systems requirement*s.
2. ISO/IEC 27002:2013 - *Code of practice for information security management*.
3. Pedoman Manajemen Keamanan Informasi SPBE.
4. Metodologi Penilaian Resiko dan Penanganan Risiko.
5. Undang-Undang dan regulasi terkait Keamanan Informasi lainnya yang berlaku.

## BAB II
## PENGENDALIAN UMUM

II.1. TUJUAN

Kebijakan dan Standar pengendalian umum bertujuan untuk memberikan pedoman atau panduan umum untuk seluruh Perangkat Daerah di lingkungan Pemerintah Kota Pontianak dalam hal mengelola manajemen keamanan informasi secara terpadu, sehingga aset informasi yang dimiliki setiap Perangkat Daerah dapat terlindungi meliputi aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

II.2. RUANG LINGKUP

1. Kebijakan dan standar ini berlaku untuk pengelolaan pengamanan seluruh aset informasi di setiap Perangkat Daerah di lingkungan Pemerintah Kota Pontianak dan dilaksanakan oleh seluruh unit kerja, seluruh pegawai, baik sebagai pengguna maupun pengelola Teknologi Informasi dan Komunikasi di lingkungan Pemerintah Kota Pontianak. Juga berrlaku bagi pihak luar yang berhubungan dengan Pemerintah Kota Pontianak melalui akses fisik maupun lojik antara lain tamu, pihak ketiga maupun pegawai di lingkungan perusahaan yang menggunakan fasilitas Pemerintah Kota Pontianak.
2. Aset informasi adalah aset dalam bentuk klasifikasi data dan informasi yang dihasilkan atau diterima Pemerintah Daerah, tersimpan dalam media elektronik yang dikelola dengan Teknologi Informasi, dan informasi lainnya yang berhubungan dengan Sistem Informasi yang digunakan oleh Pemerintah Daerah.
3. Data atau dokumen meliputi data keuangan, data kepegawaian, data barang milik negara, dokumen perjanjian kerahasiaan/kontrak, kebijakan lembaga, prosedur operasional, rencana kelangsungan kegiatan (*business continuity plan*), dokumentasi sistem, manual pengguna, hasil audit, dan beberapa dokumen lainnya.
4. Perangkat lunak meliputi perangkat lunak aplikasi, perangkat lunak sistem, dan perangkat bantu pengembangan sistem dan utilitas.
5. Perangkat keras meliputi perangkat komputer, perangkat jaringan dan komunikasi, removable media, perangkat pendukung dan perangkat infrastruktur lainnya.
6. Bisnis Proses: mencakup bisnis proses Keamanan TI, Perencanaan TI, Penanganan Keluhan TI, Pengembangan Aplikasi Inti, Pengembangan Aplikasi Pendukung, Pengembanan Data Manajemen, *Quality Assurance*, Manajemen Basis Data, Layanan TI, DC, Jaringan dan Infrastruktur.

7. Aset tak berwujud (*intangible*) meliputi pengetahuan, pengalaman, keahlian, citra dan reputasi.

II.3. KEBIJAKAN

1. Perangkat Daerah bertanggung jawab untuk mengidentifikasikan persyaratan dan kebutuhan keamanan informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi di lingkungan kerjanya.
2. Perangkat Daerah bertanggung jawab mengatur pelaksanaan pengamanan dan perlindungan aset informasi di lingkungan kerjanya.
3. Perangkat Daerah bertanggung jawab melaksanakan pengamanan aset informasi di lingkungan kerjanya.
4. Setiap Perangkat Daerah bertanggung jawab meningkatkan pengetahuan, keterampilan dan kepedulian terhadap keamanan informasi pada seluruh pengguna di lingkungan kerjanya.
5. Setiap Perangkat Daerah menerapkan manajemen risiko keamanan informasi yang setidaknya mencakup kajian terhadap pemenuhan persyaratan dan kebutuhan keamanan informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi di lingkungan kerjanya.
6. Setiap Perangkat Daerah melakukan audit internal Manajemen Keamanan Informasi SPBE secara berkala untuk memastikan pengendalian, proses dan prosedur Manajemen Keamanan Informasi SPBE dilaksanakan secara efektif sesuai dengan Kebijakan dan Standar Manajemen Keamanan Informasi SPBE yang telah ditetapkan dan dipelihara dengan baik.
7. Kepala Perangkat Daerah secara berkala melakukan evaluasi terhadap kepatuhan dan keefektifan pelaksanaan Manajemen Keamanan Informasi SPBE serta melakukan tindak lanjut yang diperlukan untuk secara berkesinambungan meningkatkan kepatuhan dan keefektifan implementasi Manajemen Keamanan Informasi SPBE di lingkungan kerjanya.
8. Kepala Perangkat Daerah tidak bertanggung jawab atas kerugian atau kerusakan data maupun perangkat lunak milik pihak ketiga yang diakibatkan dari upaya untuk melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi.

II.4. STANDAR

1. Sasaran keamanan informasi setidaknya mencakup kriteria berikut ini:
   a. Terukur.
   b. Mencakup derajat pencapaian persyaratan dan kebutuhan keamanan informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi di setiap Perangkat Daerah.
   c. Mencakup derajat kepatuhan dan keefektifan implementasi Manajemen Keamanan Informasi SPBE terhadap Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di setiap Perangkat Daerah yang telah ditetapkan.
2. Standar manajemen risiko keamanan informasi mengikuti ketentuan mengenai Penerapan Manajemen Risiko di setiap Perangkat Daerah.

3. Standar Catatan Penerapan Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di setiap Perangkat Daerah di lingkungan Pemerintah Kota Pontianak adalah sebagai berikut:
   a. Kepala Perangkat Daerah harus memastikan terdokumentasinya catatan penerapan Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di lingkungan kerjanya, sehingga kepatuhan dan efektivitas penerapan Manajemen Keamanan Informasi SPBE dapat diukur.
   b. Catatan penerapan Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di setiap Perangkat Daerah setidaknya meliputi:
      (1) Formulir-formulir sesuai prosedur operasional yang dijalankan.
      (2) Catatan gangguan keamanan informasi.
      (3) Catatan dari sistem.
      (4) Catatan pengunjung di area terbatas.
      (5) Kontrak dan perjanjian layanan.
      (6) Perjanjian kerahasiaan *(confidentiality agreements)*.
      (7) Laporan audit.
4. Dokumen pendukung kebijakan keamanan informasi setidaknya memuat informasi-informasi sebagai berikut:
   a. Tujuan dan ruang lingkup dokumen pendukung kebijakan keamanan informasi.
   b. Kerangka kerja setiap tujuan/sasaran pengendalian keamanan informasi.
   c. Metodologi penilaian risiko *(risk assessment)*.
   d. Penjelasan singkat mengenai standar, prosedur dan kepatuhan termasuk persyaratan peraturan yang harus dipenuhi, pengelolaan kelangsungan kegiatan, konsekuensi apabila terjadi pelanggaran.
   e. Tanggung jawab dari setiap bagian terkait.
   f. Dokumen referensi yang digunakan dalam menyusun dokumen pendukung kebijakan keamanan informasi.
5. Standar pengendalian dokumentasi Manajemen Keamanan Informasi SPBE adalah sebagai berikut:
   a. Setiap Kepala Perangkat Daerah harus mengendalikan dokumen Manajemen Keamanan Informasi SPBE untuk menjaga kemutakhiran dokumen, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan, dan mencegah akses oleh pihak yang tidak berwenang.
   b. Setiap Kepala Perangkat Daerah harus menempatkan dokumen Manajemen Keamanan Informasi SPBE di semua area operasional sehingga mudah diakses oleh pengguna di unit kerja masing-masing sesuai peruntukannya.
6. Audit internal Manajemen Keamanan Informasi SPBE dilaksanakan setidaknya satu kali dalam dua tahun oleh Inspektorat.
7. Evaluasi kepatuhan dan implementasi Manajemen Keamanan Informasi SPBE setidaknya mencakup hal-hal sebagai berikut:
   a. Evaluasi terhadap hasil audit internal Manajemen Keamanan Informasi SPBE.
   b. Evaluasi terhadap pencapaian Sasaran Keamanan Informasi *(information security objective)*.
   c. Evaluasi terhadap pencapaian persyaratan dan kebutuhan persyaratan dan kebutuhan keamanan informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi di lingkungan Diskominfo Kota Pontianak.
   d. Evaluasi terhadap umpan balik dari pihak-pihak di luar Diskominfo Kota Pontianak.

e. Evaluasi dari penerapan manajemen risiko Manajemen Keamanan Informasi SPBE.
f. Evaluasi terhadap kemungkinan-kemungkinan untuk peningkatan kinerja Manajemen Keamanan Informasi SPBE.

8. Peningkatan berkelanjutan
   a. Peningkatan kinerja manajemen layanan teknologi informasi secara berkelanjutan dikoordinasikan melalui:
      (1) Pengembangan proses manajemen keamanan informasi agar dapat menyesuaikan dengan *best practices* yang didefinisikan dalam ISO 27001.
      (2) Pengkajian tingkat keamanan informasi secara berkala untuk melihat kesesuaiannya dengan kondisi terkini.
      (3) Sarana perbaikan dari pengguna keamanan informasi yang didokumentasikan dalam *Security Improvement Program* (SIP).
      (4) Pengkajian SIP secara berkala untuk memastikan tindak lanjut dari pelaksanaan peningkatan keamanan informasi yang telah direncanakan.
      (5) Perumusan rencana peningkatan terhadap keamanan informasi berdasarkan hasil evaluasi yang telah dilakukan.
      (6) Pencapaian dan pemeliharaan sertifikasi manajemen keamanan informasi berdasarkan standar ISO 27001.
   b. Kriteria peningkatan kinerja manajemen layanan teknologi informasi antara lain berdasakan :
      (1) Pengembangan proses bisnis.
      (2) Hasil ketidaksesuaian dari gangguan/insiden, proses perubahan dan lain-lain.
      (3) Hasil audit internal dan/atau eksternal.
      (4) Hasil Tinjauan Manajemen.
      (5) Hasil ketidaksesuaian dari inspeksi atau temuan dari *stakeholders* lain.

## BAB III
## PENGENDALIAN ORGANISASI KEAMANAN INFORMASI

### III.1. TUJUAN

Pengendalian organisasi keamanan informasi bertujuan memberikan pedoman dalam membentuk organisasi fungsional keamanan informasi yang bertanggung jawab untuk mengelola keamanan informasi dan perangkat pengolah informasi di lingkungan kerja setiap Perangkat Daerah termasuk hubungan dengan pihak luar.

### III.2. RUANG LINGKUP

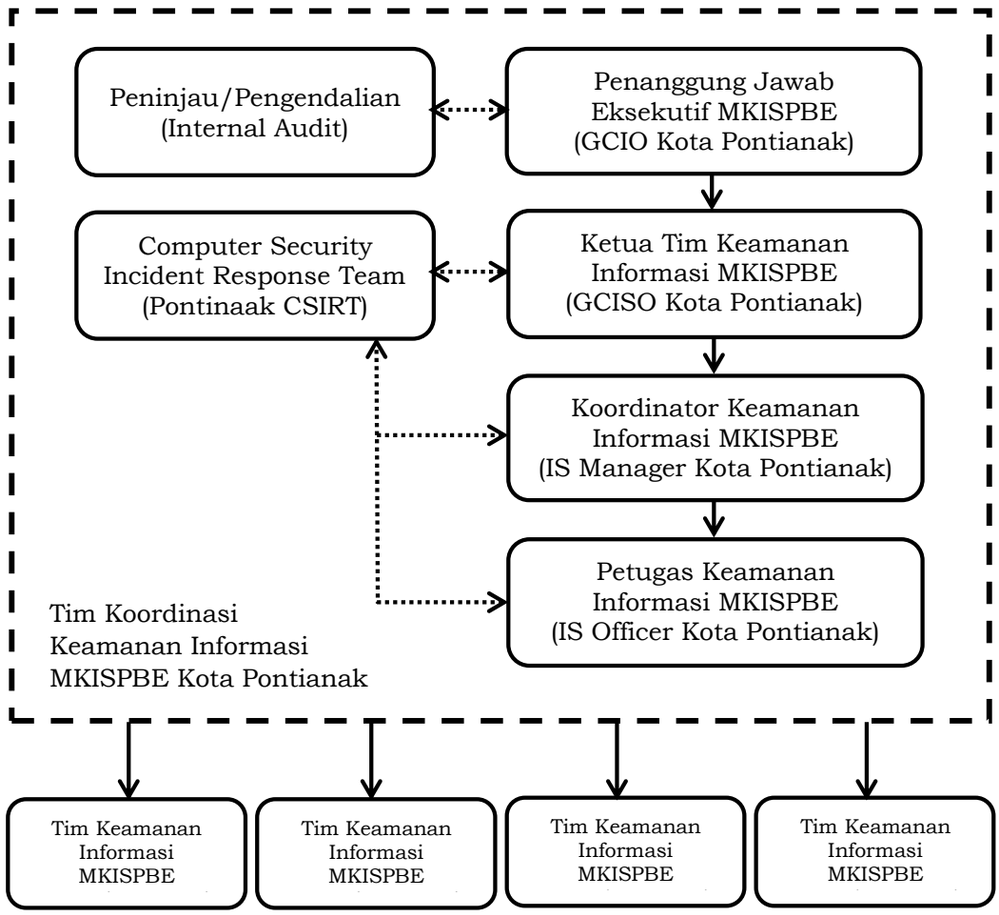
Kebijakan dan standar organisasi keamanan informasi meliputi:
1. Struktur Tim Keamanan Informasi di setiap Perangkat Daerah.
2. Perjanjian kerahasiaan.
3. Pemisahan tugas.
4. Hubungan dengan pihak berwenang, komunitas keamanan informasi, dan pihak ketiga.
5. Keamanan informasi pada pengelolaan proyek.
6. Pengendalian terhadap *mobile device* dan *teleworking*.

III.3. KEBIJAKAN

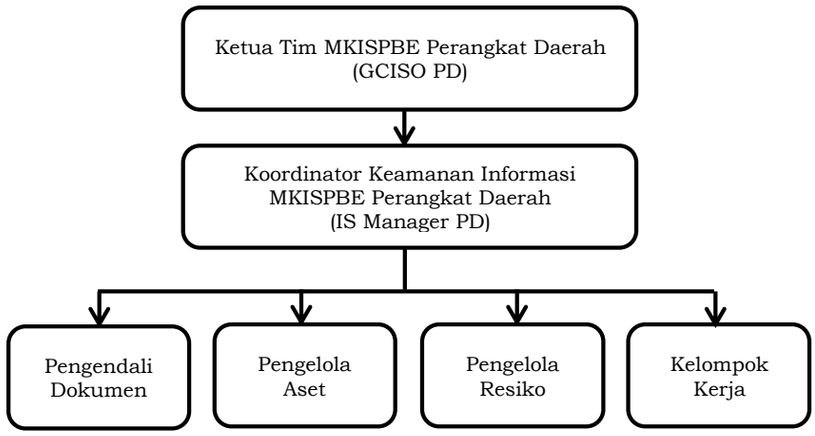
1. Struktur Tim Keamanan lnformasi setiap perangkat daerah berikut tanggung jawab dan wewenangnya diuraikan dalam standar organisasi keamanan informasi.
2. Tanggung jawab dan wewenang Tim Keamanan Informasi di setiap perangkat daerah dapat dipetakan dalam jabatan struktural dan/atau diperankan oleh Pejabat struktural dan/atau Pejabat fungsional.
3. Perjanjian Kerahasiaan
   Setiap Kepala Perangkat Daerah mengidentifikasi dan mengkaji secara berkala persyaratan untuk menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen perjanjian kerahasiaan.
4. Pemisahan tugas
   Setiap Kepala Perangkat Daerah harus melakukan pemisahan tugas untuk proses yang melibatkan informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA untuk menghindari adanya Pegawai yang memiliki pengendalian eksklusif terhadap seluruh aset informasi dan perangkat pengolahnya.
5. Hubungan dengan Pihak Berwenang
   Setiap Kepala Perangkat Daerah mengidentifikasi dan menjalin kerjasama dengan pihak-pihak berwenang di luar perangkat daerah yang terkait dengan keamanan informasi.
6. Hubungan dengan Komunitas Keamanan Informasi
   Setiap Kepala Perangkat Daerah menjalin kerjasama dengan komunitas keamanan informasi di luar Kepala Perangkat Daerah melalui pelatihan, seminar, atau forum lain yang relevan dengan keamanan informasi.
7. Keamanan informasi pada pengelolaan proyek
   Pengendalian terhadap keamanan informasi harus diterapkan dalam pengelolaan proyek dan harus diaplikasikan pada seluruh fase dalam metodologi pengelolaan proyek.
8. Pengendalian terhadap *mobile device* dan *teleworking*
   a. Setiap Kepala Perangkat Daerah membangun kepedulian pengguna perangkat *mobile device* dan *teleworking* akan risiko-risiko keamanan yang terus meningkat terhadap informasi yang tersimpan dalam perangkat *mobile device*.
   b. Pengguna perangkat *mobile device* dan *teleworking* harus mengikuti prosedur yang terkait penggunaan perangkat mobile device dan teleworking untuk menjaga keamanan perangkat dan informasi di dalamnya.

III.4. STANDAR

1. Tim Keamanan Informasi
   a. Struktur Tim Keamanan Informasi Manajemen Keamanan Informasi SPBE Pemerintah Kota Pontianak




   b. Struktur Tim Keamanan Informasi Manajemen Keamanan Informasi SPBE Perangkat Daerah




   c. Tugas dan Tanggung jawab Tim Keamanan Informasi Manajemen Keamanan Informasi SPBE Pemerintah Kota Pontianak.
      (1) Penanggung Jawab Eksekutif Manajemen Keamanan Informasi SPBE Kota Pontianak (*Goverment Chief Information Officer/GCIO* Kota Pontianak)
      Dijabat oleh Sekretaris Daerah, memiliki tugas:

- Mengkoordinir penyusunan kebijakan keamanan, sistem, dan prosedur keamanan informasi yang berlaku di lingkungan pemerintah Kota Pontianak.
- Menjamin ketersediaan, keakuratan, ketepatan, dan keamanan informasi yang dibutuhkan oleh Pemerintah Kota Pontianak dan stakeholder.
- Menetapkan pembagian tugas dan tanggung jawab untuk pengambilan keputusan terkait manajemen risiko keamanan informasi.
- Memastikan tersedianya sumber daya dalam pelaksanaan Manajemen Keamanan Informasi SPBE.

(2) Ketua Tim Keamanan Informasi Manajemen Keamanan Informasi SPBE Kota Pontianak (*Goverment Chief Information Security Officer/ GCISO* Kota Pontianak)
Dijabat oleh Kepala Perangkat Daerah yang menyelenggarakan tugas dan fungsi di bidang persandian, memiliki tugas:
- Menjadi koordinator perencanaan, pengembangan, implementasi, pengoperasian, monitoring, pemeliharaan dan peningkatan tata kelola keamanan informasi.
- Melakukan peninjauan manajemen atas kebijakan keamanan informasi secara berkala.
- Menyampaikan usulan revisi kebijakan keamanan informasi, untuk selanjutnya dibahas oleh Tim Koordinasi Manajemen Keamanan Informasi SPBE sebelum mendapat persetujuan dan pengesahan Wali Kota.
- Memberikan masukan atas sanksi yang akan diberikan kepada setiap pelanggaran keamanan informasi.
- Melakukan publikasi dan sosialiasi kendali risiko keamanan informasi kepada Staf Ahli, Inspektorat, Dinas Daerah, Badan Daerah, Kecamatan/ Kelurahan dan pihak eksternal Pemerintah Kota Pontianak.
- Memberikan masukan dan melakukan koordinasi dengan GCIO dalam pengelolaan akses aset informasi Pemerintah Kota Pontianak.

(3) Koordinator Keamanan Informasi Manajemen Keamanan Informasi SPBE Kota Pontianak (*Information Security Manager/ IS Manager* Kota Pontianak)
Dijabat oleh Pejabat Administrator atau Pejabaat Fungsional yang setara yang membawahi bidang tugas dan fungsi di bidang persandian
- Mendefinisikan standar teknis dan non teknis, prosedur, dan panduan keamanan informasi.
- Membantu Inspektorat dan GCISO dalam mendefinisikan dan mengimplementasikan kendali, proses, dan perangkat-perangkat pendukung supaya mematuhi kebijakan dan mengelola resiko keamanan informasi.
- Mereviu dan memonitor kepatuhan terhadap kebijakan dan berkontribusi pada proses audit internal dan C*ontrol Self Assesment* (CSA).
- Mengumpulkan, menganalisa, dan memberikan saran terkait metrik keamanan informasi dan insiden.
- Mendukung Inspektorat dalam melakukan penyelidikan dan remediasi insiden keamanan informasi atau pelanggaran kebijakan lainnya.

- Mengorganisasi kampanye kesadaran keamanan untuk pegawai Pemerintah Kota Pontianak dalam meningkatkan budaya keamanan dan mengembangkan pemahaman yang luas akan persyaratan ISO/IEC 27001.
- Mengordinasi implementasi kebijakan keamanan informasi selain keamanan fasilitas fisik.
- Memastikan keberadaan dan implementasi kendali teknis, fisik, dan prosedural. Salah satunya dengan memastikan kendali diterapkan dengan tepat oleh seluruh Pegawai Pemerintah Kota Pontianak. Manajer Keamanan Informasi memastikan:
  - Pegawai Pemerintah Kota Pontianak diinformasikan kewajibankewajibannya untuk melaksanakan kebijakan keamanan informasi.
  - Pegawai Pemerintah Kota Pontianak mematuhi kebijakan keamanan informasi dan mendukung secara aktif kendali-kendali kendali keamanan informasi tersebut.
  - Pegawai Pemerintah Kota Pontianak dimonitor untuk menilai tingkat kapatuhan terhadap kebijakan keamanan informasi dan menilai penerapan kendali-kendali keamanan informasi tersebut.
- Memberikan arahan, dukungan dan alokasi sumber daya dalam rangka memastikan perlindungan secara tepat aset-aset informasi.
- Menginformasikan GCISO dan GCIO dan/atau Inspektorat jika ada pelanggaran kebijakan (pelanggaran yang sudah terjadi atau pelanggaran yang baru dicurigai dan berpengaruh terhadap aset pihak terkait).
- Melakukan evaluasi kepatuhan terhadap kebijakan melalui proses *Control Self-Assessment* (CSA) dan audit internal secara periodik.

(4) Petugas Keamanan Informasi Manajemen Keamanan Informasi SPBE Kota Pontianak (*Information Security Officer/ IS Officer* Kota Pontianak)

Dikoordinir oleh Pejabat Pengawas atau Pejabat Fungsional yang setara yang memiliki tugas dan fungsi di bidang persandian, didukung oleh tenaga teknis keamanan informasi, bertugas

- Melaksanakan dan mengawasi penerapan Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Kota Pontianak.
- Memberi masukan untuk peningkatan penerapan Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Kota Pontianak.
- Mendefinisikan kebutuhan, merekomendasikan dan mengupayakan penyelenggaraan Pendidikan dan pelatihan keamaan informasi bagi seluruh pegawai.
- Memantau, mencatat dan menguraikan secara jelas gangguan keamanan informasi yang diketahui atau laporan yang diterima dan menindaklanjuti laporan tersebut sesuai prosedur pelaporan gangguan keamanan informasi dengan berkoodinasi bersama CSIRT.
- Memberi panduan dan/atau bantuan penyelesaian masalah-masalah keamanan informasi.

(5) Peninjau/Pengendalian Manajemen Keamanan Informasi SPBE (Internal Audit)
Ditugaskan kepada Inspektorat untuk bertanggung jawab:
- Menyusun dan memantau program dan jadwal audit Manajemen Keamanan Informasi SPBE
- Mengkoordinasikan pelaksanaan proses audit internal Manajemen Keamanan Informasi SPBE.
- Melakukan peninjauan independen atas tata kelola Manajemen Keamanan Informasi SPBE pada Perangkat Daerah di lingkungan Pemerintah Kota Pontianak. Mencakup peninjauan implementasi kebijakan, pedoman dan prosedur keamanan informasi untuk menjamin efektivitasnya.
- Merangkum dan melaporkan hasil audit internal Manajemen Keamanan Informasi SPBE kepada GCIO dan Wali Kota.
- Memberikan rekomendasi terkait kontrol keamanan informasi yang diperlukan untuk meningkatkan efektifitas Manajemen Keamanan Informasi SPBE.
- Mengkoordinasikan proses verifikasi tindakan lanjut perbaikan dan pencegahan terhadap ketidaksesuaian yang ditemukan dalam proses audit internal maupun eksternal Manajemen Keamanan Informasi SPBE.

(6) *Computer Security Incident Response Team* (CSIRT)
Dibentuk melalui Keputusan Wali Kota, memiliki wewenang sebagai berikut:
- melakukan pencegahan terjadinya insiden siber dengan cara terlibat aktif pada penilaian dan deteksi ancaman, perencanaan mitigasi, penyusunan pedoman keamanan Sistem Elektronik dan data elektronik serta pemberian peringatan terkait keamanan siber.
- memantau dan memonitor keamanan serta melindungi seluruh Sistem Elektronik atau data elektronik.
- menanggapi, menyelidiki dan menangani secara komprehensif serta melakukan pemulihan atas insiden keamanan siber yang menimpa Sistem Elektronik.
- melakukan evaluasi internal kinerja penyelenggaraan Teknologi Informasi.
- melakukan edukasi dan pelatihan keamanan siber bagi seluruh Pegawai di lingkungan Pemerintah Daerah.

Susunan Organisasi CSIRT adalah sebagai berikut
- Ketua
  Dijabat oleh Kepala Perangkat Daerah yang menyelenggarakan tugas dan fungsi di bidang persandian.
- Sekretaris
  Dijabat oleh Pejabat Administrator atau Pejabat Fungsional yang setara yang memiliki tugas dan fungsi dibidang pesandian.
- Koodinator
  Dijabat oleh Pejabat Pengawas atau Pejabat Fungsional yang setara yang memiliki tugas dan fungsi dibidang persandian.
- Kelompok Kerja Pengelola Jaringan dan Server
  Terdiri dari Pengendali Teknis dan didukung oleh anggota teknis.

- Kelompok Kerja Keamanan Sistem Informasi
  Terdiri dari Pengendali Teknis dan didukung oleh anggota teknis.
- Agen Siber
  Aparatur Sipil Negara penyelenggara sistem elektronik pada masing-masing Perangkat Daerah di lingkungan Pemerintah Kota Pontianak.

d. Tugas dan tanggung jawab Tim Keamanan Informasi Manajemen Keamanan Informasi SPBE Perangkat Daerah.
   (1) Ketua Tim Keamanan Informasi Manajemen Keamanan Informasi SPBE Perangkat Daerah (*Goverment Chief Information Security Officer/ GCISO Perangkat Daerah*)
   Dijabat oleh masing-masing Kepala Perangkat Daerah di lingkungan Pemerintah Kota Pontianak, memiliki tugas:
   - Memelihara dan mengendalikan penerapan Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di lingkungan Perangkat Daerah.
   - Menjadi koordinator perencanaan, pengembangan, implementasi, pengoperasian, monitoring, pemeliharaan dan peningkatan tata kelola keamanan informasi di Perangkat Daerah.
   - Mengukur efektifikats dan konsistensi penerapan kebijakan dna standar Manajemen Keamanan Informasi SPBE di lingkungan Perangkat Daerah.
   - Menyampaikan masukan peningktan penerapan Kebijakan dan Standar Manajemen Keamanan Informasi SPBE serta usulan revisi kebijakan keamanan informasi, untuk selanjutnya dibahas Tim Koordinasi Manajemen Keamanan Informasi SPBE Kota Pontianak sebelum mendapat persetujuan dan pengesahan Wali Kota.
   - Memrintahkan penutupan akses Sistem Elektronik yang terdampak insiden untuk mencegah dampak insiden meluas berdasarkan rekomendasi dari *Computer Security Incident Response Team.*

   (2) Koordinator Keamanan Informasi Manajemen Keamanan Informasi SPBE Perangkat Daerah (*Information Security Manager/ IS Manager* Perangkat Daerah)
   Ditunjuk oleh masing-masing Kepala Perangkat Daerah di lingkungan Pemerintah Kota Pontianak, memiliki tugas:
   - Memastikan Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di Perangkat Daerah diterapkan secara efektif.
   - Memastikan langkah-langkah perbaikan sudah dlakukan berdasarkan evaluasi dan/atau audit internal.
   - Memastian peningkatan kesadaran, kepedualian dan kepatuhan seluruh pegawai di Perangkat Daerah terhadap Kebijakan dan Standar Manajemen Keamanan Informasi SPBE.
   - Melakukan evaluasi, pengendalian dan melaporkan kinerja penerapan Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di lingkungan Perangkat Daerah sesuai lingkup tanggung jawabnya kepada *GCISO* Perangkat Daerah sebagai basis peningkatan lebih lanjut.

- Mengkoordinasikan penanganan gangguan keamanan informasi di lingkup Perangkat Daerah dan menginformasikannya kepada CSIRT Kota Pontianak.
- Memastikan terlaksananya audit internal terhadap penerapan Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di Perangkat Daerah.

(3) Pengendali Dokumen
- Memelihara '*Master List*' dokumen Manajemen Keamanan Informasi SPBE berupa Kebijakan Keamanan Informasi, Standar Sistem Manajemen Keamanan Informasi, Standar Penilaian Risiko Manajemen Keamanan Informasi SPBE, Prosedur, Formulir yang digunakan serta Standar lain yang digunakan.
- Memastikan seluruh dokumen Manajemen Keamanan Informasi SPBE serta turunannya didistribusikan ke personil yang berwenang.
- Mengelola pengadministrasian seluruh dokumen, pengesahan, registrasi, penarikan, dan pemusnahan dokumen.
- Melakukan inventarisasi untuk setiap kegiatan Audit Internal/Eksternal, Hasil Laporan Temuan Audit Internal/Eksternal, Risalah Rapat Tinjauan Manajemen.

(4) Pengelola Aset
- Mengelola data inventaris aset pemroses dan penyimpan informasi yang digunakan dalam pelaksanaan pekerjaan di setiap Perangkat Daerah.
- Mendokumentasikan setiap penambahan, permohonan, perpindahan, peminjaman, pengembalian, perbaikan, dan penghapusan terkait aset pemroses informasi.

(5) Pengelola Risiko
- Melaksanakan *Risk Assessment* terkait dengan Manajemen Keamanan Informasi SPBE.
- Melakukan pemantauan terhadap risiko keamanan informasi yang baru di organisasi, baik dari pihak internal maupun eksternal.
- Melakukan pengkinian terhadap daftar risiko (*risk register*).

(6) Kelompok Kerja Manajemen Keamanan Informasi SPBE
- Melakukan monitoring pelaksanaan Manajemen Keamanan Informasi SPBE di masing-masing unit kerja.
- Memastikan bahwa semua prosedur, instruksi kerja dan formulir dapat digunakan dan diterapkan di unit kerja terkait untuk mengurangi terjadinya kesalahan dalam penerapan sistem manajemen.
- Memantau pengukuran sasaran implementasi Manajemen Keamanan Informasi SPBE pada masing-masing unit kerja.
- Melakukan tindak lanjut hasil temuan audit internal.
- Memberikan rekomendasi penutupan akses Sistem Elektronik yang terdampak insiden untuk mencegah dampak insiden meluas.

2. Perjanjian Kerahasiaan

Perjanjian kerahasiaan harus memuat unsur-unsur sebagai berikut:

a. Definisi dari informasi yang akan dilindungi.
b. Durasi yang diharapkan dari sebuah perjanjian kerahasiaan.

c. Tanggung jawab yang diharapkan dari sebuah perjanjian kerahasiaan.
b. Penanda-tangan untuk menghindari pengungkapan informasi secara tidak sah.
c. Perlindungan kepemilikan informasi, rahasia organisasi, dan kekayaan intelektual.
d. Izin menggunakan informasi rahasia, dan hak-hak penanda-tangan untuk menggunakan informasi.
e. Hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia.
f. Proses untuk pemberitahuan dan pelaporan dari penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan informasi.
g. Tindakan yang diperlukan pada saat sebuah perjanjian kerahasiaan diakhiri.
h. Syarat-syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian.
i. Tindakan yang akan diambil apabila terjadi pelanggaran terhadap perjanjian ini.

## BAB IV
## KEAMANAN SUMBER DAYA MANUSIA

### IV.1. TUJUAN

Keamanan sumber daya manusia bertujuan memastikan bahwa seluruh pegawai dan pihak ketiga di setiap Perangkat Daerah memahami tanggung jawabnya masing-masing, sadar atas ancaman Keamanan Informasi, serta mengetahui proses terkait Keamanan Informasi sebelum, selama, dan setelah bertugas.

### IV.2. RUANG LINGKUP

Kebijakan dan standar keamanan sumber daya manusia ini mencakup peran dan tanggung jawab seluruh pegawai dan pihak ketiga di setiap Perangkat Daerah yang harus dipahami dan dilaksanakan. Peran dan tanggung jawab pegawai juga mengacu pada ketentuan peraturan perundang- undangan lainnya yang berlaku.

### IV.3. KEBIJAKAN

1. Seluruh pegawai bertanggung jawab untuk menjaga Keamanan Informasi di setiap Perangkat Daerah sesuai dengan tugas dan fungsinya.
2. Pihak ketiga harus menyetujui dan menandatangani syarat dan perjanjian untuk menjaga keamanan informasi di setiap Perangkat Daerah.
3. Peran dan tanggung jawab pegawai dan pihak ketiga terhadap keamanan informasi didefinisikan, didokumentasikan, dan dikomunikasikan kepada yang bersangkutan.
4. Pimpinan Perangkat Daerah akan melakukan pemeriksaan data pribadi yang diberikan oleh pegawai dan pihak ketiga sesuai dengan ketentuan peraturan perundang-undangan.

5. Seluruh Aparatur Sipil Negara harus mendapatkan pendidikan, pelatihan, dan sosialisasi keamanan informasi secara berkala sesuai tingkat tanggung jawabnya.
6. Pihak ketiga, jika diperlukan, mendapatkan sosialisasi untuk meningkatkan kepedulian terhadap keamanan informasi.
7. Seluruh pegawai dan pihak ketiga yang melanggar Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di Lingkungan Pemerintah Kota Pontianak dikenai sanksi atau tindakan disiplin sesuai ketentuan peraturan perundang-undangan.
8. Kepatuhan pegawai terhadap Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di setiap Perangkat Daerah harus dievaluasi secara berkala oleh atasan masing-masing dan menjadi bagian dari penilaian kinerja pegawai.
9. Pimpinan Perangkat Daerah harus menghentikan hak penggunaan Aset Informasi bagi pegawai yang sedang menjalani pemeriksaan yang terkait dengan dugaan adanya pelanggaran Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di setiap Perangkat Daerah dan/atau yang sedang menjalani proses hukum.
10. Pimpinan Perangkat Daerah harus mencabut hak akses terhadap Aset Informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi bekerja di Perangkat Daerah tersebut.

IV.4. STANDAR

Keamanan Sumber Daya Manusia meliputi:

1. Peran dan tanggung jawab pegawai di setiap Perangkat Daerah terhadap keamanan informasi harus menjadi bagian dari penjabaran tugas dan fungsi, khususnya bagi yang memiliki akses terhadap Aset Informasi.
2. Pimpinan dari pegawai berkeahlian khusus atau yang berada di posisi kunci (*key person*) harus memastikan ketersediaan pengganti pegawai tersebut dengan kompetensi yang setara apabila pegawai yang bersangkutan mutasi/berhenti.
3. Peran dan tanggung jawab pegawai terhadap Keamanan Informasi harus menyertakan persyaratan untuk:
   a. melaksanakan dan bertindak sesuai dengan organisasi keamanan informasi;
   b. melindungi aset dari akses yang tidak sah, penyingkapan, modifikasi, kerusakan atau gangguan;
   c. melaksanakan proses keamanan atau kegiatan keamanan informasi sesuai dengan peran dan tanggung jawabnya; dan
   d. melaporkan kejadian, potensi kejadian, atau risiko keamanan informasi sesuai dengan Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di setiap Perangkat Daerah.
4. Pemeriksaan latar belakang calon pegawai dan pihak ketiga setiap Perangkat Daerah harus memperhitungkan privasi, perlindungan data pribadi dan/atau pekerjaan berdasarkan undang-undang, meliputi:
   a. ketersediaan referensi, dari referensi hubungan kerja dan referensi pribadi;
   b. pemeriksaan kelengkapan dan ketepatan dari riwayat hidup pemohon;
   c. konfirmasi kualifikasi akademik dan profesional yang diklaim;
   b. pemeriksaan independen identitas (paspor atau dokumen yang sejenis); dan
   c. pemeriksaan lebih rinci, seperti pemeriksaan dari catatan kriminal.

# BAB V
# PENGENDALIAN PENGELOLAAN ASET INFORMASI

## V.1. TUJUAN

Pengendalian Pengelolaan Aset Informasi bertujuan memberikan pedoman dalam mengelola Aset Informasi di setiap Perangkat Daerah untuk melindungi dan menjamin keamanan Aset Informasi.

## V.2. RUANG LINGKUP

Kebijakan dan standar pengelolaan aset informasi ini meliputi:
1. tanggung jawab terhadap Aset Informasi.
2. pengklasifikasian Aset Informasi.
3. penanganan Aset Informasi.
4. penanganan media removable.
5. pengamanan penggunaan kembali, penghapusan atau pemusnahan perangkat.
6. pertukaran media informasi secara fisik.

## V.3. KEBIJAKAN

1. Tanggung Jawab terhadap Aset Informasi
   a. Pimpinan Perangkat Daerah mengidentifikasi Aset Informasi dan mendokumentasikannya dalam Daftar Inventaris Aset Informasi. Daftar Inventaris Aset Informasi dipelihara dan dikelola perubahannya oleh penanggung jawab Pengendalian Dokumen.
   b. Pimpinan Perangkat Daerah menetapkan Pemilik Aset Informasi.
   c. Pimpinan Perangkat Daerah menetapkan Aset Informasi yang terkait dengan perangkat pengolah informasi.
   d. Pemilik Aset Informasi menetapkan aturan penggunaan Aset Informasi.
   e. seluruh pegawai yang berhenti bekerja atau mutasi harus mengembalikan seluruh Aset Informasi yang dipergunakan selama bekerja sesuai dengan ketentuan.
   f. pihak ketiga yang habis masa kontrak kerjanya harus mengembalikan seluruh Aset Informasi yang dipergunakan selama bekerja di Perangkat Daerah yang bersangkutan.
2. Klasifikasi Aset Informasi
   a. Aset Informasi diklasifikasikan sesuai tingkat kerahasiaan, nilai, tingkat kritikalitas, serta aspek hukumnya.
   b. ketentuan rinci klasifikasi Aset Informasi diuraikan dalam standar pengelolaan Aset Informasi.
   c. pemberian label klasifikasi Aset Informasi harus dilakukan secara konsisten terhadap seluruh Aset Informasi.
3. Penanganan Aset Informasi
   Pimpinan Perangkat Daerah perlu menyusun dan menetapkan peraturan atau prosedur terkait penanganan Aset Informasi sesuai dengan klasifikasi informasi yang telah ditetapkan.
4. Penanganan Media *Removable*
   Pimpinan Perangkat Daerah perlu menyusun dan menetapkan peraturan atau prosedur terkait penanganan media removable sesuai dengan klasifikasi informasi yang telah ditetapkan.
5. Pengamanan penggunaan kembali atau penghapusan atau pemusnahan perangkat.

a. perangkat pengolah informasi penyimpan Data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dihapuskan atau dimusnahkan.
b. penanganan perangkat pengolah informasi penyimpan Data di setiap Perangkat Daerah sesuai dengan standar penanganan media penyimpan Data yang yang berlaku di Perangkat Daerah yang bersangkutan.

7. Pertukaran Media Informasi secara Fisik
   Pimpinan Perangkat Daerah perlu menyusun dan menetapkan peraturan terkait pertukaran informasi yang tidak menggunakan perangkat komunikasi elektronik misalnya melalui jasa pengantar media informasi melalui transportasi untuk melindungi informasi di dalam media terhadap akses yang tidak sah, penyalahgunaan dan kerusakan ketika pengiriman.

V.4. STANDAR

Pengelolaan Aset Informasi

1. Pemilik Aset Informasi menetapkan dan mengkaji secara berkala klasifikasi Aset Informasi dan jenis perlindungan keamanannya.
2. Pemilik Aset Informasi menetapkan pihak yang berwenang untuk mengakses Aset Informasi.
3. dalam pengelolaan Aset Informasi di setiap Perangkat Daerah, Aset Informasi diklasifikasikan sebagaimana berikut:

| KLASIFIKASI ASET | KETERANGAN |
|---|---|
| Sangat Rahasia (*Strictly Confidential*) | Informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menyebabkan kerugian negara. |
| Rahasia (*Confidential*) | Informasi yang apabila secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu citra dan reputasi yang menurut peraturan perundang-undangan dinyatakan rahasia. |
| Terbatas (*Internal*) | Informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yag tidak berhak akan mengganggu citra dan reputasi. |
| Publik | Informasi yang dihasilkan, disimpan, dikelola, dikirim dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan negara dan/atau penyelenggara dan penyelenggaraan badan publik lainya yang sesuai dengan undang-undang serta informasi lain yang berkaitan dengan kepentingan publik. |

# BAB VI
# PENGENDALIAN AKSES

## VI.1. TUJUAN

Pengendalian akses bertujuan untuk memastikan otorisasi akses Pengguna dan mencegah akses pihak yang tidak berwenang terhadap Aset Informasi khususnya perangkat pengolah informasi.

## VI.2. RUANG LINGKUP

Kebijakan dan standar pengendalian akses ini meliputi:
1. Persyaratan untuk pengendalian akses.
2. Pengelolaan akses pengguna.
3. Tanggung jawab pengguna.
4. Pengendalian akses jaringan.
6. Pengendalian akses ke sistem operasi.
7. Pengendalian akses ke aplikasi dan Sistem Informasi.

## VI.3. KEBIJAKAN

1. Persyaratan untuk Pengendalian Akses
   Setiap Perangkat Daerah harus menyusun, mendokumentasikan, dan mengkaji ketentuan akses ke Aset Informasi berdasarkan kebutuhan organisasi dan persyaratan keamanan.
2. Pengelolaan Akses Pengguna
   a. Pendaftaran Pengguna
      Setiap Perangkat Daerah harus menyusun prosedur pengelolaan hak akses Pengguna sesuai dengan peruntukannya.
   b. Pengelolaan Hak Akses Khusus
      Setiap Perangkat Daerah harus membatasi dan mengendalikan penggunaan Hak Akses Khusus.
   c. Pengelolaan Kata Sandi Pengguna
      (1) Pimpinan Perangkat Daerah harus mengatur pengelolaan Kata Sandi Pengguna.
      (2) Pengelolaan Kata Sandi Pengguna sesuai dengan standar yang berlaku di lingkungan Perangkat Daerah yang bersangkutan.
   d. Kajian hak akses pengguna
      Pimpinan Perangkat Daerah harus memantau dan mengevaluasi hak akses Pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya.
3. Tanggung Jawab Pengguna
   a. Pengguna harus mematuhi aturan pembuatan dan penggunaan Kata Sandi. Tanggung jawab pengguna terhadap Kata Sandi sesuai dengan standar tanggung jawab Pengguna yang berlaku di setiap Perangkat Daerah.
   b. Pengguna harus memastikan perangkat pengolah informasi yang digunakan mendapatkan perlindungan terutama pada saat ditinggalkan.
   c. Pengguna harus melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang.

4. Pengendalian Akses Jaringan
   a. Penggunaan layanan jaringan
      (1) Setiap Pimpinan Perangkat Daerah harus mengatur akses Pengguna dalam mengakses jaringan yang digunakan pada Perangkat Daerah yang bersangkutan sesuai dengan peruntukannya.
      (2) Setiap Pimpinan Perangkat Daerah harus mengatur akses Pengguna dalam mengakses internet. Akses Pengguna dalam mengakses internet sesuai dengan standar yang berlaku pada Perangkat Daerah yang bersangkutan.
   b. Otorisasi Pengguna untuk Koneksi Eksternal
      Setiap Perangkat Daerah harus menerapkan proses otorisasi Pengguna untuk setiap akses ke dalam jaringan internal melalui Koneksi Eksternal.
   c. Perlindungan terhadap diagnosa jarak jauh dan konfigurasi *port*
      (1) Akses ke Perangkat Keras dan Perangkat Lunak untuk diagnosa harus dikendalikan berdasarkan prosedur dan hanya digunakan oleh pegawai yang berwenang untuk melakukan pengujian, pemecahan masalah, dan pengembangan sistem.
      (2) *Port* pada Fasilitas jaringan yang tidak dibutuhkan dalam kegiatan atau fungsi layanan harus dinonaktifkan.
   d. Pemisahan dalam jaringan
      Setiap Perangkat Daerah harus memisahkan jaringan untuk pengguna, Sistem Informasi, dan layanan informasi.
   a. Pengendalian koneksi jaringan
      Setiap Perangkat Daerah harus menerapkan mekanisme pengendalian akses Pengguna sesuai dengan persyaratan pengendalian akses.
   b. Pengendalian routing jaringan
      Pengendalian routing jaringan internal di setiap Perangkat Daerah harus dilakukan sesuai pengendalian akses dan kebutuhan layanan informasi.
5. Pengendalian Akses ke Sistem Operasi
   a. Prosedur akses yang aman
      Akses ke sistem operasi harus dikontrol dengan menggunakan prosedur akses yang aman.
   b. Identifikasi dan otorisasi Pengguna
      (1) Setiap Pengguna harus memililki Akun yang unik dan hanya digunakan sesuai dengan peruntukannya.
      (2) Proses otorisasi Pengguna harus menggunakan teknik autentikasi yang sesuai untuk memvalidasi identitas dari pengguna.
   c. Sistem pengelolaan Kata Sandi
      Sistem pengelolaan Kata Sandi harus mudah digunakan dan dapat memastikan kualitas Kata Sandi yang dibuat pengguna.
   d. Penggunaan *system utilities*
      Setiap Perangkat Daerah harus membatasi dan mengendalikan penggunaan *system utilities*.
   e. *Session time-out*
      Fasilitas *session time-out* harus diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas Pengguna setelah periode tertentu.
   f. Pembatasan waktu koneksi
      Setiap Perangkat Daerah harus membatasi waktu koneksi untuk Sistem Informasi dan aplikasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA.

6. Pengendalian Akses ke Aplikasi dan Sistem Informasi
   a. Pimpinan Perangkat Daerah harus memastikan bahwa akses terhadap aplikasi dan sistem informasi hanya diberikan kepada pengguna sesuai peruntukannya.
   b. Aplikasi dan Sistem Informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus diletakkan pada lokasi terpisah untuk mengurangi kemungkinan diakses oleh pihak yang tidak berwenang.

VI.4. STANDAR

1. Persyaratan untuk Pengendalian Akses
   Persyaratan untuk pengendalian akses mencakup:
   a. Penentuan kebutuhan keamanan dari pengolah Aset Informasi.
   b. Pemisahan peran pengendalian akses, seperti administrasi akses dan otorisasi akses.
2. Pengelolaan Akses Pengguna
   Prosedur pengelolaan akses Pengguna harus mencakup:
   a. Penggunaan Akun yang unik untuk mengaktifkan Pengguna agar terhubung dengan Sistem Informasi atau layanan, dan Pengguna dapat bertanggung jawab dalam penggunaan Sistem Informasi atau layanan tersebut. Penggunaan Akun khusus hanya diperbolehkan sebatas yang diperlukan untuk kegiatan atau alasan operasional, dan harus disetujui Pejabat yang berwenang serta didokumentasikan.
   b. Pemeriksaan bahwa Pengguna memiliki otorisasi dari pemilik sistem untuk menggunakan Sistem Informasi atau layanan, dan jika diperlukan harus mendapat persetujuan yang terpisah dari Pejabat yang berwenang.
   c. Pemeriksaan bahwa tingkat akses yang diberikan sesuai dengan tujuan kegiatan dan konsisten dengan Kebijakan dan Standar Manajemen Keamanan Informasi SPBE di Lingkungan Perangkat Daerah yang bersangkutan.
   b. Pemberian pernyataan tertulis kepada Pengguna tentang hak aksesnya dan meminta Pengguna menandatangani pernyataan ketentuan akses tersebut.
   c. Pemastian penyedia layanan tidak memberikan akses kepada Pengguna sebelum prosedur otorisasi telah selesai.
   d. Pemeliharaan catatan Pengguna layanan yang terdaftar dalam menggunakan layanan.
   e. Penghapusan atau penonaktifan akses Pengguna yang telah berubah tugas dan/atau fungsinya, setelah penugasan berakhir atau mutasi.
   f. Pemeriksaan, penghapusan, serta penonaktifan Akun secara berkala dan untuk Pengguna yang memiliki lebih dari 1 (satu) akun.
   g. Pemastian bahwa Akun tidak digunakan oleh Pengguna lain yang tidak berhak.
3. Pengelolaan Hak Akses Khusus
   Pengelolaan Hak Akses Khusus harus mempertimbangkan:
   a. Hak Akses Khusus setiap sistem dari pabrikan perlu diidentifikasi untuk dialokasikan atau diberikan kepada Pengguna yang terkait dengan produk, seperti sistem operasi, sistem pengelolaan basis data, aplikasi.

b. Hak Akses Khusus hanya diberikan kepada Pengguna sesuai dengan peruntukkannya berdasarkan kebutuhan dan kegiatan tertentu.
c. Pengelolaan proses otorisasi dan catatan dari seluruh hak Akses Khusus yang dialokasikan atau diberikan kepada pengguna. Hak Akses Khusus tidak boleh diberikan sebelum proses otorisasi selesai.
d. Pengembangan dan penggunaan sistem rutin (misalnya: *job scheduling*) harus diutamakan untuk menghindari kebutuhan dalam memberikan Hak Akses Khusus secara terus-menerus kepada pengguna; dan
e. Hak Akses Khusus harus diberikan secara terpisah dari Akun yang digunakan untuk kegiatan umum, seperti Akun *system administrator, database administrator*, dan *network administrator*.

4. Kajian Hak Akses Pengguna
   Kajian hak akses Pengguna harus mempertimbangkan:
   a. Hak akses Pengguna harus dikaji paling sedikit 6 (enam) bulan sekali atau setelah terjadi perubahan pada sistem, atau struktur organisasi.
   b. Hak Akses Khusus harus dikaji paling sedikit 6 (enam) bulan sekali dalam jangka waktu lebih sering dibanding jangka waktu pengkajian hak akses pengguna, atau apabila terjadi perubahan pada sistem, atau struktur organisasi.
   c. Pemeriksaan Hak Akses Khusus harus dilakukan secara berkala, untuk memastikan pemberian Hak Akses Khusus telah diotorisasi.
5. Pengendalian Akses Jaringan
   a. Menerapkan prosedur otorisasi untuk pemberian akses kejaringan dan layanan jaringan.
   b. Menerapkan teknik autentikasi akses dari koneksi eksternal,seperti teknik kriptografi, *token hardware*, dan *dial-back*.
   c. Melakukan penghentian atau isolasi layanan jaringan pada area jaringan yang mengalami gangguan keamanan informasi.
6. Pemisahan dalam Jaringan
   Melakukan pemisahan dalam jaringan antara lain:
   a. Pemisahan berdasarkan kelompok layanan informasi, pengguna, dan aplikasi.
   b. Pemberian akses jaringan kepada tamu, hanya dapat diberikan akses terbatas misalnya internet dan/atau surat elektronik tanpa bisa terhubung ke jaringan internal Perangkat Daerah yang bersangkutan.

## BAB VII
## PENGENDALIAN TERHADAP PENERAPAN KRIPTOGRAFI

### VII.1. TUJUAN

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

### VII.2. RUANG LINGKUP

Kebijakan dan standar penerapan kriptografi ini meliputi:
1. Penentuan kondisi yang mengharuskan penerapan kriptografi.
2. Persyaratan penerapan kriptografi dan kunci kriptografi.

VII.3. KEBIJAKAN

1. Setiap Perangkat Daerah mengembangkan dan/atau menerapkan sistem kriptografi untuk perlindungan informasi dan membuat rekomendasi yang tepat bagi penerapannya.
2. Sistem kriptografi harus digunakan untuk melindungi aset informasi yang memiliki klasifikasi SANGAT RAHASIA, RAHASIA, dan TERBATAS.

VII.4. STANDAR

Pengembangan dan/atau penerapan sistem kriptografi untuk perlindungan informasi harus mempertimbangkan:

1. Kondisi dari suatu kegiatan yang menentukan bahwa informasi harus dilindungi, seperti risiko kegiatan, media pengiriman informasi, tingkat perlindungan yang dibutuhkan.
2. Kontrol kriptografi dapat mencakup namun tidak terbatas pada:
   a. Enkripsi informasi dan jaringan komunikasi.
   b. Pemeriksaan integritas informasi, seperti *hashing*.
   c. Otentikasi identitas.
   d. *Digital signatures*.
3. Pemilihan kontrol kriptografi harus mempertimbangkan:
   a. Jenis dari kontrol kriptografi;
   b. Kekuatan dari algoritma kriptografi; dan
   c. Panjang dari kunci kriptografi.
4. Tingkat perlindungan yang dibutuhkan harus diidentifikasi berdasarkan penilaian risiko, dengan mempertimbangkan jenis, kekuatan, dan kualitas dari algoritma enkripsi yang akan digunakan.
5. Keperluan enkripsi untuk perlindungan informasi SANGAT RAHASIA, RAHASIA dan TERBATAS yang melalui perangkat mobile computing, removable media, atau jalur komunikasi.
6. Kemudahan dan teknologi yang diperlukan dalam pengelolaan kunci kriptografi, seperti perlindungan kunci kriptografi, pemulihan informasi terenkripsi dalam hal kehilangan atau kerusakan kunci kriptografi.
7. Dampak penggunaan informasi terenkripsi, seperti pengendalian terkait pemeriksaan suatu konten, kecepatan pemrosesan pada sistem.
8. Implementasi dari kontrol kriptografi harus secara berkala ditinjau untuk memastikan kecukupan dan kesesuaian dari kontrol tersebut dalam mengamankan kerahasiaan dan integritas dari informasi.
9. Pengelolaan dari kunci kriptografi harus dikendalikan secara ketat dan dibatasi hanya pada personil yang terotorisasi.
10. Pengelolaan dari kunci kriptografi didasarkan pada prinsip *dual custody* untuk mengurangi risiko penyalahgunaan.

## BAB VIII
## PENGENDALIAN PENGELOLAAN KEAMANAN FISIK DAN LINGKUNGAN

VIII.1. TUJUAN

Pengendalian pengelolaan keamanan fisik dan lingkungan bertujuan untuk mencegah akses fisik oleh pihak yang tidak berwenang, menghindari terjadinya kerusakan, pencurian, persekongkolan terhadap aset dan informasi, serta gangguan lainnya pada perangkat pengolah informasi serta gangguan pada aktivitas organisasi.

VIII.2. RUANG LINGKUP

Kebijakan dan standar keamanan fisik dan lingkungan ini meliputi:
1. Pengamanan area.
2. Pengamanan perangkat.

VIII.3. KEBIJAKAN

1. Pengamanan Area
   a. Seluruh pegawai, pihak ketiga, dan tamu yang memasuki lingkungan Perangkat Daerah harus mematuhi aturan yang berlaku.
   b. Ketentuan rinci tentang pengamanan area lingkungan kerja di setiap Perangkat Daerah diuraikan dalam Kebijakan Keamanan Informasi pada Perangkat Daerah yang bersangkutan.
2. Pengamanan Perangkat
   a. Penempatan dan perlindungan perangkat
      Perangkat pengolah informasi dan perangkat pendukung harus ditempatkan di lokasi yang aman dan diposisikan sedemikian rupa untuk mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang.
   b. Penyediaan perangkat pendukung
      Perangkat pendukung harus dipasang untuk menjamin beroperasinya perangkat pengolah informasi dan secara berkala harus diperiksa dan diuji ulang kinerjanya.
   c. Pengamanan kabel
      (1) Kabel sumber daya listrik harus dilindungi dari kerusakan.
      (2) Kabel telekomunikasi yang mengalirkan informasi harus dilindungi dari kerusakan dan penyadapan.
   d. Pemeliharaan perangkat
      Perangkat harus dipelihara secara berkala untuk menjamin ketersediaan, keutuhannya, dan fungsinya.
   e. Pengamanan perangkat di luar lingkungan Perangkat Daerah.
      Penggunaan perangkat yang dibawa ke luar dari lingkungan setiap Perangkat Daerah harus disetujui oleh Pejabat yang berwenang.
   f. Pengamanan penggunaan kembali atau penghapusan atau pemusnahan perangkat.
      (1) Perangkat pengolah informasi penyimpan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dihapuskan atau dimusnahkan.
      (2) Penanganan perangkat pengolah informasi penyimpan data di setiap Perangkat Daerah sesuai dengan standar penanganan media penyimpan data yang berlaku.

   g. Pengamanan perangkat yang tidak dalam pengawasan
      Pengguna harus memastikan perangkat TI yang tidak berada dalam pengawasan memiliki perlidungan yang tepat terhadap akses oleh pihak yang tidak berwenang.
   h. Kebersihan meja kerja dan layar
      Peraturan terkait kebersihan meja kerja serta layar dari informasi penting perlu disusun dan diterapkan.

VIII.4. STANDAR

1. Perangkat harus dipelihara sesuai dengan petunjuk manualnya. Untuk pemeliharaan yang dilakukan oleh pihak ketiga, harus diadakan Perjanjian Tingkat Layanan (*Service Level Agreement/ SLA*) yang mendefinisikan tingkat pemeliharaan yang disediakan dan tingkat kinerja yang harus dipenuhi pihak ketiga.
2. Pemeliharaan terhadap perangkat keras atau perangkat lunak dilakukan hanya oleh pegawai yang berwenang.
3. Dalam hal pemeliharaan perangkat tidak dapat dilakukan di tempat, maka pemindahan perangkat harus mendapatkan persetujuan Pejabat yang berwenang. Terhadap data yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA yang disimpan dalam perangkat tersebut harus dipindahkan terlebih dahulu.
4. Otorisasi penggunaan perangkat harus dilakukan secara tertulis dan data-data yang terkait dengan aset informasi yang digunakan, seperti nama pemakai aset, lokasi, dan tujuan penggunaan aset, harus dicatat dan disimpan.
5. Pengamanan Area
   a. Setiap Perangkat Daerah menyimpan perangkat pengolah informasi di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai antara lain pintu elektronik, sistem pemadam kebakaran, alarm bahaya dan perangkat pemutus aliran listrik.
   b. Akses ke ruang server, pusat data, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus dibatasi dan hanya diberikan kepada pegawai yang berwenang.
   c. Pihak ketiga yang memasuki ruang server, pusat data, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus didampingi pegawai dan sudah diketahui oleh Kepala Perangkat Daerah sepanjang waktu kunjungan. Waktu masuk dan keluar serta maksud kedatangan harus dicatat dalam buku catatan kunjungan.
   d. Kantor, ruangan, dan perangkat yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus dilindungi secara memadai.
   e. Pegawai dan pihak ketiga tidak diizinkan merokok, makan, minum di ruang *server* dan pusat data
   f. Area keluar masuk barang dan area publik harus selalu dijaga, diawasi dan dikendalikan, dan jika memungkinkan disterilkan dari perangkat pengolah informasi untuk menghindari akses oleh pihak yang tidak berwenang.
6. Pengamanan Kantor, Ruangan dan Fasilitas
   Pengamanan kantor, ruangan dan fasilitas mencakup:
   a. Pengamanan kantor, ruangan, dan fasilitas harus sesuai dengan peraturan dan standar keamanan dan keselamatan kerja yang berlaku.
   b. Fasilitas utama harus ditempatkan khusus untuk menghindari akses publik.
   c. Pembatasan pemberian identitas atau tanda-tanda keberadaan aktivitas pengolahan informasi.
   d. Direktori dan buku telepon internal yang mengidentifikasi lokasi perangkat pengolah informasi tidak mudah diakses oleh publik.

7. Perlindungan terhadap Ancaman Eksternal dan Lingkungan
   Perlindungan terhadap ancaman eksternal dan lingkungan harus mempertimbangkan:
   a. Bahan-bahan berbahaya atau mudah terbakar harus disimpan pada jarak yang aman dari area terbatas.
   b. Perlengkapan umum seperti alat tulis tidak boleh disimpan di dalam area terbatas.
   c. Perangkat *fallback* dan *media backup* harus diletakkan pada jarak yang aman untuk menghindari kerusakan dari bencana yang mempengaruhi fasilitas utama.
   d. Perangkat pemadam kebakaran harus disediakan dan diletakkan di tempat yang tepat.
8. Penempatan dan Perlindungan Perangkat
   Penempatan dan perlindungan perangkat harus mencakup:
   a. Perangkat harus diletakkan pada lokasi yang meminimalkan akses yang tidak perlu ke dalam area kerja.
   b. Perangkat pengolah informasi yang menangani informasi sensitif harus diposisikan dan dibatasi arah sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak yang tidak berwenang selama digunakan, dan perangkat penyimpanan diamankan untuk menghindari akses oleh pihak yang tidak berwenang.
   c. Perangkat yang memerlukan perlindungan khusus seperti perangkat cetak khusus, perangkat jaringan di luar ruang *server* harus terisolasi untuk mengurangi tingkat perlindungan atau perlakuan standar yang perlu dilakukan.
   d. Langkah-langkah pengendalian dilakukan untuk meminimalkan risiko potensi ancaman fisik, seperti pencurian, api, bahan peledak, asap, air termasuk kegagalan penyediaan air, debu, getaran, efek kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetis, dan perusakan.
   e. Kondisi lingkungan, seperti suhu dan kelembaban harus dimonitor untuk mencegah perubahan kondisi yang dapat mempengaruhi pengoperasian perangkat pengolah informasi.
   f. Perlindungan petir harus diterapkan untuk semua bangunan dan filter perlindungan petir harus dipasang untuk semua jalur komunikasi dan listrik.
   g. Perangkat pengolah informasi sensitif harus dilindungi untuk meminimalkan risiko kebocoran informasi.
9. Pengamanan Kabel
   Perlindungan keamanan kabel mencakup:
   a. Pemasangan kabel sumber daya listrik·dan kabel telekomunikasi ke perangkat pengolah informasi selama memungkinkan harus terletak di bawah tanah, atau menerapkan alternatif perlindungan lain yang memadai.
   b. Pemasangan kabel jaringan harus dilindungi dari penyusupan yang tidak sah atau kerusakan, misalnya dengan menggunakan *conduit* (saluran) atau menghindari rute melalui area publik.
   c. Pemisahan antara kabel sumber daya listrik dengan kabel telekomunikasi untuk mencegah interferensi.
   d. Penandaan atau penamaan kabel dan perangkat harus diterapkan secara jelas untuk memudahkan penanganan kesalahan.
   e. Penggunaan dokumentasi daftar *panel patch* diperlukan untuk mengurangi kesalahan.

f. Pengendalian untuk sistem informasi yang sensitif harus mempertimbangkan:
   (1) Menggunaan *conduit*.
   (2) Penggunaan ruangan terkunci pada tempat inspeksi dan titik pemutusan kabel.
   (3) Penggunaan rute alternatif dan/atau media transmisi yang menyediakan keamanan yang sesuai.
   (4) Penggunaan kabel *fiber optic*.
   (5) Penggunaan lapisan elektromagnet untuk melindungi kabel.
   (6) Inisiasi penghapusan teknikal (*technical sweeps*) dan pemeriksaan secara fisik untuk peralatan yang tidak diotorisasi saat akan disambungkan ke kabel.
   (7) Penerapan akses kontrol ke *panel patch* dan ruangan kabel.

## BAB IX
## PENGENDALIAN PENGELOLAAN KEAMANAN OPERASIONAL

### IX.1. TUJUAN

Pengelolaan keamanan operasional bertujuan untuk memastikan keamanan dalam pengoperasian fasilitas pemrosesan informasi yang berada di setiap lingkungan Perangkat Daerah.

### IX.2. RUANG LINGKUP

Kebijakan dan standar pengelolaan operasional ini meliputi:
1. Prosedur operasional dan tanggung jawab.
2. Perencanaan dan penerimaan sistem.
3. Perlindungan terhadap *Malicious Code*.
4. *Information Backup*.
5. Penanganan media penyimpan data.
6. *Logging* dan *Monitoring*.
7. Pengendalian operasional perangkat lunak.
8. Pengelolaan Kerentanan Teknis.
9. Audit Operasional.

### IX.3. KEBIJAKAN

1. Prosedur Operasional dan Tanggung Jawab
   a. Dokumentasi prosedur operasional
      Setiap Perangkat Daerah harus mendokumentasikan, memelihara, dan menyediakan seluruh prosedur operasional yang terkait dengan penggunaan perangkat pengolah informasi bagi pengguna sesuai dengan peruntukannya.
   b. Pengelolaan perubahan perangkat Teknologi Informasi
      Setiap Perangkat Daerah harus mengendalikan perubahan terhadap perangkat pengolah informasi. Pengelolaan perubahan layanan Teknologi Informasi di setiap Perangkat Daerah akan ditetapkan dalam ketentuan tersendiri.
   c. Pemisahan tugas
      Kepala Perangkat Daerah harus melakukan pemisahan tugas untuk proses yang melibatkan informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA untuk menghindari adanya pegawai yang memiliki pengendalian eksklusif terhadap seluruh aset informasi dan perangkat pengolahnya.

d. Pengelolaan kapasitas
Kepala Perangkat Daerah harus memantau dan mengelola penggunaan sumber daya Teknologi Informasi serta menyusun proyeksi penggunaan sumber daya Teknologi Informasi di masa-masa mendatang, untuk menjamin ketersediaan layanan Teknologi Informasi dalam hal pemrosesan dan penyimpanan informasi.

e. Pemisahan perangkat pengembangan, pengujian dan operasional
Kepala Perangkat Daerah harus melakukan pemisahan perangkat pengembangan, pengujian, dan operasional untuk mengurangi risiko perubahan atau akses oleh pihak yang tidak berwenang terhadap sistem operasional.

2. Perencanaan dan Penerimaan Sistem
Kegiatan perencanaan dan penerimaan sistem meliputi:
a. Pengelolaan kapasitas dalam rangka perencanaan sistem
(1) Kepala Perangkat Daerah harus memantau penggunaan perangkat pengolah informasi dan membuat perkiraan pertumbuhan kebutuhan ke depan untuk memastikan ketersediaan kapasitas.
(2) Pengelolaan kapasitas di setiap Perangkat Daerah akan ditetapkan dalam ketentuan tersendiri.
b. Penerimaan Sistem
(1) Kepala Perangkat Daerah harus menetapkan kriteria penerimaan (*acceptance criteria*) untuk sistem informasi baru, pemutakhiran (*upgrade*) dan versi baru serta melakukan pengujian sebelum penerimaan.
(2) Penerimaan sistem di setiap Perangkat Daerah akan ditetapkan dalam ketentuan tersendiri.

3. Perlindungan Terhadap *Malicious Code*
a. Setiap Perangkat Daerah harus menerapkan sistem yang dapat melakukan pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan (*Malicious Code*).
b. Perlindungan terhadap ancaman program yang membahayakan (*Malicious Code*) di setiap Perangkat Daerah akan ditetapkan dalam ketentuan tersendiri.

*4. Information Backup*
a. Setiap Perangkat Daerah harus melakukan *backup* informasi dan perangkat lunak yang berada di data center secara berkala.
b. Proses backup data di setiap Perangkat Daerah harus dilakukan sesuai dengan standar *backup* data yang berlaku.

5. Penanganan Media Penyimpan Data
a. Setiap Perangkat Daerah harus mempunyai prosedur yang mengatur penanganan media penyimpan data untuk melindungi aset informasi.
b. Penanganan media penyimpanan data di setiap Perangkat Daerah sesuai dengan standar penanganan media penyimpan data yang berlaku.

*6. Logging* dan *Monitoring*
*a. Event logging*
Setiap Perangkat Daerah harus mengaktifkan dan secara rutin me-review *event logging* yang mencatat aktivitas pengguna, pengecualian, dan kejadian keamanan informasi.

b. Memantau penggunaan sistem
   Setiap Perangkat Daerah harus memantau penggunaan sistem dan mengkaji secara berkala hasil kegiatan monitoring.
c. Perlindungan terhadap informasi *log*
   Setiap Perangkat Daerah harus memastikan perlindungan terhadap fasilitas *logging* dan informasi *log* agar terhindar dari kerusakan dan akses oleh pihak yang tidak berwenang.
d. Pencatatan *log system administrator* dan *system operator*
   Setiap Perangkat Daerah harus memastikan agar kegiatan pencatatan *log system administrator* dan *system operator* tercatatkan di dalam *log*.
e. Pencatatan kesalahan (*fault logging*)
   Setiap Perangkat Daerah harus menerapkan pencatatan kesalahan (*fault logging*) untuk dianalisis dan diambil tindakan penanganan yang tepat.
f. Sinkronisasi waktu
   Setiap Perangkat Daerah harus memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.

7. Pengendalian operasional perangkat lunak
   Setiap Perangkat Daerah harus mempunyai prosedur untuk pengendalian perangkat lunak pada sistem operasional.
8. Pengelolaan Kerentanan Teknis
   a. Setiap Perangkat Daerah harus mengumpulkan informasi kerentanan teknis secara berkala dari seluruh sistem informasi yang digunakan maupun komponen pendukung sistem informasi.
   b. Setiap Perangkat Daerah harus melakukan evaluasi dan penilaian risiko terhadap kerentanan teknis yang ditemukan dalam sistem informasi serta menetapkan pengendalian yang tepat terhadap risiko terkait.
9. Audit Operasional
   Audit yang mencakup verifikasi terhadap perangkat pemrosesan informasi harus direncanakan dan disepakati dengan pihak terkait sehingga gangguan terhadap proses bisnis dapat diminimalisasi.

IX.4. STANDAR

1. Dokumentasi Prosedur Operasional
   Prosedur operasional harus mencakup:
   a. Tata cara pengolahan dan penanganan informasi.
   b. Tata cara menangani kesalahan-kesalahan atau kondisi khusus yang terjadi beserta pihak yang harus dihubungi bila mengalami kesulitan teknis.
   c. Cara memfungsikan kembali perangkat dan cara mengembalikan perangkat ke keadaan awal (*recovery*) saat terjadi kegagalan sistem.
   d. Tata cara *backup* dan *restore*.
   e. Tata cara pengelolaan jejak audit (*audit trails*) pengguna dan catatan kejadian atau kegiatan sistem.
2. Pemisahan Perangkat Pengembangan, Pengujian dan Operasional
   Pemisahan perangkat pengembangan dan operasional harus mempertimbangkan:
   a. Pengembangan dan operasional perangkat lunak harus dioperasikan di sistem atau prosesor komputer dan domain atau direktori yang berbeda.

b. Instruksi Kerja (*working instruction*) rilis dari pengembangan perangkat lunak ke operasional harus ditetapkan dan didokumentasikan.
c. *Compiler, editor*, dan alat bantu pengembangan lain tidak boleh diakses dari sistem operasional ketika tidak dibutuhkan.
d. Lingkungan sistem pengujian harus diusahakan sama dengan lingkungan sistem operasional.
e. Pengguna harus menggunakan profil pengguna yang berbeda untuk sistem pengujian dan sistem operasional, serta aplikasi harus menampilkan pesan identifikasi dari sistem untuk mengurangi risiko kesalahan.
b. Data yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA tidak boleh disalin ke dalam lingkungan pengujian sistem.

3. *Logging* dan *monitoring*
Prosedur *logging* dan *monitoring* penggunaan sistem pengolah informasi ditetapkan untuk menjamin agar kegiatan akses yang tidak sah tidak perlu terjadi. Prosedur ini mencakup monitoring:
a. Kegagalan akses (*access failures*).
b. Pola-pola *log-on* yang mengindikasikan penggunaan yang tidak wajar.
c. Alokasi dan penggunaan hak akses khusus (*privileged access capability*).
d. Penelusuran transaksi dan pengiriman file tertentu yang mencurigakan.
e. Penggunaan sumber daya sensitif.
4. Pengendalian operasional perangkat lunak
Prosedur pengendalian operasional perangkat lunak mencakup beberapa hal berikut:
a. Pengendalian akses terhadap perangkat lunak sebelum dilakukan deployment.
b. Petunjuk *deployment*, penggunaan lisensi, pengoperasian dan pemeliharaan perangkat lunak.
5. Pengelolaan Kerentanan Teknis
Pengelolaan kerentanan teknis mencakup:
a. Penunjukan fungsi dan tanggung jawab yang terkait dengan pengelolaan kerentanan teknis termasuk di dalamnya monitoring kerentanan, penilaian risiko kerentanan, *patching*, registrasi aset, dan koordinasi dengan pihak terkait.
b. Pengidentifikasian sumber informasi yang dapat digunakan untuk mengidentifikasi dan meningkatkan kepedulian terhadap kerentanan teknis.
c. Penentuan rentang waktu untuk melakukan aksi terhadap munculnya potensi kerentanan teknis. Apabila terjadi kerentanan teknis yang butuh penanganan maka harus diambil tindakan sesuai kontrol yang telah ditetapkan atau melaporkan kejadian tersebut melalui pelaporan kejadian dan kelemahan keamanan informasi.
d. Pengujian dan evaluasi penggunaan patch sebelum proses instalasi untuk memastikan *patch* dapat bekerja secara efektif dan tidak menimbulkan risiko yang lain. Apabila *patch* tidak tersedia, harus melakukan hal sebagai berikut:
(1) Mematikan *patch* yang berhubungan dengan kerentanan.
(2) Menambahkan pengendalian akses seperti *firewall*.
(3) Meningkatkan pengawasan untuk mengidentifikasi atau mencegah terjadinya serangan atau kejadian.
(4) Meningkatkan kepedulian terhadap kerentanan teknis.

e. Penyimpanan *audit log* yang memuat prosedur dan langkah-langkah yang telah diambil.
f. Monitoring dan evaluasi terhadap pengelolaan kerentanan teknis harus dilakukan secara berkala.
g. Pengelolaan kerentanan teknis diutamakan terhadap sistem informasi yang memiliki tingkat risiko tinggi.

6. Audit Operasional
Prosedur audit yang mencakup kegiatan verifikasi operasional harus disusun yang mencakup hal-hal sebagai berikut:
a. Proses perencanaan audit.
b. Proses untuk melakukan audit.
c. Proses pelaporan dan monitoring tindak lanjut audit.
d. Persyaratan auditor.

## BAB X
## PENGENDALIAN KEAMANAN KOMUNIKASI

### X.1. TUJUAN

Tujuan dari pengendalian keamanan komunikasi adalah untuk memberikan perlindungan terhadap informasi yang ditransmisikan melalui jaringan komunikasi beserta perangkat pendukungnya yang berada di lingkungan Perangkat Daerah.

### X.2. RUANG LINGKUP

Kebijakan pengendalian keamanan komunikasi ini meliputi :
1. Pengelolaan keamanan jaringan.
2. Keamanan dalam transfer Informasi.

### X.3. KEBIJAKAN

1. Pengelolaan Keamanan Jaringan
   a. Pengendalian jaringan
      (1) Setiap Perangkat Daerah harus mengelola dan melindungi jaringan dari berbagai bentuk ancaman.
      (2) Ketentuan rinci pengendalian jaringan di setiap Perangkat Daerah diuraikan dalam standar pengelolaan komunikasi dan operasional.
   b. Keamanan layanan jaringan
      Setiap Perangkat Daerah harus mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan serta mencantumkannya dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh pihak ketiga.
2. Keamanan dalam Transfer Informasi
   a. Pertukaran informasi dan perangkat lunak antara Perangkat Daerah dengan pihak ketiga hanya akan dilakukan atas kesepakatan tertulis kedua belah pihak.
   b. Setiap Perangkat Daerah harus melakukan penilaian risiko yang memadai sebelum melaksanakan pertukaran informasi.
   c. Setiap Perangkat Daerah harus 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.

d. Ketentuan rinci pertukaran informasi di setiap Perangkat Daerah diuraikan dalam standar pengelolaan komunikasi dan operasional.

X.4. STANDAR

1. Pengelolaan Keamanan Jaringan
   Pengelolaan keamanan jaringan mencakup:
   a. Monitoring kegiatan pengelolaan jaringan untuk menjamin bahwa perangkat jaringan digunakan secara efektif dan efisien.
   b. Pengendalian dan pengaturan tentang penyambungan atau perluasan jaringan internal atau eksternal Perangkat Daerah.
   c. Pengendalian dan pengaturan akses ke sistem jaringan internal atau eksternal Perangkat Daerah.
   d. Pencatatan informasi pihak ketiga yang diizinkan mengakses ke jaringan Perangkat Daerah dan menerapkan monitoring serta pencatatan kegiatan selama menggunakan jaringan.
   e. Pemutusan layanan tanpa pemberitahuan sebelumnya jika terjadi gangguan keamanan informasi.
   f. Perlindungan jaringan dari akses yang tidak berwenang mencakup.
      (1) Penetapan untuk penanggung jawab pengelolaan jaringan dipisahkan dari pengelolaan perangkat pengolah informasi.
      (2) Penerapan pengendalian khusus untuk melindungi keutuhan informasi yang melewati jaringan umum antara lain dengan penggunaan enkripsi dan tanda tangan elektronik.
      (3) Pendokumentasian arsitektur jaringan seluruh komponen perangkat keras jaringan dan perangkat lunak.
   g. Penerapan fitur keamanan layanan jaringan mencakup:
      (1) Teknologi keamanan seperti autentikasi, enkripsi, dan pengendalian sambungan jaringan.
      (2) Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan keamanan dan aturan koneksi jaringan.
      (3) Prosedur untuk penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau aplikasi.
2. Keamanan dalam Transfer lnformasi
   a. Prosedur pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup :
      (1) Perlindungan pertukaran informasi dari pencegatan, penyalinan, modifikasi, miss-routing, dan perusakan.
      (2) Pendeteksian dan perlindungan terhadap kode berbahaya yang dapat dikirim melalui penggunaan komunikasi elektronik.
      (3) Perlindungan informasi elektronik dalam bentuk attachment yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA.
      (4) Pertimbangan risiko terkait penggunaan perangkat komunikasi nirkabel.
   b. Pertukaran informasi yang tidak menggunakan perangkat komunikasi elektronik, mengacu pada ketentuan yang berlaku.
   c. Pengendalian pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:
      (1) Pencegahan terhadap penyalahgunaan wewenang pegawai dan pihak ketiga yang dapat membahayakan organisasi.
      (2) Penggunaan teknik kriptografi.
      (3) Penyelenggaraan penyimpanan dan penghapusan atau pemusnahan untuk semua korespondensi kegiatan, termasuk pesan, yang sesuai dengan ketentuan yang berlaku.

(4) Larangan meninggalkan informasi sensitif pada perangkat pengolah informasi.
(5) Pembatasan penerusan informasi secara otomatis.
(6) Pembangunan kepedulian atas ancaman pencurian informasi, misalnya terhadap:
- Pengungkapan informasi sensitif untuk menghindari mencuri dengar (penyadapan) saat melakukan panggilan telepon.
- Akses pesan diluar kewenangannya.
- Pemrograman mesin faksimili baik sengaja maupun tidak sengaja untuk mengirim pesan ke nornor tertentu.
- Pengiriman dokumen dan pesan ke tujuan yang salah.

d. Pembangunan kepedulian atas pendaftaran data demografis, seperti alamat surat elektronik atau informasi pribadi lainnya untuk menghindari pengumpulan inforrnasi yang tidak sah.
e. Penyediaan informasi internal Perangkat Daerah bagi masyarakat umum harus disetujui oleh pemilik informasi dan sesuai dengan ketentuan yang berlaku.

## BAB XI
## PENGENDALIAN KEAMANAN INFORMASI DALAM AKUISISI, PENGEMBANGAN DAN PEMELIHARAAN SISTEM INFORMASI

### XI.1. TUJUAN

Keamanan informasi dalam pengadaan, pengembangan, dan pemeliharaan sistem informasi bertujuan untuk memastikan bahwa keamanan informasi merupakan bagian yang terintegrasi dengan sistem informasi, mencegah terjadinya kesalahan, kehilangan, serta modifikasi oleh pihak yang tidak berwenang.

### XI.2. RUANG LINGKUP

1. Persyaratan keamanan pada sistem informasi.
2. Keamanan dalam proses pengembangan dan pendukung (*support proceses*).
3. Keamanan *system files*.

### XI.3. KEBIJAKAN

1. Persyaratan keamanan pada sistem informasi mencakup setidaknya hal-hal berikut ini:
   a. Kepala Perangkat Daerah menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi yang relevan sebelum pengadaan, pengembangan, atau pemeliharaan sistem informasi baru.
   b. Pengolahan Informasi pada Aplikasi, mencakup:
      (1) Validasi data yang masuk
      (2) Data yang akan dimasukkan ke aplikasi harus diperiksa terlebih dahulu kebenaran dan kesesuaiannya.
      (3) Pengendalian proses internal
      (4) Pada setiap aplikasi harus disertakan proses validasi untuk mendeteksi bahwa informasi yang dihasilkan utuh dan sesuai dengan yang diharapkan.
      (5) Validasi data keluaran

(6) Data keluaran aplikasi harus divalidasi untuk memastikan data yang dihasilkan adalah benar.

2. Keamanan dalam proses pengembangan dan pendukung (*support proceses*)
   a. Prosedur pengendalian perubahan sistem operasi
      Setiap Perangkat Daerah harus mengendalikan perubahan pada sistem operasi dengan penggunaan prosedur pengendalian perubahan.
   b. Prosedur pengendalian perubahan pada perangkat lunak
      Setiap Perangkat Daerah harus mengendalikan perubahan terhadap perangkat lunak, baik perangkat lunak yang dikembangkan sendiri maupun pihak ketiga.
   c. Kajian teknis aplikasi setelah perubahan sistem operasi dan/atau perangkat lunak
      Setiap Perangkat Daerah harus meninjau dan menguji sistem operasi dan/atau perangkat lunak untuk memastikan tidak ada dampak merugikan pada proses operasional atau keamanan informasi di Perangkat Daerah yang bersangkutan apabila terjadi perubahan sistem operasi dan/atau perangkat lunak, terutama pada perangkat lunak yang memproses informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA.
   d. Kebocoran informasi
      Setiap Perangkat Daerah harus mencegah kemungkinan terjadinya kebocoran informasi.
   e. Pengembangan perangkat lunak oleh pihak ketiga
      Kepala Perangkat Daerah harus melakukan supervisi dan memantau pengembangan perangkat lunak oleh pihak ketiga.
3. Keamanan *System File*
   a. Pengendalian operasional perangkat lunak
      Setiap Perangkat Daerah harus mempunyai prosedur untuk pengendalian perangkat lunak pada sistem operasional.
   b. Perlindungan terhadap sistem pengujian data
      Setiap Perangkat Daerah harus menentukan sistem pengujian data, melindunginya dari kemungkinan kerusakan, kehilangan atau perubahan oleh pihak yang tidak berwenang.
   c. Pengendalian akses ke kode program (*source code*)
      Setiap Perankgat Daerah harus mengendalikan akses ke kode program (*source code)* secara ketat dan salinan versi terkini dari perangkat lunak disimpan di tempat yang aman.

XI.4. STANDAR

1. Spesifikasi kebutuhan perangkat pengolah informasi yang dikembangkan baik oleh internal atau pihak ketiga harus didokumentasikan secara formal.
2. Standar Pengolahan Data pada Aplikasi adalah sebagai berikut:
   a. Pemeriksaan data masukan harus mempertimbangkan:
      1) Penerapan masukan rangkap (*dual input*) atau mekanisme pengecekan masukan lainnya untuk mendeteksi kesalahan berikut :
         - Di luar rentang/batas nilai-nilai yang diperbolehkan.
         - Karakter tidak valid dalam field data.
         - Data hilang atau tidak lengkap.
         - Melebihi batas atas dan bawah volume data.
         - Data yang tidak diotorisasi dan tidak konsisten.

(2) Pengkajian secara berkala terhadap isi field kunci (*key field*) atau file data untuk mengkonfirmasi keabsahan dan integritas data.
(3) Memeriksa dokumen *hard copy* untuk memastikan tidak adanya perubahan data masukan yang tidak melalui otorisasi.
(4) Menampilkan pesan yang sesuai dalam menanggapi kesalahan validasi.
(5) Prosedur untuk menguji kewajaran dari data masukan.
(6) Menguraikan tanggung jawab dari seluruh pegawai yang terkait dalam proses perekaman data.
(7) Sistem mampu membuat dari mengeluarkan catatan aktivitas terkait proses perekaman data.

b. Menyusun daftar pemeriksaan (*check list*) yang sesuai, mendokumentasikan proses pemeriksaan, dan menyimpan hasilnya secara aman. Proses pemeriksaan mencakup:
(1) Pengendalian session atau batch, untuk mencocokkan data setelah perubahan transaksi.
(2) Pengendalian balancing untuk memeriksa data sebelum dan sesudah transaksi.
(3) Validasi data masukan yang dihasilkan sistem.
(4) Keutuhan dan keaslian data yang diunduh/diunggah (*download/upload*).
(5) *Hash totals* dari *record* dan *file*.
(6) Aplikasi berjalan sesuai dengan rencana dan waktu yang ditentukan.
(7) Program dijalankan dalam urutan yang benar dan menghentikan sementara jika terjadi kegagalan sampai masalah diatasi.
(8) Sistem mampu membuat dan mengeluarkan catatan aktivitas pengelolaan internal.

c. Pemeriksaan data keluaran harus mempertimbangkan:
(1) Kewajaran dari data keluaran yang dihasilkan.
(2) Pengendalian rekonsiliasi data untuk memastikan kebenaran pengolahan data.
(3) Menyediakan informasi yang cukup untuk pengguna atau sistem pengolahan informasi untuk menentukan akurasi, kelengkapan, ketepatan, dan klasifikasi informasi.
(4) Prosedur untuk menindaklanjuti validasi data keluaran.
(5) Menguraikan tanggung jawab dari seluruh pegawai yang terkait proses data keluaran.
(6) Sistem mampu membuat dan mengeluarkan catatan aktivitas dalam proses validasi data keluaran.

3. Keamanan *System File*

a. Pengembangan prosedur pengendalian perangkat lunak pada sistem operasional harus mempertimbangkan:
(1) Proses pemutakhiran perangkat lunak operasional, aplikasi hanya boleh dilakukan oleh *system administrator* terlatih setelah melalui proses otorisasi.
(2) Sistem operasional hanya berisi program aplikasi *executable* yang telah diotorisasi, tidak boleh berisi kode program (*source code*) atau *compiler*.
(3) Aplikasi dan perangkat lunak sistem operasi hanya dapat diimplementasikan setelah melewati proses pengujian yang ekstensif.

(4) Sistem pengendalian konfigurasi harus digunakan untuk mengendalikan seluruh perangkat lunak yang telah diimplementasikan beserta dokumentasi sistem.
(5) Strategi *rollback* harus tersedia sebelum suatu perubahan diimplementasikan.
(6) Catatan audit harus dipelihara untuk menjaga kemutakhiran informasi atau data operasional.
(7) Versi terdahulu dari suatu aplikasi harus tetap disimpan untuk keperluan kontinjensi.
(8) Versi lama dari suatu perangkat lunak harus diarsip, bersama dengan informasi terkait dan prosedur, parameter, konfigurasi rinci, dan perangkat lunak pendukung.

b. Perlindungan terhadap sistem pengujian data harus mempertimbangkan:
(1) Prosedur pengendalian akses, yang berlaku pada sistem aplikasi operasional, harus berlaku juga pada sistem aplikasi pengujian.
(2) Proses otorisasi setiap kali informasi atau data operasional digunakan pada sistem pengujian.
(3) Penghapusan informasi atau data operasional yang digunakan pada sistem pengujian segera setelah proses pengujian selesai.
(4) Pencatatan jejak audit penggunaan informasi atau data operasional.

c. Pengendalian akses ke kode program (*source code*) harus mempertimbangkan:
(1) Kode program (*source code*) tidak boleh disimpan pada sistem operasional;
(2) Pengelolaan kode program (*source code*) dan library harus mengikuti prosedur yang telah ditetapkan.
(3) Pengelola Teknologi Informasi tidak boleh memiliki akses yang tidak terbatas ke kode program (*source code*) dan library.
(4) Proses pemutakhiran kode program (*source code*) dan item terkait, serta pemberian kode program (*source code*) kepada programmer hanya dapat dilakukan setelah melalui proses otorisasi.
(5) Daftar program harus disimpan dalam *secure areas*.
(6) Catatan audit dari seluruh akses ke kode program (*source code*) library harus dipelihara.
(7) Pemeliharaan dan penyalinan kode program (*source code*) library harus mengikuti prosedur pengendalian perubahan.

4. Keamanan dalam proses pengembangan dan pendukung (support proceses)
a. Prosedur pengendalian perubahan sistem operasi dan perangkat lunak, mencakup:
(1) Memelihara catatan persetujuan sesuai dengan kewenangannya.
(2) Memastikan permintaan perubahan diajukan oleh pihak yang berwenang.
(3) Melakukan review untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan.
(4) Melakukan identifikasi terhadap perangkat lunak, informasi, basis data, dan perangkat keras yang perlu diubah.
(5) Mendapatkan persetujuan formal dari pihak yang berwenang sebelum pelaksanaan perubahan.

(6) Memastikan pihak yang berwenang menerima perubahan yang diminta sebelum dilakukan implementasi.
(7) Memastikan bahwa dokumentasi sistem mutakhir dan dokumen versi sebelumnya diarsip.
(8) Memelihara versi perubahan aplikasi.
(9) Memelihara jejak audit perubahan aplikasi.
(10) Memastikan dokumentasi penggunaan dan prosedur telah diubah sesuai dengan perubahan yang dilaksanakan.
(11) Memastikan bahwa implementasi perubahan dilakukan pada waktu yang tepat dan tidak menganggu kegiatan.

b. Prosedur kajian teknis aplikasi setelah perubahan sistem operasi dan/atau perangkat lunak, mencakup:
(1) Melakukan review untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan.
(2) Memastikan rencana dan anggaran *annual support* yang mencakup review dan sistem *testing* dari perubahan sistem operasi.
(3) Memastikan pemberitahuan perubahan sistem informasi dilakukan dalam jangka waktu yang tepat untuk memastikan tes dan review telah dilaksanakan sebelum implementasi.
(4) Memastikan bahwa perubahan telah diselaraskan dengan rencana Kelangsungan kegiatan.

c. Kebocoran informasi
Pengendalian yang dapat diterapkan untuk membatasi risiko kebocoran informasi, antara lain:
(1) Melakukan monitoring terhadap aktivitas pegawai dan pihak ketiga, sistem sesuai dengan ketentuan yang berlaku.
(2) Melakukan monitoring terhadap aktivitas penggunaan desktop dan perangkat *mobile*.

d. Pengembangan perangkat lunak oleh pihak ketiga harus mempertimbangkan :
(1) Perjanjian lisensi, kepemilikan *source code*, dan Hak Atas Kekayaan Intelektual (HAKI).
(2) Perjanjian *escrow* (jaminan pelaksanaan).
(3) Hak untuk melakukan audit terhadap kualitas dan akurasi pekerjaan.
(4) Persyaratan kontrak mengenai kualitas dan fungsi keamanan aplikasi.
(5) Uji coba terhadap aplikasi untuk memastikan tidak terdapat *malicious code* sebelum implementasi.

## BAB XII
## PENGENDALIAN HUBUNGAN DENGAN PIHAK KETIGA ATAU PENYEDIA JASA/BARANG

### XII.1. TUJUAN

Pengelolaan hubungan dengan pihak ketiga atau penyedia jasa/barang bertujuan untuk memastikan terlindungnya aset-aset organisasi di setiap Perangkat Daerah yang dapat diakses oleh pihak ketiga atau penyedia jasa/barang serta mempertahankan tingkat keamanan informasi dan pelayanan yang telah disepakati dengan pihak ketiga atau penyedia jasa/barang.

XII.2. RUANG LINGKUP

Kebijakan dan standar pengelolaan hubungan dengan pihak ketiga atau penyedia jasa/barang ini meliputi:

1. Pengendalian hubungan dengan pihak ketiga atau penyedia jasa/barang.
2. Keamanan informasi dalam kesepakatan dengan penyedia layanan (pihak ketiga atau penyedia jasa/barang).
3. Pengkajian terhadap kinerja penyedia layanan (pihak ketiga atau penyedia jasa/barang).
4. Pengelolaan perubahan terhadap layanan yang disediakan oleh pihak ketiga atau penyedia jasa/barang.

XII.3. KEBIJAKAN

1. Kepala Perangkat Daerah harus menerapkan pengendalian keamanan informasi berdasarkan hasil penilaian risiko untuk mencegah atau mengurangi dampak risiko terkait dengan pemberian akses kepada pihak ketiga.
2. Kepala Perangkat Daerah harus memastikan bahwa pengendalian keamanan informasi, definisi layanan, dan tingkat layanan yang tercantum dalam kesepakatan penyediaan layanan telah diterapkan, dioperasikan, dan dipelihara oleh pihak ketiga atau penyedia jasa/barang.
3. Kepala Perangkat Daerah harus memastikan terdapat persyaratan untuk mengatasi risiko keamanan informasi pada kesepakatan dengan pihak ketiga atau penyedia jasa/barang yang berhubungan dengan layanan teknologi informasi dan komunikasi serta rantai pasokan produk.
4. Kepala Perangkat Daerah harus melakukan monitoring dan kajian terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh pihak ketiga atau penyedia jasa/barang secara berkala.
5. Kepala Perangkat Daerah harus memperhatikan kritikalitas, proses yang terkait, dan hasil penilaian ulang risiko layanan apabila terjadi perubahan pada layanan yang disediakan pihak ketiga atau penyedia jasa/barang.

XII.4. STANDAR

Standar monitoring dan pengkajian layanan dari pihak ketiga, serta laporan dan catatan dari pihak ketiga mencakup proses sebagai berikut:

1. Monitoring tingkat kinerja layanan untuk memastikan kesesuaian kepatuhan dengan perjanjian.
2. Pengkajian laporan layanan pihak ketiga dan pengaturan pertemuan berkala dalam rangka pembahasan perkembangan layanan sebagaimana diatur dalam perjanjian atau kesepakatan.
3. Pemberian informasi tentang gangguan keamanan informasi dan pengkajian informasi ini bersama pihak ketiga sebagaimana diatur dalam perjanjian atau kesepakatan.
4. Pemeriksaan jejak audit pihak ketiga dan pencatatan peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan.
5. Penyelesaian dan pengelolaan masalah yang teridentifikasi.

# BAB XIII
# PENGENDALIAN PENGELOLAAN GANGGUAN KEAMANAN INFORMASI

## XIII.1. TUJUAN

Pengelolaan gangguan keamanan informasi bertujuan untuk memastikan kejadian dan kelemahan keamanan informasi yang terhubung dengan sistem informasi dikomunikasikan untuk dilakukan perbaikan, serta dilakukan pendekatan yang konsisten dan efektif agar dapat dihindari atau tidak terulang kembali.

## XIII.2. RUANG LINGKUP

Kebijakan dan standar pengelolaan gangguan keamanan informasi ini meliputi:
1. Pelaporan kejadian dan kelemahan keamanan informasi.
2. Pengelolaan gangguan keamanan informasi dan perbaikannya.

## XIII.3. KEBIJAKAN

1. Pelaporan Kejadian dan Kelemahan Keamanan Informasi
   a. Pegawai dan pihak ketiga harus melaporkan kepada Tim Keamanan Informasi Perangkat Daerah sesegera mungkin pada saat menemui kelemahan atau terjadi gangguan keamanan informasi dalam sistem atau layanan Teknologi Informasi pada Perangkat Daerah.
   b. Proses penanganan gangguan di setiap Perangkat Daerah akan ditetapkan dalam ketentuan tersendiri.
2. Pengelolaan Gangguan Keamanan Informasi dan Perbaikannya
   a. Prosedur dan tanggung jawab
      (1) Setiap Perangkat Daerah harus menyusun prosedur dan menguraikan tanggung jawab pegawai, terkait dalam rangka memastikan gangguan keamanan informasi dapat ditangani secara cepat dan efektif.
      (2) Setiap Perangkat Daerah harus melaporkan kejadian gangguan/kerentanan terhadap keamanan informasi elektronik kepada CSIRT melalui portal layanan elektronik CSIRT pada alamat *https://csirt.pontianak.go.id/*
   b. Peningkatan penanganan gangguan keamanan informasi
      (1) Seluruh gangguan keamanan informasi yang terjadi dan tindakan mengatasinya harus dicatat dalam suatu basis data dan/atau buku catatan pelaporan gangguan keamanan informasi, dan akan menjadi masukan pada proses peningkatan penanganan gangguan keamanan informasi.
      (2) Seluruh catatan gangguan keamanan informasi akan dievaluasi dan dianalisa untuk perbaikan dan pencegahan agar gangguan keamanan informasi tidak terulang.
   c. Pengumpulan bukti pelanggaran.
      Mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap Kebijakan dan Standar Manajemen Keamanan Informasi SPBE kepada Tim Keamanan Informasi yang ada di Perangkat Daerah yang bersangkutan.
   d. Pengkajian terhadap kejadian keamanan informasi
      Kepala Perangkat Daerah perlu melakukan pengkajian terhadap kejadian keamanan informasi serta memutuskan dari hasil kajian apakah kejadian tersebut tergolong ke dalam gangguan keamanan informasi.

e. Kepala Perangkat Daerah harus memastikan bahwa seluruh gangguan keamanan informasi yang terjadi ditanggapi sesuai dengan prosedur formal penanganan gangguan keamanan informasi yang berlaku.

XIII.4. STANDAR

1. Pelaporan Kejadian dan Kelemahan Keamanan Informasi
   a. Gangguan keamanan informasi antara lain:
      (1) Hilangnya layanan, perangkat, atau fasilitas Teknologi Informasi.
      (2) Kerusakan fungsi sistem atau kelebihan beban.
      (3) Perubahan sistem diluar kendali.
      (4) Kerusakan fungsi perangkat lunak atau perangkat keras.
      (5) Pelanggaran akses ke dalam sistem pengolah informasi Teknologi Informasi.
      (6) Kelalaian manusia.
      (7) Ketidaksesuaian dengan ketentuan yang berlaku.
   b. Pegawai dan pihak ketiga harus menyadari tanggung jawab mereka untuk melaporkan setiap gangguan keamanan informasi secepat mungkin. Pelaporan gangguan harus mencakup:
      (1) Proses umpan balik yang sesuai untuk memastikan bahwa pihak yang melaporkan kejadian keamanan informasi mendapatkan pemberitahuan penanganan masalah.
      (2) Formulir laporan gangguan keamanan informasi untuk mendukung tindakan pelaporan dan membantu pelapor mengingat kronologis kejadian keamanan informasi.
      (3) Perilaku yang benar dalam menghadapi gangguan keamanan informasi, antara lain:
         - Mencatat semua rincian penting gangguan dengan segera, seperti jenis pelanggaran, jenis kerusakan, pesan pada layar, atau anomali sistem.
         - Segera melaporkan gangguan ke pihak berwenang sebelum melakukan tindakan penanganan sendiri.
      (4) Bukti-bukti pendukung sebagai referensi yang digunakan dalam proses penanganan pelanggaran disiplin bagi pegawai dan pihak ketiga yang melakukan pelanggaran keamanan informasi.
2. Prosedur Pengelolaan Gangguan Keamanan Informasi
   Prosedur pengelolaan gangguan keamanan informasi harus mempertimbangkan:
   a. Prosedur yang harus ditetapkan untuk menangani berbagai jenis gangguan keamanan informasi, antara lain:
      (1) Kegagalan sistem informasi dan hilangnya layanan.
      (2) Serangan program yang membahayakan (*malicious code*).
      (3) Serangan *denial of service*.
      (4) Kesalahan akibat data tidak lengkap atau tidak akurat.
      (5) Pelanggaran kerahasiaan dan keutuhan.
      (6) Penyalahgunaan sistem informasi.
   b. Untuk melengkapi rencana kontingensi, prosedur harus mencakup:
      (1) Analisis dan identifikasi penyebab gangguan.
      (2) Mengarantina atau membatasi gangguan.
      (3) Perencanaan dan pelaksanaan tindakan korektif untuk mencegah gangguan berulang.

(4) Komunikasi dengan pihak-pihak yang terkena dampak pemulihan gangguan.
(5) Pelaporan tindakan ke pihak berwenang.

c. Jejak audit dan bukti serupa harus dikumpulkan dan diamankan untuk:
(1) Analisis masalah internal.
(2) Digunakan sebagai bukti forensik yang berkaitan dengan potensi pelanggaran kontrak atau peraturan atau persyaratan dalam hal proses pidana atau perdata.
(3) Digunakan sebagai bahan tuntutan ganti rugi pada pihak ketiga yang menyediakan perangkat lunak dan layanan.

b. Tindakan untuk memulihkan keamanan dari pelanggaran dan perbaikan kegagalan sistem harus dikendalikan secara hati-hati dan formal, prosedur harus memastikan bahwa:
(1) Hanya pegawai yang sudah diidentifikasi dan berwenang yang diizinkan akses langsung ke sistem dan data.
(2) Semua tindakan darurat yang diambil, didokumentasikan secara rinci.
(3) Tindakan darurat dilaporkan kepada pihak berwenang.
(4) Keutuhan sistem dan pengendaliannya dikonfirmasikan dengan pihakpihak terkait sesegera mungkin.

## BAB XIV
## PENGENDALIAN ASPEK KEAMANAN INFORMASI DALAM PENGELOLAAN KELANGSUNGAN KEGIATAN

### XIV.1. TUJUAN

Pengendalian terhadap aspek keamanan informasi dalam pengelolaan kelangsungan kegiatan bertujuan untuk melindungi sistem informasi, memastikan berlangsungnya kegiatan dan layanan pada saat keadaan darurat, serta memastikan pemulihan yang tepat.

### XIV.2. RUANG LINGKUP

Kebijakan dan standar keamanan informasi dalam pengelolaan kelangsungan kegiatan ini meliputi:
1. Proses Pengelolaan Kelangsungan Kegiatan.
2. Penilaian Risiko dan Analisis Dampak Bisnis (*Business Impact Analysis/BIA*).
3. Penyusunan dan Penerapan Rencana Kelangsungan Kegiatan (*Business Continuity Plan/BCP*).
4. Pengujian, Pemeliharaan, dan Pengkajian Ulang Rencana Kelangsungan Kegiatan.
5. Menerapkan Kelangsungan Keamanan Informasi.

### XIV.3. KEBIJAKAN

1. Setiap Perangkat Daerah harus mengelola proses kelangsungan kegiatan pada saat keadaan darurat di lingkungan kerja masing-masing.
2. Setiap Perangkat Daerah harus mengidentifikasi risiko, dan menganalisis dampak yang diakibatkan pada saat terjadi keadaan darurat untuk menjamin kelangsungan kegiatan.

3. Setiap Perangkat Daerah harus menyusun dan menerapkan Rencana Kelangsungan Kegiatan untuk menjaga dan mengembalikan kegiatan operasional dalam jangka waktu yang disepakati dan level yang dibutuhkan.
4. Setiap Perangkat Daerah harus memelihara dan memastikan rencana-rencana yang termuat dalam Rencana Kelangsungan Kegiatan masih sesuai, dan mengidentifikasi prioritas untuk kegiatan uji coba.
5. Setiap Perangkat Daerah harus melakukan uji coba Rencana Kelangsungan Kegiatan secara berkala untuk memastikan Rencana Kelangsungan Kegiatan dapat dilaksanakan secara efektif.
6. Setiap Perangkat Daerah harus menetapkan, mendokumentasikan, menerapkan dan memelihara proses, prosedur dan kontrol untuk memastikan tingkat kelangsungan keamanan informasi yang diperlukan selama terjadi situasi yang merugikan.
7. Fasilitas yang digunakan untuk memproses data atau informasi perlu mengimplementasikan sistem cadangan (*redudancy*) untuk menjamin ketersediaan terhadap data atau informasi organisasi.

XIV.4. STANDAR

1. Pengelolaan Kelangsungan Kegiatan pada saat Keadaan Darurat Komponen yang harus diperhatikan dalam mengelola proses kelangsungan kegiatan:
   a. Identifikasi risiko dan analisis dampak yang diakibatkan pada saat terjadi keadaan darurat.
   b. Identifikasi seluruh aset informasi yang menunjang proses kegiatan kritikal.
   c. Identifikasi sumber daya, mencakup biaya, struktur organisasi, teknis pelaksanaan, pegawai dan pihak ketiga.
   d. Memastikan keselamatan pegawai, dan perlindungan terhadap perangkat pengolah informasi dan aset organisasi.
   e. Penyusunan dan pendokumentasian Rencana Kelangsungan Kegiatan sesuai dengan Rencana Strategi (Renstra) Kepala Perangkat Daerah.
   f. Pelaksanaan uji coba dan pemeliharaan Rencana Kelangsungan Kegiatan secara berkala.
2. Proses identifikasi risiko mengikuti ketentuan mengenai Penerapan Manajemen Risiko di setiap Perangkat Daerah.
3. Proses analisis dampak kegiatan harus melibatkan pemilik proses bisnis dan dievaluasi secara berkala.
4. Penyusunan Rencana Kelangsungan Kegiatan mencakup:
   a. Prosedur saat keadaan darurat, mencakup tindakan yang harus dilakukan serta pengaturan hubungan dengan pihak berwenang.
   b. Prosedur *fallback*, mencakup tindakan yang harus diambil untuk memindahkan kegiatan kritikal atau layanan pendukung ke lokasi kerja sementara, dan mengembalikan operasional kegiatan kritikal dalam jangka waktu sesuai dengan standar ketersediaan data yang berlaku di setiap Perangkat Daerah.
   c. Prosedur saat kondisi telah normal (*resumption*), adalah tindakan mengembalikan kegiatan operasional ke kondisi normal.
   d. Jadwal uji coba, mencakup langkah-langkah dan waktu pelaksanaan uji coba serta proses pemeliharaannya.

e. Pelaksanaan pelatihan dan sosialisasi dalam rangka meningkatkan kepedulian dan pemahaman proses kelangsungan kegiatan dan memastikan proses kelangsungan kegiatan dilaksanakan secara efektif.
f. Tanggung jawab dan peran setiap Petugas Pelaksana Pengelolaan Proses Kelangsungan.
g. Daftar kebutuhan aset informasi kritikal dan sumber daya untuk dapat menjalankan prosedur saat keadaan darurat, *fallback* dan saat kondisi telah normal (*resumption*).

5. Uji Coba Rencana Kelangsungan Kegiatan harus dilaksanakan untuk memastikan setiap rencana yang disusun dapat dilakukan atau dipenuhi pada saat penerapannya. Kegiatan uji coba Rencana Kelangsungan Kegiatan ini mencakup:
   a. Simulasi terutama untuk Petugas Pelaksana Pengelolaan Proses Kelangsungan Kegiatan.
   b. Uji coba *recovery* sistem informasi untuk memastikan sistem informasi dapat berfungsi kembali.
   c. Uji coba proses *recovery* di lokasi kerja sementara untuk menjalankan proses bisnis secara paralel.
   d. Uji coba terhadap perangkat dan layanan yang disediakan oleh pihak ketiga.
   e. Uji coba keseluruhan mulai dari organisasi, petugas, peralatan, perangkat, dan prosesnya.

## BAB XV
## PENGENDALIAN KEPATUHAN

### XV.1. TUJUAN

Pengendalian kepatuhan bertujuan untuk menghindari pelanggaran terhadap peraturan perundangan yang terkait keamanan informasi.

### XV.2. RUANG LINGKUP

Kebijakan dan standar kepatuhan ini meliputi:
1. Kepatuhan terhadap peraturan perundangan yang terkait keamanan informasi.
2. Kepatuhan teknis.
3. Audit sistem informasi.

### XV.3. KEBIJAKAN

1. Kepatuhan terhadap Peraturan Perundangan yang terkait Keamanan lnformasi
   a. Seluruh pegawai dan pihak ketiga harus menaati peraturan perundangan yang terkait dengan keamanan informasi.
   b. Identifikasi peraturan perundangan yang dapat diterapkan
      Setiap Perangkat Daerah harus mengidentifikasi, mendokumentasikan dan memelihara kemutakhiran semua peraturan perundangan yang terkait dengan sistem keamanan informasi.
   c. Hak Atas Kekayaan Intelektual
      Perangkat lunak yang dikelola Perangkat Daerah harus mematuhi ketentuan penggunaan lisensi. Penggandaan perangkat lunak secara tidak sah tidak diizinkan dan merupakan bentuk pelanggaran.

d. Perlindungan terhadap rekaman
   Rekaman milik Perangkat Daerah harus dilindungi dari kehilangan, kerusakan atau penyalahgunaan.
e. Pengamanan data
   Setiap Perangkat Daerah melindungi kepemilikan dan kerahasiaan data. Data hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundangan dan kesepakatan.

2. Kepatuhan Teknis
   Setiap Perangkat Daerah melakukan pemeriksaan kepatuhan teknis secara berkala untuk menjamin efektivitas standar dan prosedur keamanan informasi yang ada di area operasional.
3. Audit Sistem Informasi
   a. Pengendalian audit sistem informasi
      Kepala Perangkat Daerah bersama dengan Unit Terkait harus membuat perencanaan persyaratan, ruang lingkup, dan kegiatan audit yang melibatkan pemeriksaan sistem operasional untuk mengurangi kemungkinan risiko gangguan yang bisa terjadi terhadap kegiatan pada Perangkat Daerah selama proses audit.
   b. Perlindungan terhadap alat bantu (*tools*) audit sistem informasi
      Penggunaan alat bantu (baik perangkat lunak maupun perangkat keras) untuk mengetahui kelemahan keamanan, memindai (*scanning*) kata sandi, atau untuk melemahkan dan menerobos sistem keamanan informasi tidak diizinkan kecuali atas persetujuan Pimpinan Perangkat Daerah yang bersangkutan.
   c. Audit sistem informasi di setiap Perangkat Daerah akan ditetapkan dalam ketentuan tersendiri.

XV.4. STANDAR

1. Kepatuhan terhadap Hak Kekayaan Intelektual
   Hal yang perlu diperhatikan dalam melindungi segala materi yang dapat dianggap kekayaan intelektual meliputi:
   a. Mendapatkan perangkat lunak hanya melalui sumber yang dikenal dan memiliki reputasi baik, untuk memastikan hak cipta tidak dilanggar.
   b. Memelihara daftar aset informasi sesuai persyaratan untuk melindungi hak kekayaan intelektual.
   b. Memelihara bukti kepemilikan lisensi, master disk, buku manual, dan lain sebagainya.
   c. Menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki
   d. Melakukan pemeriksaan bahwa hanya perangkat lunak dan produk berlisensi yang dipasang.
   e. Patuh terhadap syarat dan kondisi untuk perangkat lunak dan informasi yang didapat dari jaringan publik.
   f. Dilarang melakukan duplikasi, konversi ke format lain atau mengambil dari rekaman komersial (*film* atau *audio*), selain yang diperbolehkan oleh Undang-Undang Hak Cipta.
   g. Tidak menyalin secara penuh atau sebagian buku, artikel, laporan, atau dokumen lainnya, selain yang diizinkan oleh Undang-Undang Hak Cipta.
2. Kepatuhan terhadap Kebijakan dan Standar
   Hal yang perlu dilakukan jika terdapat ketidakpatuhan teknis meliputi:
   a. Menentukan dan mengevaluasi penyebab ketidakpatuhan.

b. Menentukan tindakan yang perlu dilakukan berdasarkan hasil evaluasi agar ketidakpatuhan tidak terulang kembali.
c. Menentukan dan melaksanakan tindakan perbaikan yang sesuai.
d. Mengkaji tindakan perbaikan yang dilakukan.

3. Kepatuhan Teknis
Sistem informasi harus diperiksa secara berkala untuk memastikan pengendalian perangkat keras dan perangkat lunak telah diimplementasikan secara benar. Kepatuhan teknis juga mencakup pengujian penetrasi (*penetration testing*) untuk mendeteksi kerentanan dalam sistem, dan memeriksa pengendalian akses untuk mencegah kerentanan tersebut telah diterapkan.

4. Kepatuhan terkait Audit Sistem Informasi
Proses audit sistem informasi harus memperhatikan hal-hal berikut:
a. Persyaratan audit harus disetujui oleh Kepala Perangkat Daerah.
b. Ruang lingkup pemeriksaan atau audit harus disetujui dan dikendalikan oleh pihak berwenang.
c. Pemeriksaan perangkat lunak dan data harus dibatasi untuk akses baca saja (*read-only*).
d. Selain akses baca saja, hanya diizinkan untuk salinan dari *file* sistem yang diisolasi, yang harus dihapus bila audit telah selesai, atau diberikan perlindungan yang tepat jika ada kewajiban untuk menyimpan file tersebut di bawah persyaratan dokumentasi audit.
e. Sumber daya untuk melakukan pemeriksaan harus secara jelas diidentifikasi dan tersedia.
f. Persyaratan untuk pengolahan khusus atau tambahan harus diidentifikasi dan disepakati.
g. Semua akses harus dipantau dan dicatat untuk menghasilkan jejak audit, dan untuk data dan sistem informasi sensitif harus mempertimbangkan pencatatan waktu (*timestamp*) pada jejak audit.
h. Semua prosedur, persyaratan, dan tanggung jawab harus didokumentasikan.
i. Auditor harus independen dari kegiatan yang diaudit.

DAFTAR ISTILAH YANG DIGUNAKAN

1. Akun adalah identifikasi pengguna yang diberikan oleh unit Pengelola Teknologi Informasi, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem Teknologi Informasi.
2. Akun khusus adalah akun yang diberikan oleh unit Pengelola Teknologi Informasi sesuai kebutuhan tetapi tidak terbatas pada pengelolaan Teknologi Informasi (baik berupa aplikasi atau sistem), dan kelompok kerja (baik berupa acara kedinasan, tim, atau unit kerja).
3. Aset fisik adalah jenis aset yang memiliki wujud fisik, misalnya perangkat komputer, perangkat jaringan dan komunikasi, *removable media*, dan perangkat pendukung lainnya.
4. Aset tak berwujud adalah jenis aset 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 empat puluh tahun.

5. Catatan dalam penggunaannya, data dapat berupa informasi yang menjadi data baru, sebaliknya informasi dapat berfungsi sebagai data untuk menghasilkan informasi baru.
6. *Conduit* adalah sebuah tabung atau saluran untuk melindungi kabel yang biasanya terbuat dari baja.
7. Daftar inventaris aset informasi adalah kumpulan informasi yang memuat bentuk, pemilik, lokasi, retensi, dan hal-hal yang terkait dengan aset informasi.
8. Data adalah catatan atas kumpulan fakta yang mempunyai arti baik secara kualitatif maupun kuantitatif.
9. *Denial of service* adalah suatu kondisi dimana sistem tidak dapat memberikan layanan secara normal, yang disebabkan oleh suatu proses yang tidak terkendali baik dari dalam maupun dari luar sistem.
10. Direktori adalah hirarki atau tree structure.
11. Dokumen Manajemen Keamanan Informasi SPBE adalah dokumen terkait pelaksanaan Manajemen Keamanan Informasi SPBE yang meliputi antara lain dokumen kebijakan, standar, prosedur, dan catatan penerapan Manajemen Keamanan Informasi SPBE.
12. *Fallback* adalah suatu tindakan pembalikan atau menarik diri dari posisi awal.
13. Fasilitas adalah sarana untuk melancarkan pelaksanaan fungsi atau mempermudah sesuatu.
14. Fasilitas utama adalah sarana utama gedung atau bangunan, seperti: pusat kontrol listrik, CCTV.
15. *Fault logging* adalah pencatatan permasalahan sistem informasi.
16. Hak akses khusus adalah akses terhadap sistem informasi sensitif, termasuk di dalamnya dan tidak terbatas pada sistem operasi, perangkat penyimpanan (*storage devices*), *file server*, dan aplikasi-aplikasi sensitif, hanya diberikan kepada pengguna yang membutuhkan dan pemakaiannya terbatas dan dikontrol.
17. *Hash totals* adalah nilai pemeriksa kesalahan yang diturunkan dari penambahan satu himpunan bilangan yang diambil dari data (tidak harus berupa data numerik) yang diproses atau dimanipulasi dengan cara tertentu.
18. Informasi adalah hasil pemrosesan, manipulasi dan pengorganisasian data yang dapat disajikan sebagai pengetahuan.
19. Jejak audit (*audit trails*) adalah urutan kronologis catatan audit yang berkaitan dengan pelaksanaan suatu kegiatan.
20. Kata sandi adalah serangkaian kode yang dibuat Pengguna, bersifat rahasia dan pribadi digunakan bersamaan dengan Akun Pengguna.
21. Keamanan informasi adalah perlindungan aset informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.
22. Komunitas keamanan informasi adalah kelompok/komunitas yang memiliki pengetahuan/keahlian khusus dalam bidang keamanan informasi atau yang relevan dengan kemanan informasi, seperti: Indonesia Security Incident Response Team on Internet and Infrastructure (ID-SIRTII), Unit Cybercrime POLRI, ISC2, ISACA.
23. Koneksi eksternal (remote access) adalah suatu akses jaringan komunikasi dari luar organisasi ke dalam organisasi.
24. Kriptografi adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal untuk meningkatkan keamanan informasi. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi.

25. *Malicious Code* adalah semua macam program yang membahayakan termasuk makro atau script yang dapat diesekusi dan dibuat dengan tujuan untuk merusak sistem komputer.
26. *Master disk* adalah media yang digunakan sebagai sumber dalam melakukan instalasi perangkat lunak.
27. *Mobile Device* adalah penggunaan perangkat komputasi yang dapat dipindah (*portable*) misalnya *notebook* dan *personal data assistant* (PDA) untuk melakukan akses, pengolahan data dan penyimpanan.
28. Penanggung jawab pengendalian dokumen adalah pihak yang memiliki kewenangan dan bertanggung jawab dalam proses pengendalian dokumen Manajemen Keamanan Informasi SPBE.
29. Pengguna adalah pegawai pada Perangkat Daerah atau pihak ketiga serta tidak terbatas pada pengelola Teknologi Informasi dan kelompok kerja yang diberikan hak mengakses sistem Teknologi Informasi di setiap Perangkat Daerah.
30. Pemilik aset informasi adalah unit kerja yang memiliki kewenangan terhadap aset informasi.
31. Penyedia Jasa dan Barang adalah badan usaha atau orang atau perseorangan yang menyediakan barang atau pekerjaan konstruksi/jasa konsultasi/jasa lainnya.
32. Pencatatan waktu (*timestamp*) adalah catatan waktu dalam tanggal dan/atau format waktu tertentu saat suatu aktivitas atau transaksi terjadi. Format ini biasanya disajikan dalam format yang konsisten, yang memungkinkan untuk membandingkan dua aktivitas/transaksi yang berbeda berdasarkan waktu.
33. Perangkat jaringan adalah peralatan jaringan komunikasi data seperti: *modem, hub, switch, router*, dan lain-lain.
34. Perangkat lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya.
35. 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 atau generator, antena komunikasi.
36. Perangkat pengolah informasi adalah setiap sistem pengolah informasi, layanan atau infrastruktur. Contoh perangkat pengolah informasi adalah komputer, faksimili, telepon, mesin fotocopy.
37. Perjanjian *escrow* adalah perjanjian dengan pihak ketiga untuk memastikan apabila pihak ketiga tersebut bangkrut (mengalami *failure*) maka Perangkat Daerah yang bersangkutan berhak untuk mendapatkan kode program (*source code*).
38. Perjanjian kerahasiaan adalah perikatan antara para pihak yang mencantumkan bahan rahasia, pengetahuan, atau informasi yang mana pihak-pihak ingin berbagi satu sama lain untuk tujuan tertentu, tetapi ingin membatasi akses dengan pihak lain.
39. Pihak berwenang adalah pihak yang mempunyai kewenangan terkait suatu hal, seperti: kepolisian, instansi pemadam kebakaran, dan penyedia jasa telekomunikasi atau internet.
40. Pihak ketiga adalah semua unsur di luar pengguna unit Teknologi Informasi yang bukan bagian dari Perangkat Daerah, misal mitra kerja pada Perangkat Daerah (seperti: konsultan, penyedia jasa komunikasi, penyedia jasa/barang dan pemelihara perangkat pengolah informasi), dan kementerian/lembaga lain.

41. Proses pendukung (*support proceses*) adalah proses-proses penunjang yang mendukung suatu proses utama yang terkait. Contoh proses pendukung dalam pengembangan (*development*) adalah proses pengujian perangkat lunak, proses perubahan perangkat lunak.
42. Rencana Kontijensi adalah suatu rencana ke depan pada keadaan yang tidak menentu dengan skenario, tujuan, teknik, manajemen, pelaksanaan, serta sistem penanggulangannya telah ditentukan secara bersama untuk mencegah dan mengatasi keadaan darurat.
43. *Rollback* adalah sebuah mekanisme yang digunakan untuk mengembalikan sistem ke kondisi semula sebelum perubahan diimplementasikan. Mekanisme ini biasanya terdapat pada sistem basis data.
44. *Routing* adalah sebuah mekanisme yang digunakan untuk mengarahkan dan menentukan rute atau jalur yang akan dilewati paket dari satu perangkat ke perangkat yang berada di jaringan lain.
45. Sanitasi adalah proses penghilangan informasi yang disimpan secara permanen dengan menggunakan medan magnet besar atau perusakan fisik.
46. Sistem Manajemen Keamanan Informasi SPBE adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penangung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan keamanan informasi.
47. Sistem informasi adalah serangkaian perangkat keras, perangkat lunak, sumber daya manusia, serta prosedur dan atau aturan yang diorganisasikan secara terpadu untuk mengolah data menjadi informasi yang berguna untuk mencapai suatu tujuan.
48. Sistem TI adalah sistem operasi, sistem surat elektronik, sistem aplikasi, sistem basis data, sistem jaringan intranet/ internet, dan sebagainya.
49. *Subnet* (kependekan dari *sub network*) adalah pengelompokan secara logis dari perangkat jaringan yang terhubung.
50. *System administrator* adalah akun khusus untuk mengelola sistem informasi.
51. *System utilities* adalah sebuah sistem perangkat lunak yang melakukan suatu tugas atau fungsi yang sangat spesifik, biasanya disediakan oleh sistem operasi, dan berkaitan dengan pengelolaan sumber daya sistem (*system resources*), seperti *memory*, *disk*, *printer*, dan sebagainya.
52. *Teleworking* adalah penggunaan teknologi telekomunikasi untuk memungkinkan pegawai bekerja di suatu lokasi yang berada di luar kantor ntuk mengakses jaringan internal kantor.

Pj WALI KOTA PONTIANAK,

ttd

ANI SOFIAN