BUPATI MAPPI
PROVINSI PAPUA

PERATURAN BUPATI MAPPI
NOMOR 09 TAHUN 2023

TENTANG
PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN
INFORMASI PEMERINTAH KABUPATEN MAPPI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MAPPI,

Menimbang : a. bahwa untuk melaksanakan urusan Pemerintahan bidang persandian di daerah diperlukan norma, standar, prosedur dan kriteria;

b. bahwa setiap pemerintah daerah wajib mengelola informasi yang dimilikinya dan untuk melindungi informasi perlu dilakukan upaya pengamanan informasi melalui penyelenggaraan persandian;

c. bahwa berdasarkan Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan daerah sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2022 tentang Hubungan Keuangan antara Pemerintah Pusat dan Pemerintah Daerah, dan untuk melaksanakan Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 Tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, maka Penyelenggaraan Persandian untuk pengamanan Informasi Pemerintah Daerah Kabupaten merupakan urusan Pemerintahan wajib yang tidak berkaitan dengan Pelayanan Dasar yang menjadi kewenangan Pemerintah Daerah Kabupaten perlu diatur dengan Peraturan Bupati;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c perlu menetapkan Peraturan Bupati tentang Pelaksanaan Persandian untuk Pengamanan Informasi Pemerintah Kabupaten Mappi;

Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Republik Indonesia Nomor 3881) sebagaimana telah diubah dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta kerja menjadi Undang-undang;

3. Undang-Undang Nomor 21 Tahun 2001 tentang Otonomi Khusus Bagi Provinsi Papua (Lembaran Negara Republik Indonesia Tahun 2001 Nomor 135, Tambahan Lembaran Negara Republik Indonesia Nomor 4151), sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 2 Tahun 2021 tentang Perubahan Kedua atas Undang-Undang Nomor 21 Tahun 2001 tentang Otonomi Khusus Bagi Provinsi Papua (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 155, Tambahan Lembaran Negara Republik Indonesia Nomor 6697);
4. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lebaran 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);
5. 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);
6. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
7. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234), telah diubah terakhir Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan;
8. 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 terakhir dengan Undang-Undang Nomor 1 Tahun 2022 tentang Hubungan Keuangan antara Pemerintah Pusat dan Pemerintah Daerah (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6757);
9. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601) sebagaimana telah diubah dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta kerja menjadi Undang-undang;

10. Undang-Undang Nomor 14 Tahun 2022 tentang Pembentukan Provinsi Papua Selatan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 157, Tambahan Lembaran Negara Republik Indonesia Nomor 6803);
11. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelengaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
12. Peraturan Pemerintah Nomor 106 Tahun 2021 Tentang Kewenangan dan Kelembagaan Pelaksanaan Kebijakan Otonomi Khusus Provinsi Papua (Lembaran Negara Tahun 2021 Nomor 238, Tambahan Lembaran Negara Nomor 6730);
13. Peraturan Pemerintah Nomor 107 Tahun 2021 Tentang Penerimaan, Pengelolaan, Pengawasan dan Rencana Induk Percepatan Pembangunan Dalam Rangka Pelaksanaan Otonomi Khusus Provinsi Papua (Lembaran Negara Tahun 2021 Nomor 239, Tambahan Lembaran Negara Nomor 6731);
14. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);
15. Peraturan Presiden Nomor 79 Tahun 2008 tentang Tunjangan Pengamanan Persandian;
16. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
17. Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik (Berita Negara Republik Indonesia Tahun 2022 Nomor 1017);
18. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi Di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
19. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);
20. 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);
21. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2021 tentang Penyelenggaraan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001 Menggunakan Indeks Keamanan Informasi (Berita Negara Republik Indonesia Tahun 2021 Nomor 975);

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI PEMERINTAH KABUAPATEN MAPPI.

BAB I

KETENTUAN UMUM

Pasal 1

1. Daerah adalah Kabupaten Mappi;
2. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan Kabupaten Mappi.
3. Pemerintahan Daerah adalah penyelenggaraan urusan pemerintah oleh Pemerintah Daerah dan Dewan Perwakilan Rakyat Daerah menurut asas otonomi dan tugas pembantuan dengan prinsip otonomi seluas-luasnya dalam sisten dan prinsip Negara Kesatuan Republik Indonesia sebagaimana dimaksud pada undang-undang dasar Negara Republik Indonesia Tahun 1945.
4. Bupati adalah Bupati Mappi.
5. Wakil Bupati adalah Wakil Bupati Mappi.
6. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
7. Dinas Komunikasi dan Informasi Kabupaten Mappi yang selanjutnya disebut Dinas adalah Perangkat Daerah yang Menyelenggarakan urusan dibidang Komunikasi dan Informatika, Statistik, dan Persandian.
8. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.
9. Balai Sertifikasi Elektronik yang selanjutnya disebut BSrE merupakan unit pelaksana teknis penyelenggara Otoritas Sertifikat Digital BSSN yang berada di bawah dan bertanggung jawab kepada Kepala BSSN.
10. Dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya yang dapat dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memilki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
11. Informasi Publik adalah informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelengara dan penyelenggaraan negara dan/atau penyelenggara dan penyelenggaraan badan publik lainnya yang sesuai dengan Undang-Undang serta informasi lainnya yang berkaitan dengan kepentingan publik.

12. Jaring komunikasi sandi adalah keterhubungan antar pengguna persandian melalui jaring telekomunikasi.
13. Keamanan informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan informasi.
14. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data.
15. Layanan keamanan informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan urusan pemerintahan bidang persandian dan yang memiliki nilai manfaat.
16. Otoritas Sertifikat Digital yang selanjutnya disingkat OSD adalah sistem penyelenggaraan sertifikasi elektronik secara keseluruhan atau salah satu/beberapa sistem penyelengaraan sertifikasi elektronik.
17. Pengamanan informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan keamanan informasi.
18. Pengguna layanan keamanan informasi yang selanjutnya disebut pengguna layanan adalah para pihak yang memanfaatkan layanan keamanan informasi
19. Persandian adalah kegiatan di bidang pengamanan data/informasi yang dilaksanakan dengan menerapkan konsep, teori, seni dan ilmu kripto beserta ilmu pendukung lainnya secara sistematis, metodologis dan konsisten serta terkait pada etika profesi sandi.
20. Pola hubungan komunikasi sandi adalah bentuk atau pola hubungan antara dua entitas atau lebih dalam proses pengiriman dan penerimaan informasi/pesan/berita secara aman menggunakan persandian.
21. Sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
22. 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 BSrE.
23. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah Penyelenggaraan Pemerintahan yang Memanfaatkan Teknologi Informasi dan Komunikasi untuk Memberikan Layanan kepada Pengguna SPBE.
24. Penanda tangan adalah gelar yang digunakan untuk menggambarkan seseorang yang telah menandatangani atau akan menandatangani semacam dokumen atau hal lain.
25. 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.

BAB II
MAKSUD, TUJUAN DAN RUANG LINGKUP

Pasal 2

Pelaksanaan persandian untuk pengamanan informasi Pemerintah Kabupaten Mappi bertujuan untuk:

a. menciptakan harmonisasi dalam melaksanakan persandian untuk pengamanan informasi antara Pemerintah Pusat dan Pemerintah Daerah;
b. meningkatkan komitmen, efektivitas, dan kinerja dalam melaksanakan kebijakan, program dan kegiatan pelaksanaan persandian untuk pengamanan informasi; dan
c. memberikan pedoman dalam menetapkan pola hubungan komunikasi sandi antar Perangkat Daerah.

Pasal 3

Pelaksanaan persandian untuk pengamanan informasi sebagaimana dimaksud dalam Pasal 2 meliputi:

a. penyelenggaraan persandian untuk pengamanan informasi; dan
b. penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.

Pasal 4

Ruang lingkup dari Peraturan Bupati ini adalah:

a. penyelenggaraan persandian untuk pengamanan informasi; dan
b. penetapan pola hubungan komunikasi sandi antar perangkat daerah.

BAB III
PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

Bagian Kesatu
Umum

Pasal 5

(1) Penyelenggaraan persandian untuk pengamanan informasi sebagaimana dimaksud dalam Pasal 3 huruf a dilaksanakan melalui:
    a. penyusunan kebijakan pengamanan informasi;
    b. pengelolaan sumber daya keamanan informasi;
    c. pengamanan sistem elektronik dan pengamanan informasi non elektronik; dan
    d. penyediaan layanan keamanan informasi.
(2) Pelaksanaan penyelenggaraan persandian untuk pengamanan informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Perangkat Daerah.

Bagian Kedua
Penyusunan Kebijakan Pengamanan Informasi

Pasal 6

Penyusunan kebijakan pengamanan informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf a dilakukan dengan:
a. menyusun rencana strategis pengamanan informasi;
b. menetapkan arsitektur keamanan informasi; dan
c. menetapkan aturan mengenai tata kelola keamanan informasi.

Pasal 7

(1) Penyusunan rencana strategis pengamanan informasi sebagaimana dimaksud dalam Pasal 6 huruf a terdiri atas:
    a. tujuan, sasaran, program, kegiatan dan target pelaksanaan pengamanan informasi setiap tahun untuk jangka waktu 5 (lima) tahun; dan
    b. peta rencana penyelenggaraan pengamanan informasi yang merupakan penjabaran dari tahapan rencana strategis yang akan dicapai setiap tahun untuk jangka waktu 5 (lima) tahun.
(2) Rencana strategis pengamanan informasi yang telah disusun sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah (RPJMD).
(3) Perangkat Daerah dalam melakukan penyusunan rencana strategis pengamanan informasi sebagaimana dimaksud pada ayat (1) dapat melakukan koordinasi dan konsultasi kepada BSSN.

Pasal 8

(1) Arsitektur keamanan informasi sebagaimana dimaksud dalam Pasal 6 huruf b memuat:
    a. infrastruktur teknologi informasi;
    b. desain keamanan perangkat teknologi informasi dan keamanan jaringan; dan
    c. aplikasi keamanan perangkat teknologi informasi dan keamanan jaringan.
(2) Perangkat Daerah dalam menetapkan arsitektur keamanan informasi sebagaimana dimaksud pada ayat (1) dapat melakukan koordinasi dan konsultasi kepada BSSN.
(3) Arsitektur keamanan informasi yang telah ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.
(4) Arsitektur keamanan informasi dilakukan evaluasi oleh Bupati pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu waktu sesuai dengan kebutuhan.

Pasal 9

(1) Penetapan aturan mengenai tata kelola keamanan informasi sebagaimana dimaksud dalam Pasal 6 huruf c paling sedikit terdiri atas:
   a. keamanan sumber daya teknologi informasi;
   b. keamanan akses kontrol;
   c. keamanan data dan informasi;
   d. keamanan sumber daya manusia;
   e. keamanan jaringan;
   f. keamanan surat elektronik;
   g. keamanan pusat data; dan/atau
   h. keamanan komunikasi.

(2) Perangkat Daerah dalam menetapkan aturan mengenai tata kelola keamanan informasi sebagaimana dimaksud pada ayat (1) dapat melakukan koordinasi dan konsultasi kepada BSSN melalui Dinas.

Pasal 10

(1) Keamanan sumber daya teknologi informasi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a meliputi:
   a. aspek keamanan dan keberlangsungan sistem; dan
   b. mekanisme dasar.

(2) Aspek keamanan dan keberlangsungan sistem sebagaimana dimaksud pada ayat (1) huruf a yang harus terpenuhi meliputi:
   a. *confidentiality*, akses terhadap data/informasi dibatasi hanya bagi mereka yang punya otoritas;
   b. *integrity,* data tidak boleh diubah tanpa ijin dari yang berhak;
   c. *authentication*, untuk meyakinkan identitas pengguna sistem; dan
   d. *availability*, terkait dengan ketersediaan layanan, termasuk *up-time* dari sistem dan teknologi informasi; dan
   e. *non-repudiation*, terkait penerapan tanda tangan digital dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat digital.

(3) Mekanisme dasar sebagaimana dimaksud pada ayat (1) huruf b untuk memastikan tercapainya aspek-aspek keamanan dan keberlangsungan sistem yang harus terpenuhi meliputi:
   a. pengamanan dari sisi software aplikasi; dan
   b. pengamanan dari sisi infrastruktur teknologi.

(4) Pengamanan dari sisi software aplikasi sebagaimana dimaksud pada ayat (3) huruf a dapat diimplementasikan melalui:
   a. metode *scripting* software aplikasi yang aman;
   b. implementasi mekanisme autentikasi dan otorisasi di dalam software aplikasi yang tepat; dan
   c. pengaturan keamanan sistem basis data yang tepat.

(5) Pengamanan dari sisi infrastruktur teknologi sebagaimana dimaksud pada ayat (3) huruf b dapat diimplementasikan melalui:
   a. hardening dari sisi sistem operasi;
   b. *firewall*, sebagai pagar untuk menghadang ancaman dari luar sistem;
   c. *Intrusion Detection System/ Intrution-Prevention Systems* (IDS/IPS), sebagai pendeteksi atau pencegah aktivitas ancaman terhadap sistem;
   d. *network monitoring tool*, sebagai usaha untuk melakukan monitoring atas aktivitas di dalam jaringan; dan
   e. *log processor and analysis*, untuk melakukan pendeteksian dan analisis kegiatan yang terjadi di sistem.

(6) Dalam hal sumber daya teknologi informasi dan komunikasi yang kritikal, pengamanan dapat ditempuh melalui penyediaan sistem cadangan yang dapat secara cepat mengambil alih sistem utama jika terjadi gangguan ketersediaan pada sistem utama.

(7) Dalam hal evaluasi keamanan sumber daya teknologi informasi, *assessment* kerentanan keamanan sistem dapat dilakukan secara teratur sesuai dengan kebutuhan.

Pasal 11

(1) Keamanan akses kontrol sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf b meliputi:
   a. persyaratan organisasi untuk kendali akses;
   b. manajemen akses pengguna;
   c. tanggung jawab pengguna; dan
   d. kendali akses sistem dan aplikasi.

(2) Persyaratan organisasi untuk kendali akses sebagaimana dimaksud pada ayat (1) huruf a meliputi:
   a. kebijakan kendali akses, bahwa kebijakan kendali akses harus ditetapkan, didokumentasikan dan direviu berdasarkan persyaratan organisasi dan kemanan informasi; dan
   b. akses ke jaringan dan layanan jaringan, bahwa pengguna hanya akan disediakan akses ke jaringan dan layanan jaringan yang telah secara khusus diberi wewenang untuk digunakan.

(3) Manajemen akses pengguna sebagaimana dimaksud pada ayat (1) huruf b meliputi:
   a. registrasi dan pembatalan registrasi pengguna, bahwa proses registrasi dan pembatalan registrasi pengguna yang resmi harus diimplementasikan untuk mengaktifkan penetapan hak akses;
   b. penyediaan akses pengguna, bahwa proses penyediaan akses pengguna yang resmi harus diimplementasikan untuk menetapkan atau mencabut hak akses untuk semua tipe pengguna ke semua sistem dan layanan;

c. manajemen hak akses istimewa, bahwa pengalokasian dan penggunaan hak akses istimewa harus dibatasi dan dikendalikan;
d. manajemen informasi autentikasi rahasia dari pengguna, bahwa alokasi dari informasi autentikasi rahasia harus dikendalikan melalui proses manajemen resmi;
e. reviu hak akses pengguna, bahwa pemilik aset harus mereviu hak akses pengguna secara periodik; dan
f. penghapusan atau penyesuaian hak akses, bahwa hak akses semua pegawai dan pengguna pihak eksternal pada informasi dan fasilitas pengolahan informasi harus dihapus sewaktu terjadi penghentian kepegawaian, kontrak, atau perjanjian, atau disesuaikan atas perubahan yang terjadi.

(4) Tanggung jawab pengguna sebagaimana dimaksud pada ayat (1) huruf c berkenaan dengan penggunaan informasi autentikasi rahasia, bahwa pengguna harus mengikuti praktik organisasi dalam penggunaan informasi autentikasi rahasia.

(5) Kendali akses sistem dan aplikasi sebagaimana dimaksud pada ayat (1) huruf d meliputi:
a. pembatasan akses informasi, bahwa akses ke informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan kendali akses;
b. prosedur *log-on* yang aman, bahwa ketika disyaratkan oleh kebijakan pengendalian akses, akses ke sistem dan aplikasi harus dikendalikan oleh prosedur *log-on* yang aman;
c. sistem manajemen kata kunci, bahwa sistem manajemen kata kunci harus interaktif dan manajemen kualitas kata kunci;
d. penggunaan program utilitas istimewa, bahwa penggunaan program utilitas yang mungkin mampu membatalkan kendali sistem dan aplikasi harus dibatasi dan dikendalikan secara ketat; dan
e. kendali akses ke kode sumber program, bahwa akses ke kode sumber program harus dibatasi.

Pasal 12

(1) Keamanan data dan informasi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c dilaksanakan melalui perlindungan informasi berklasifikasi, mencakup:
a. perlindungan fisik, dilakukan untuk melindungi keberadaan dan fungsi sarana fisik komunikasi serta segala kegiatan yang berlangsung di dalamnya dari ancaman dan gangguan seperti pencurian, perusakan dan radiasi gelombang elektromagnetik;
b. perlindungan administrasi, dilakukan untuk mencegah kelalaian dan tindakan indisipliner; dan
c. perlindungan *logical*, dilakukan dengan menggunakan perlindungan *logical* menggunakan teknik kriptografi dan steganografi untuk memenuhi aspek kerahasiaan, keutuhan, autentikasi dan kenirsangkalan.

(2) Perlindungan fisik sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui:
   a. kendali akses ruang;
   b. pemasangan teralis;
   c. penggunaan kunci ganda;
   d. pemasangan CCTV; dan/atau
   e. penggunaan ruang TEMPEST.

(3) Perlindungan administrasi sebagaimana dimaksud pada ayat (1) huruf b dituangkan dalam bentuk peraturan tertulis yang menerangkan kebijakan, standar dan prosedur operasional dalam pengamanan informasi berklasifikasi.

(4) Perlindungan *logical* sebagaimana dimaksud pada ayat (1) huruf c harus memenuhi standar dan direkomendasikan oleh BSSN.

Pasal 13

(1) Keamanan sumber daya manusia sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf d mencakup:
   a. sumber daya manusia sebelum dipekerjakan;
   b. sumber daya manusia selama bekerja; dan
   c. sumber daya manusia saat penghentian dan perubahan kepegawaian.

(2) Keamanan sumber daya manusia sebelum dipekerjakan sebagaimana dimaksud pada ayat (1) huruf a dilaksanakan untuk memastikan bahwa Perangkat Daerah menyadari dan memenuhi tanggung jawab keamanan informasi mereka, meliputi:
   a. penyaringan, bahwa verifikasi latar belakang dari semua calon pegawai harus dilaksanakan berdasarkan undang-undang terkait dan harus proporsional terhadap persyaratan Pemerintah Daerah, klasifikasi informasi yang akan diakses dan risiko yang dipersepsikan; dan
   b. syarat dan ketentuan kepegawaian, bahwa perjanjian tertulis dengan Pemerintah Daerah harus menyatakan tanggung jawab keamanan informasi.

(3) Keamanan sumber daya manusia selama bekerja sebagaimana dimaksud pada ayat (1) huruf b dilaksanakan untuk memastikan bahwa Perangkat Daerah menyadari dan memenuhi tanggung jawab keamanan informasi mereka, meliputi:
   a. tanggung jawab manajemen;
   b. kepedulian, pendidikan, dan pelatihan keamanan informasi; dan
   c. proses pendisiplinan.

(4) Keamanan sumber daya manusia saat penghentian dan perubahan kepegawaian sebagaimana dimaksud pada ayat (1) huruf c dilaksanakan untuk melindungi kepentingan organisasi sebagai bagian dari proses perubahan atau penghentian kepegawaian, dengan cara penghentian atau perubahan tanggung jawab kepegawaian.

Pasal 14

(1) Keamanan jaringan sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf e dilaksanakan untuk menjamin perlindungan informasi dalam jaringan dan fasilitas pendukung pengolahan informasi.
(2) Keamanan jaringan sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf e dilaksanakan melalui:
    a. kendali jaringan, bahwa jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi;
    b. keamanan layanan jaringan, bahwa mekanisme jaringan, tingkat layanan dan persyaratan manajemen dari semua layanan jaringan harus diidentifikasi dan dimasukkan dalam perjanjian layanan jaringan; dan
    c. pemisahan dalam jaringan, bahwa kelompok layanan informasi, pengguna dan sistem informasi harus dipisahkan pada jaringan.

Pasal 15

(1) Keamanan surat elektronik sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf f dilaksanakan melalui pemanfaatan layanan sertifikat elektronik.
(2) Pemanfaatan layanan sertifikat elektronik sebagaimana dimaksud pada pasal (1) dilakukan melalui:
    a. pelaksanaan verifikasi identitas dan berkas untuk pendaftaran, pembaruan dan pencabutan sertifikat elektronik;
    b. pengembangan aplikasi pendukung penggunaan sertifikat elektronik;
    c. fasilitasi kegiatan sosialisasi dan bimbingan teknis terkait sertifikat elektronik; dan
    d. pengawasan dan evaluasi penggunaan sertifikat elektronik.
(3) Pelaksanaan verifikasi identitas dan berkas untuk pendaftaran, pembaruan dan pencabutan sertifikat elektronik sebagaimana dimaksud pada ayat (2) huruf a, meliputi:
    a. menangani verifikasi identitas berdasarkan identitas resmi, keanggotaan pada instansi, dan rekomendasi dari instansi;
    b. menyetujui/menolak permintaan pendaftaran sertifikat elektronik;
    c. menindaklanjuti permintaan sertifikat elektronik kepada BSrE;
    d. menyampaikan sertifikat elektronik kepada pemohon; dan
    e. melakukan pengarsipan berkas pendaftaran sertifikat elektronik *(hardcopy and softcopy)*.

Pasal 16

(1) Keamanan pusat data sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf g meliputi kontrol akses dan keamanan fisik dan *logical*.

(2) Kontrol akses dan keamanan fisik dan *logical* pusat data sebagaimana dimaksud pada ayat (1) wajib memenuhi persyaratan sebagai berikut:
   a. memiliki pengaman fisik di setiap jendela yang memungkinkan akses langsung ke pusat data;
   b. memastikan setiap sumber daya manusia di pusat data memiliki pengetahuan dan kesadaran yang cukup terhadap keamanan fisik pusat data;
   c. melakukan pengamanan pusat data selama 24 (dua puluh empat) jam dengan jumlah petugas paling sedikit 2 (dua) orang per *shift*;
   d. memasang perangkat sistem pemantau visual yang berfungsi untuk memantau dan merekam setiap aktivitas pada ruang komputer, ruang mekanik dan kelistrikan, ruang telekomunikasi dan kawasan kantor;
   e. menggunakan sistem akses elektronik dan sistem pengawasan (surveillance) yang dikendalikan dengan mekanisme autentikasi yang berfungsi untuk mencegah dan menanggulangi akses fisik tanpa izin terhadap fasilitas, peralatan dan sumber daya dalam ruang komputer;
   f. memastikan setiap tamu/pengunjung memiliki izin dan dilengkapi dengan tanda masuk serta tanda pengenal untuk dapat masuk ke ruang komputer, ruang mekanikal dan kelistrikan, ruang telekomunikasi dan kawasan kantor; dan
   g. melengkapi pusat data dengan sistem audit *trail* untuk pencatatan akses fisik dan akses *logical* yang terjadi.

Pasal 17

(1) Keamanan komunikasi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf g mencakup keamanan perpindahan informasi.
(2) Perpindahan informasi sebagaimana dimaksud pada ayat (1) dilaksanakan untuk memelihara keamanan informasi yang dipindahkan antar Perangkat Daerah ataupun pihak luar.
(3) Perpindahan informasi sebagaimana dimaksud pada ayat (1) dilaksanakan melalui:
   a. prosedur dan kebijakan perpindahan informasi, bahwa kebijakan, prosedur dan kendali perpindahan yang resmi harus ada untuk melindungi perpindahan informasi melalui penggunaan semua jenis fasilitas komunikasi;
   b. perjanjian perpindahan informasi, bahwa perjanjian harus mengatur perpindahan informasi yang aman antara Perangkat Daerah dan pihak luar;
   c. pesan elektronik, bahwa informasi yang terdapat dalam pesan elektronik harus dilindungi dengan tepat; dan

d. perjanjian kerahasiaan atau menjaga rahasia, bahwa persyaratan untuk perjanjian kerahasiaan atau menjaga rahasia mencerminkan kebutuhan Pemerintah Daerah untuk perlindungan informasi harus diidentifikasi, direviu secara teratur dan didokumentasikan.

Bagian Ketiga
Pengelolaan Sumber Daya Keamanan Informasi

Pasal 18

Pengelolaan sumber daya keamanan informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf b terdiri atas:
a. pengelolaan aset keamanan teknologi informasi dan komunikasi;
b. pengelolaan sumber daya manusia; dan
c. manajemen pengetahuan.

Pasal 19

(1) Pengelolaan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 18 huruf a dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.
(2) Aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (1) merupakan perangkat yang digunakan untuk mengidentifikasi, mendeteksi, memproteksi, menganalisis, menanggulangi, dan/atau memulihkan insiden keamanan informasi dalam sistem elektronik.

Pasal 20

(1) Perangkat Daerah merumuskan rencana kebutuhan aset keamanan teknologi informasi dan komunikasi dan menetapkannya sebagai aset keamanan teknologi informasi dan komunikasi Pemerintah Daerah.
(2) Perumusan rencana aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud pada ayat (1) harus berdasarkan pada aset keamanan teknologi Informasi dan komunikasi yang telah direkomendasikan oleh BSSN.
(3) Hasil penetapan aset keamanan teknologi Informasi dan komunikasi diajukan Perangkat Daerah melalui Dinas kepada BSSN untuk permohonan pemenuhan peralatan sandi kebutuhan Pemerintah Daerah.

Pasal 21

(1) Perangkat Daerah berkewenangan untuk melakukan pengajuan terkait pengadaan aset keamanan teknologi Informasi dan komunikasi.
(2) Pengadaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan prinsip efisien, efektif, transparan & terbuka, bersaing, adil, dan akuntabel.

Pasal 22

(1) Perangkat Daerah melakukan pemanfaatan aset keamanan teknologi informasi dan komunikasi untuk kepentingan pengamanan informasi.
(2) Pemanfaatan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud pada ayat (1) dilaksanakan melalui :
    a. penggunaan aset keamanan teknologi Informasi dan komunikasi;
    b. pemeliharaan aset keamanan teknologi Informasi dan komunikasi;
    c. perbaikan aset keamanan teknologi Informasi dan komunikasi;
    d. pendistribusian aset keamanan teknologi Informasi dan komunikasi; dan
    e. pengawasan dan pengendalian aset keamanan teknologi Informasi dan komunikasi.
(3) Penggunaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud pada ayat (2) huruf a meliputi:
    a. materiil sandi;
    b. tempat kegiatan sandi; dan
    c. alat pendukung utama (APU) Persandian.
(4) Pemeliharaan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksudkan pada ayat (2) huruf b mencakup:
    a. memastikan peralatan sandi bebas dari debu/kotoran atau benda lain yang memicu gangguan operasional peralatan sandi;
    b. menjaga ketersediaan dan kestabilan arus listrik sesuai persyaratan pada peralatan sandi;
    c. menjaga dan memonitor ketersediaan koneksi saluran telekomunikasi pada peralatan sandi;
    d. memastikan peralatan sandi dapat berfungsi sebagaimana mestinya;
    e. menjaga kestabilan suhu ruangan tempat peletakkan peralatan sandi;
    f. meletakkan peralatan sandi pada tempat yang aman dari kemungkinan bencana, pencurian, dan kehilangan;
    g. memastikan kelengkapan perangkat; dan
    h. memastikan kelengkapan dokumen serah terima barang, berita acara serah terima dan/atau penarikan.
(5) Perbaikan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (2) huruf c dilakukan melalui perbaikan umum, yang merupakan perbaikan yang tidak berkaitan dengan aspek kriptografis, dilakukan oleh Perangkat Daerah dengan berkoordinasi dengan BSSN.
(6) Pendistribusian aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (2) huruf d wajib memperhatikan ketentuan sebagai berikut:
    a. dilengkapi dengan berita acara penyerahan;
    b. terjamin keamanan dan keutuhannya sehingga terhindar dari kehilangan dan kerusakan; dan
    c. dalam keadaan netral atau non aktif (tidak terisi kunci sistem sandi).

(7) Pengawasan dan pengendalian aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud pada ayat (2) huruf e harus dilakukan secara menyeluruh, terus menerus, dan berkesinambungan.

Pasal 23

(1) Perangkat Daerah melakukan pengajuan terkait penghapusan aset keamanan teknologi informasi dan komunikasi berdasarkan prinsip kehati-hatian dan ketepatan.
(2) Penghapusan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (1) meliputi:
    a. penghapusan dari daftar barang pengguna dan/atau daftar barang kuasa pengguna; dan
    b. penghapusan dari daftar barang milik daerah.

Pasal 24

(1) Penghapusan dari daftar barang pengguna dan/atau daftar barang kuasa pengguna sebagaimana dimaksud dalam Pasal 23 ayat (2) huruf a dilakukan dalam hal barang milik daerah sudah tidak berada dalam penguasaan Pemerintah Daerah.
(2) Penghapusan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (1) dilakukan dengan menerbitkan keputusan penghapusan dari Kepala Perangkat Daerah setelah mendapatkan persetujuan dari Bupati untuk barang milik daerah dan BSSN untuk barang milik negara.
(3) Penghapusan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud pada ayat (1) dilakukan karena:
    a. pengalihan status penggunaan;
    b. pemindahtanganan; atau
    c. pemusnahan.
(4) Bupati melalui Perangkat Daerah dapat mendelegasikan persetujuan penghapusan aset keamanan teknologi Informasi dan komunikasi kepada BSSN.
(5) Penghapusan aset keamanan teknologi Informasi dan komunikasi dilaporkan kepada BSSN.

Pasal 25

(1) Penghapusan dari daftar barang milik sebagaimana dimaksud dalam Pasal 23 ayat (2) huruf b dilakukan dalam hal barang milik daerah sudah beralih kepemilikannya, terjadi pemusnahan, atau karena sebab lain.
(2) Penghapusan dari daftar barang milik daerah sebagaimana dimaksud pada ayat (1) dilakukan berdasarkan keputusan dan/atau laporan penghapusan dari Kepala Perangkat Daerah.

Pasal 26

Ketentuan lebih lanjut teknis pengelolaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud dalam Pasal 19 ayat (1) ditetapkan oleh Kepala Perangkat

Daerah dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 27

Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 18 huruf b dilakukan melalui serangkaian proses sebagai berikut:
a. pengembangan kompetensi;
b. pembinaan karir;
c. pendayagunaan; dan
d. pemberian tunjangan pengamanan persandian.

Pasal 28

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 27 huruf a dilaksanakan dengan ketentuan:
    a. melalui tugas belajar, pendidikan dan pelatihan pembentukan dan penjenjangan fungsional, pendidikan dan pelatihan teknis, bimbingan teknis, asistensi, *workshop*, seminar dan kegiatan lainnya yang terkait pengembangan kompetensi sumber daya manusia di bidang keamanan informasi;
    b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, pihak lainnya, atau Pemerintah Daerah; dan
    c. memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi bidangnya.
(2) Pembinaan karir sebagaimana dimaksud dalam Pasal 27 huruf b dilaksanakan dengan ketentuan:
    a. pembinaan jabatan fungsional di bidang keamanan informasi; dan
    b. pengisian formasi jabatan pimpinan tinggi, jabatan administrator, dan jabatan pengawas sesuai dengan standar kompetensi yang ditetapkan.
(3) Pendayagunaan sebagaimana dimaksud dalam Pasal 27 huruf c dilaksanakan agar seluruh sumber daya manusia yang bertugas di Perangkat Daerah melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan.
(4) Pemberian tunjangan pengamanan persandian sebagaimana dimaksudkan dalam Pasal 27 huruf d meliputi tunjangan pengamanan persandian dan tunjangan jabatan fungsional sandiman.

Pasal 29

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 18 huruf c dilakukan untuk meningkatkan kualitas layanan keamanan informasi dan mendukung proses pengambilan keputusan terkait Keamanan Informasi.
(2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan keamanan informasi Pemerintah Daerah.
(3) Manajemen pengetahuan sebagaimana dimaksud pada

ayat (2) dilaksanakan berdasarkan pedoman manajemen pengetahuan keamanan informasi Pemerintah Daerah.

(4) Perangkat Daerah dalam melaksanakan manajemen pengetahuan sebagaimana dimaksud pada ayat (1), dapat berkoordinasi dan melakukan konsultasi dengan BSSN.

Pasal 30

(1) Pengumpulan pengetahuan dan teknologi sebagaimana dimaksud dalam Pasal 29 ayat (2) dilakukan untuk kategori pengetahuan, meliputi:
   a. pengetahuan implisit; dan
   b. pengetahuan eksplisit.

(2) Pengetahuan implisit sebagaimana dimaksud pada ayat (1) huruf a merupakan pengetahuan yang masih berada dalam pikiran individu yang memiliki pengetahuan tersebut.

(3) Pengetahuan eksplisit sebagaimana dimaksud pada ayat (1) huruf b merupakan pengetahuan yang sudah secara eksplisit diutarakan dan tersedia dalam organisasi.

(4) Pengumpulan pengetahuan dan teknologi sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses untuk mengetahui aset pengetahuan dan teknologi yang dimiliki Pemerintah Daerah berupa produk/layanan, portofolio proyek, data, database kompetensi organisasi, literatur (buku, majalah, laporan), dan sebagainya.

(5) Pengetahuan yang telah terkumpul dan teridentifikasi kemudian diprioritaskan implementasinya menjadi ruang lingkup.

Pasal 31

(1) Pengolahan pengetahuan dan teknologi sebagaimana dimaksud dalam Pasal 29 ayat (2) dilakukan dengan mengintegrasikan pengetahuan lainnya.

(2) Pengolahan pengetahuan dan teknologi sebagaimana dimaksud pada ayat (1) juga dapat dilakukan dengan membagi pengetahuan berdasarkan kompetensi atau kategori tertentu sesuai dengan ketentuan oleh Pemerintah Daerah.

Pasal 32

(1) Penyimpanan pengetahuan dan teknologi sebagaimana dimaksud dalam Pasal 29 ayat (2) direkam dan disimpan ke dalam *database* pengetahuan organisasi.

(2) Perangkat Daerah wajib mendokumentasikan penyimpanan pengetahuan dan teknologi sebagaimana dimaksud pada ayat (1).

Pasal 33

(1) Penggunaan pengetahuan dan teknologi sebagaimana dimaksud dalam Pasal 29 ayat (2) diwujudkan dalam prosedur atau peraturan untuk mengarahkan ke perilaku pada masa yang akan datang.
(2) Penggunaan pengetahuan dan teknologi sebagaimana dimaksud pada ayat (1) dapat melakukan aktivitas pengembangan dan penyempurnaan lebih lanjut dari pengetahuan yang telah didapatkan.

Pasal 34

(1) Alih pengetahuan dan teknologi sebagaimana dimaksud dalam Pasal 29 ayat (2) dapat berlangsung secara tradisional maupun dengan menggunakan teknologi pendukung.
(2) Pemerintah Daerah wajib menjamin terjadinya alih pengetahuan dan teknologi sebagaimana dimaksud pada ayat (1) antar Perangkat Daerah yang membutuhkan.
(3) Alih pengetahuan dan teknologi sebagaimana dimaksud pada ayat (1) dilakukan melalui:
    a. pendidikan dan pelatihan kerja sesuai dengan kualifikasi jabatan yang diduduki; dan
    b. pelaksanaan pelatihan atau pengajaran dalam jangka waktu tertentu.

Pasal 35

Ketentuan lebih lanjut teknis manajemen pengetahuan sebagaimana dimaksud dalam Pasal 29 ayat (2) ditetapkan oleh Kepala Perangkat Daerah dengan berpedoman pada ketentuan peraturan perundang-undangan.

Bagian Keempat
Pengamanan Sistem Elektronik dan Pengamanan Informasi Non Elektronik

Pasal 36

Pengamanan sistem elektronik sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf c terdiri atas:
a. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian dan nirsangkal terhadap data dan informasi;
b. penjaminan ketersediaan infrastruktur yang terdiri atas pusat data, jaringan intra pemerintah dan sistem penghubung layanan penyelenggaraan pemerintahan berbasis elektronik; dan
c. penjaminan keutuhan, ketersediaan dan keaslian aplikasi.

Pasal 37

(1) Pengamanan sistem elektronik sebagaimana dimaksud dalam Pasal 36, dilaksanakan dengan melakukan:
   a. identifikasi;
   b. deteksi;
   c. proteksi; dan
   d. penanggulangan dan pemulihan.
(2) Identifikasi sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui analisis kerawanan dan risiko terhadap sistem elektronik.
(3) Deteksi sebagaimana dimaksud pada ayat (1) huruf b dilakukan melalui analisis untuk menentukan adanya ancaman atau kejadian insiden pada sistem elektronik.
(4) Proteksi sebagaimana dimaksud pada ayat (1) huruf c dilakukan dengan mitigasi risiko dan penerapan pelindungan terhadap sistem elektronik untuk menjamin keberlangsungan Penyelenggaraan Pemerintahan Berbasis Elektronik.
(5) Penanggulangan dan pemulihan sebagaimana dimaksud pada ayat (1) huruf d dilakukan dengan penanganan yang tepat dan perbaikan terhadap adanya insiden pada sistem elektronik agar Penyelenggaraan Pemerintahan Berbasis Elektronik berfungsi kembali dengan baik.

Pasal 38

(1) Pengamanan sistem elektronik sebagaimana dimaksud dalam Pasal 36, wajib menggunakan Sertifikat Elektronik pada setiap layanan publik dan layanan pemerintahan berbasis elektronik.
(2) Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) diterbitkan oleh BSSN dan/atau lembaga penyelenggara sertifikasi elektronik dalam negeri yang telah diakui.
(3) Sertifikat elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 39

(1) Penyelenggaraan layanan publik dan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 38 ayat (1) dilakukan oleh pusat operasi pengamanan informasi sesuai standar yang ditetapkan oleh BSSN.
(2) Pusat operasi pengamanan informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk pengamanan sistem elektronik dengan melakukan proses pengawasan, penanggulangan dan pemulihan atas insiden keamanan sistem elektronik dengan memperhatikan aspek personel, proses pelaksanaan dan ketersediaan teknologi.
(3) Ketentuan lebih lanjut teknis penyelenggaraan pusat operasi Pengamanan Informasi sebagaimana dimaksud pada ayat (1) ditetapkan oleh Kepala Perangkat Daerah dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 40

(1) Pengamanan informasi non elektronik sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf c dilakukan pada

tahapan pemrosesan, pengiriman, penyimpanan dan pemusnahan informasi non elektronik.

(2) Ketentuan lebih lanjut teknis pengamanan informasi nonelektronik sebagaimana dimaksud pada ayat (1) ditetapkan oleh Kepala Perangkat Daerah dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 41

(1) Perangkat Daerah melaksanakan audit keamanan informasi yang meliputi audit keamanan sistem elektronik dan audit pelaksanaan sistem manajemen.

(2) Ketentuan lebih lanjut teknis pelaksanaan audit keamanan informasi sebagaimana dimaksud pada ayat (1) ditetapkan oleh Kepala Perangkat Daerah dengan berpedoman pada ketentuan peraturan perundang-undangan.

Bagian Kelima
Penyediaan Layanan Keamanan Informasi

Pasal 42

Penyediaan layanan keamanan informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf d untuk pengguna layanan yang terdiri atas:

a. Bupati dan Wakil Bupati;
b. Perangkat Daerah;
c. pegawai atau aparatur sipil negara pada Pemerintah Daerah; dan
d. pihak lainnya.

Pasal 43

Penyediaan layanan keamanan informasi sebagaimana dimaksud dalam Pasal 42 meliputi:

a. identifikasi kerentanan dan penilaian risiko terhadap sistem elektronik;
b. asistensi dan fasilitasi penguatan keamanan sistem elektronik;
c. penerapan sertifikat elektronik untuk melindungi sistem elektronik dan dokumen elektronik;
d. perlindungan informasi melalui penyediaan perangkat teknologi keamanan informasi dan jaring komunikasi sandi;
e. fasilitasi sertifikasi penerapan manajemen pengamanan sistem elektronik;
f. audit keamanan sistem elektronik;
g. audit keamanan pelaksanaan sistem manajemen;
h. literasi keamanan informasi dalam rangka peningkatan kesadaran keamanan informasi dan pengukuran tingkat kesadaran keamanan informasi di lingkungan Pemerintah Daerah dan publik;

i. peningkatan kompetensi sumber daya manusia di bidang persandian dan keamanan informasi;
j. pengelolaan pusat operasi pengamanan informasi;

k. penanganan insiden keamanan sistem elektronik;
l. forensik digital;
m. perlindungan informasi pada kegiatan penting Pemerintah Daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;
n. perlindungan informasi pada aset/fasilitas penting milik atau yang akan digunakan Pemerintah Daerah melalui kegiatan kontra penginderaan;
o. konsultasi keamanan informasi bagi pengguna layanan; dan/atau
p. jenis layanan keamanan informasi lainnya.

Pasal 44

(1) Penyediaan layanan keamanan informasi sebagaimana dimaksud dalam Pasal 42 menetapkan manajemen layanan keamanan informasi.
(2) Manajemen layanan keamanan informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas layanan keamanan informasi kepada Pengguna Layanan.
(3) Manajemen layanan keamanan informasi sebagaimana dimaksud pada ayat (1) merupakan penanganan terhadap keluhan, gangguan, masalah, permintaan, dan/atau perubahan layanan keamanan informasi dari pengguna layanan.
(4) Ketentuan lebih lanjut teknis pelaksanaan manajemen layanan keamanan informasi sebagaimana dimaksud pada ayat (3) ditetapkan oleh Kepala Perangkat Daerah dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB IV

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH

Pasal 45

(1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 3 huruf b untuk menentukan jaring komunikasi sandi internal Pemerintah Daerah.
(2) Jaring komunikasi sandi internal Pemerintah Daerah sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. jaring komunikasi sandi antar Perangkat Daerah;
    b. jaring komunikasi sandi internal Perangkat Daerah; dan
    c. jaring komunikasi sandi pimpinan Daerah.

(3) Jaring komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (2) huruf a menghubungkan seluruh Perangkat Daerah.

(4) Jaring komunikasi sandi internal Perangkat Daerah sebagaimana dimaksud pada ayat (2) huruf b menghubungkan antar pengguna layanan di lingkup internal Perangkat Daerah.
(5) Jaring komunikasi sandi pimpinan Daerah sebagaimana dimaksud pada ayat (2) huruf c menghubungkan antara Bupati, Wakil Bupati, dan Kepala Perangkat Daerah.

Pasal 46

(1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 45 ayat (1) dilaksanakan melalui:
   a. identifikasi pola hubungan komunikasi sandi; dan
   b. analisis pola hubungan komunikasi sandi.
(2) Identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf a, dilakukan terhadap:
   a. pola hubungan komunikasi pimpinan dan pejabat struktural internal Pemerintah Daerah;
   b. alur informasi yang dikomunikasikan antar Perangkat Daerah dan internal Perangkat Daerah;
   c. teknologi informasi dan komunikasi;
   d. infrastruktur komunikasi; dan
   e. kompetensi personel.
(3) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (2).
(4) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (3) memuat:
   a. pengguna layanan yang akan terhubung dalam jaring komunikasi sandi;
   b. topologi atau bentuk atau model keterhubungan jaring komunikasi sandi antar pengguna layanan;
   c. perangkat keamanan teknologi informasi dan komunikasi dan infrastruktur komunikasi, serta fasilitas lainnya yang dibutuhkan; dan
   d. tugas dan tanggung jawab pengelola dan pengguna layanan.
(5) Hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (4) sebagai pola hubungan komunikasi sandi antar Perangkat Daerah, ditetapkan dengan Keputusan Bupati.
(6) Keputusan Bupati sebagaimana dimaksud pada ayat (5) paling sedikit memuat:
   a. entitas pengguna layanan yang terhubung dalam jaring komunikasi sandi;
   b. topologi atau bentuk atau model keterhubungan antar pengguna layanan;
   c. sarana dan prasarana yang digunakan; dan
   d. tugas dan tanggung jawab pengelola dan pengguna layanan.

(7) Salinan keputusan Bupati sebagaimana dimaksud pada ayat (6) disampaikan oleh Bupati kepada Gubernur Provinsi Papua Selatan sebagai wakil Pemerintah Pusat

dan ditembuskan kepada Kepala BSSN.

(8) Ketentuan lebih lanjut teknis penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 45 ayat (1) ditetapkan oleh Kepala Perangkat Daerah dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB V
PEMANTAUAN, EVALUASI DAN PELAPORAN

Pasal 47

(1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan persandian untuk pengamanan informasi dan penetepan pola hubungan komunikasi sandi antar Perangkat Daerah.

(2) Perangkat Daerah melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) setiap 1 (satu) tahun sekali.

(3) Perangkat Daerah menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) kepada Bupati dan Gubernur Papua Selatan sebagai wakil Pemerintah Pusat.

Pasal 48

Ketentuan lebih lanjut teknis pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan persandian untuk pengamanan informasi dan penetapan pola hubungan komunikasi sandi antar Perangkat ditetapkan oleh Kepala Perangkat Daerah dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB VI
PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 49

(1) Pemerintah Daerah mendapatkan pembinaan dan pengawasan teknis terhadap penyelenggaraan persandian untuk pengamanan informasi dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dari BSSN dan Gubernur Papua Selatan sebagai wakil Pemerintah Pusat sesuai dengan kewenangannya.

(2) Pemerintah Daerah melakukan pembinaan dan pengawasan teknis terhadap Perangkat Daerah dalam penyelenggaraan persandian untuk pengamanan informasi dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.

(3) Ketentuan lebih lanjut teknis pelaksanaan pembinaan dan pengawasan teknis terhadap Perangkat Daerah sebagaimana dimaksud dalam Pasal 48 ayat (2)

ditetapkan oleh Bupati dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB VII
PEMBIAYAAN

Pasal 50

Pembiayaan penyelenggaraan persandian untuk pengamanan informasi dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah bersumber dari:

a. Anggaran Pendapatan dan Belanja Daerah; dan/atau
b. sumber pendanaan lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB VIII
KETENTUAN PERALIHAN

Pasal 51

Ketentuan kebijakan yang ditetapkan oleh Kepala Perangkat Daerah sebagaimana diatur dalam Peraturan Bupati ini wajib ditetapkan paling lama 1 (satu) Tahun sejak Peraturan Bupati ini diundangkan.

Pasal 52

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Kepi
pada tanggal 23 Januari 2023

Pj.BUPATI MAPPI,

CAP/ TTD

MICHAEL ROONEY GOMAR

diundangkan di Kepi
Pada tanggal 23 Januari 2023

SEKRETARIS DAERAH,

CAP/ TTD

FERDINANDUS KAINAKAIMU

BERITA DAERAH KABUPATEN MAPPI TAHUN 2023 NOMOR 09

Tembusan Peraturan ini disampaikan kepada Yth :

1. Gubernur Provinsi Papua Selatan di Merauke;
2. Inspektur Daerah Provinsi Papua Selatan di Merauke;
3. Ketua DPRD Kabupaten Mappi di Kepi;
4. Sekretaris Daerah Kabupaten Mappi di Kepi;
5. Inspektur Daerah Kabupaten Mappi di Kepi;
6. Kepala BPKAD Kabupaten Mappi di Kepi;
7. Kepala Dinas Komunikasi dan Informatika Kabupaten Mappi di Kepi;;
   A r s i p (Bag. Hukum).-

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM,

ALEXANDER RAHAIL, S.STP
NIP. 19830908 200212 1 002