BUPATI MADIUN

PROVINSI JAWA TIMUR

SALINAN

PERATURAN BUPATI MADIUN

NOMOR 46 TAHUN 2020

TENTANG

PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

DI PEMERINTAH KABUPATEN MADIUN

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MADIUN,

Menimbang:

a. bahwa berdasarkan Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah beberapa kali diubah dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah, penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah Kabupaten merupakan Urusan Pemerintahan Wajib yang tidak berkaitan dengan pelayanan dasar yang menjadi kewenangan Pemerintah Daerah Kabupaten;

b. bahwa untuk melaksanakan Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintahan Daerah;

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

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

Mengingat:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016;
2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;
3. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik;
4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah;
5. Peraturan Pemerintah Nomor 79 Tahun 2005 tentang Pedoman Pembinaan dan Pengawasan Penyelenggaraan Pemerintahan Daerah;
6. Peraturan Pemerintah Nomor 38 Tahun 2007 tentang Pembagian Urusan Pemerintahan antara Pemerintah, Pemerintah Daerah Provinsi, dan Pemerintah Daerah Kabupaten/Kota;
7. Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah;
8. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 13 Tahun 2016 tentang Hasil Pemetaan Urusan Pemerintahan Daerah di Bidang Komunikasi dan Informatika;
9. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 14 Tahun 2016 tentang Pedoman Nomenklatur Perangkat Daerah Bidang Komunikasi dan Informatika;
10. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik;
11. Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 5 Tahun 2017 tentang Pedoman Nomenklatur Perangkat Daerah Provinsi dan Daerah Kabupaten/Kota yang

Melaksanakan Fungsi Penunjang Penyelenggaraan Urusan Pemerintahan;

12. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah;
13. Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 70 Tahun 2019 tentang Sistem Informasi Pemerintahan Daerah;
14. Peraturan Daerah Nomor 6 Tahun 2016 tentang Susunan Perangkat Daerah sebagaimana telah diubah beberapa kali terakhir dengan Peraturan Daerah Nomor 13 Tahun 2019 tentang Perubahan Kedua Atas Peraturan Daerah Nomor 6 Tahun 2016 tentang Susunan Perangkat Daerah.

MEMUTUSKAN:

Menetapkan: PERATURAN BUPATI MADIUN TENTANG PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI PEMERINTAH KABUPATEN MADIUN

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Madiun.
2. Pemerintah Daerah adalah Bupati dan Perangkat Daerah sebagai unsur penyelenggara pemerintahan daerah Kabupaten Madiun.
3. Bupati adalah Bupati Madiun.
4. Perangkat Daerah adalah perangkat daerah di lingkungan Pemerintah Kabupaten Madiun yang meliputi Sekretariat Daerah, Sekretariat Dewan Perwakilan Rakyat Daerah, Dinas Daerah, dan Lembaga Teknis Daerah.
5. Dinas Komunikasi dan Informatika Kabupaten Madiun yang selanjutnya disebut Dinas adalah perangkat daerah yang menyelenggarakan urusan di bidang komunikasi dan informatika, statistik, dan persandian.

6. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.
7. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
8. 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.
9. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian, dan kenirsangkalan (*nonrepudiation*) Informasi.
10. Jaring Komunikasi Sandi adalah keterhubungan antar pengguna Persandian melalui jaring telekomunikasi.
11. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
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. 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 Balai Sertifikasi Elektronik pada Badan Siber dan Sandi Negara) dan/atau lembaga penyelenggara Sertifikasi Elektronik dalam negeri yang telah diakui
14. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.

15. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.
16. Informasi Publik adalah 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 lainnya yang sesuai dengan Undang-Undang serta Informasi lain yang berkaitan dengan kepentingan publik.
17. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
18. 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.
19. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta otentikasi data.
20. Sumber Daya Manusia Teknologi Informasi komunikasi adalah pegawai Perangkat Daerah yang memiliki tugas dan wewenang terkait dengan teknologi informasi dan komunikasi.
21. 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.

22. Balai Sertifikasi Elektronik yang selanjutnya disebut BSrE merupakan unit pelaksana teknis penyelenggara OSD Badan Siber dan Sandi Negara yang berada di bawah dan bertanggung jawab kepada Kepala Lembaga Sandi Negara.
23. 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.
24. Kerahasiaan adalah penjaminan atas aset SPBE yang informasinya tidak tersedia atau diungkapkan kepada individu, entitas, atau proses yang tidak mempunyai hak untuk mengaksesnya.
25. Keutuhan adalah properti bahwa suatu aset SPBE akurat dan lengkap.
26. Ketersediaan adalah properti bahwa aset SPBE dapat diakses dan digunakan atas permintaan oleh entitas yang berwenang.
27. Keaslian adalah properti bahwa aset SPBE terkait merupakan entitas yang diklaimnya.
28. Kenirsangkalan adalah kemampuan untuk membuktikan terjadinya suatu peristiwa yang diklaim atau tindakan dan entitas asalnya.

Pasal 2

Pelaksanaan persandian untuk pengamanan informasi di pemerintah Kabupaten Madiun bertujuan untuk:

a. menciptakan harmonisasi dalam melaksanakan Persandian untuk pengamanan informasi di pemerintah Kabupaten Madiun;
b. meningkatkan komitmen, efektivitas, dan kinerja pemerintah Kabupaten Madiun dalam melaksanakan kebijakan, program, dan kegiatan pelaksanaan Persandian untuk pengamanan informasi; dan
c. memberikan pedoman bagi Pemerintah Kabupaten Madiun dalam menetapkan pola hubungan komunikasi sandi antar Perangkat Daerah.

Pasal 3

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

a. penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Kabupaten Madiun; dan
b. penetapan pola hubungan komunikasi sandi antar Perangkat Daerah Kabupaten Madiun.

BAB II

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI PEMERINTAH DAERAH KABUPATEN MADIUN

Bagian Kesatu

Umum

Pasal 4

(1) Penyelenggaraan Persandian untuk Pengamanan Informasi pemerintah Kabupaten Madiun 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 nonelektronik; dan
   d. penyediaan layanan Keamanan Informasi.
(2) Pelaksana Penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Kabupaten Madiun terdiri atas Bupati dibantu oleh Dinas.
(3) Bupati sesuai dengan kewenangannya bertanggung jawab terhadap Penyelenggaraan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1).
(4) Dinas bertanggung jawab atas kinerja pelaksanaan Urusan Pemerintahan bidang Persandian sesuai dengan tugas dan fungsinya.

Bagian Kedua

Penyusunan Kebijakan Pengamanan Informasi

Pasal 5

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 4 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 6

(1) Bupati sesuai dengan kewenangannya menyusun rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 5 huruf a.
(2) Penyusunan rencana strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.
(3) Rencana strategis sebagaimana dimaksud pada ayat (1) 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.
(4) Rencana strategis Pengamanan Informasi yang telah disusun sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah.
(5) Dalam melakukan penyusunan rencana strategis sebagaimana dimaksud pada ayat (1) Bupati dapat melakukan koordinasi dan konsultasi kepada BSSN.
(6) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (5) Bupati dapat menunjuk Dinas.

Pasal 7

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

Pasal 8

(1) Bupati sesuai dengan kewenangannya menetapkan aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 huruf c.
(2) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) 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.

(3) Dalam melakukan penyusunan aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) Bupati dapat melakukan koordinasi dan konsultasi kepada BSSN.

(4) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (3) Bupati dapat menunjuk Dinas.

Pasal 9

(1) Keamanan sumber daya teknologi informasi sebagaimana dimaksud pada pasal 8 ayat (2) 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;
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 pasal 9 ayat (3) huruf a dapat diimplementasikan melalui:
   a. metoda *scripting software* aplikasi yang aman;
   b. implementasi mekanisme otentikasi 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 & 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 (*availability*) pada sistem utama.

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

Pasal 10

(1) Keamanan akses kontrol sebagaimana dimaksud pada pasal 8 ayat (2) 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 untuk kendali akses 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 otentikasi rahasia dari pengguna, bahwa alokasi dari informasi otentikasi 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 otentikasi rahasia, bahwa pengguna harus mengikuti praktik organisasi dalam penggunaan informasi otentikasi 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 11

(1) Keamanan data dan informasi sebagaimana dimaksud pada pasal 8 ayat (2) 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 logik, dilakukan dengan menggunakan perlindungan logik menggunakan teknik Kriptografi dan

steganografi untuk memenuhi aspek kerahasiaan, keutuhan, otentikasi, dan kenirsangkalan.

(2) Perlindungan fisik sebagaimana dimaksud pada ayat (2) 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 lojik sebagaimana dimaksud pada ayat (2) huruf c harus memenuhi standar dan direkomendasikan oleh BSSN.

Pasal 12

(1) Keamanan sumber daya manusia sebagaimana dimaksud pada pasal 8 ayat (2) 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 dan 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 pengubahan atau penghentian kepegawaian, dengan cara penghentian atau perubahan tanggung jawab kepegawaian.

Pasal 13

(1) Keamanan jaringan sebagaimana dimaksud pada pasal 8 ayat (2) huruf e dilaksanakan untuk menjamin perlindungan informasi dalam jaringan dan fasilitas pendukung pengolahan informasi.

(2) Keamanan jaringan sebagaimana dimaksud pada pasal 8 ayat (2) huruf e dilaksanakan melalui:
   a. kendali jaringan, bahwa jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi;
   b. kemanan 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 14

(1) Keamanan surat elektronik sebagaimana dimaksud pada pasal 8 ayat (2) huruf f dilaksanakan melalui pemanfaatan layanan sertifikat elektronik.

(2) Proses 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* & *softcopy*).

Pasal 15

(1) Keamanan pusat data sebagaimana dimaksud pada pasal 8 ayat (2) 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 otentikasi 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 16

(1) Keamanan komunikasi sebagaimana dimaksud pada pasal 8 ayat (2) 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 (*nondisclosure agreement*), 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 17

(1) Dinas melaksanakan Pengelolaan Sumber Daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf b.

(2) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas:

a. pengelolaan aset keamanan teknologi informasi dan komunikasi;
b. pengelolaan sumber daya manusia; dan
c. manajemen pengetahuan.

Paragraf 1

Pengelolaan Aset Keamanan Teknologi Informasi dan Komunikasi

Pasal 18

(1) Pengelolaan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 17 ayat (2) 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 19

(1) Pemerintah 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 harus bersadarkan pada aset keamanan teknologi Informasi dan komunikasi yang telah direkomendasikan oleh Badan Siber dan Sandi Negara.
(3) Hasil penetapan aset keamanan teknologi Informasi dan komunikasi diajukan Pemerintah Daerah kepada Badan Siber dan Sandi Negara untuk permohonan pemenuhan peralatan sandi kebutuhan Pemerintah Daerah.

Pasal 20

(1) Bupati dibantu oleh Dinas bertanggung jawab dalam pengadaan aset keamanan teknologi Informasi dan komunikasi.

(2) Perangkat Daerah berkewenangan untuk melakukan pengajuan terkait pengadaan aset keamanan teknologi Informasi dan komunikasi.

(3) Pengadaan aset keamanan teknologi Informasi dan komunikasi dilaksanakan berdasarkan prinsip efisien, efektif, transparan & terbuka, bersaing, adil, dan akuntabel.

Pasal 21

(1) Dinas sesuai dengan kewenangannya melakukan pengelolaan dan pemanfaatan aset keamanan teknologi informasi dan komunikasi.

(2) Aset keamanan teknologi informasi dan komunikasi dimanfaatkan untuk kepentingan pengamanan informasi.

(3) Pemanfaatan aset keamanan teknologi Informasi dan komunikasi 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.

(4) Penggunaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksudkan pada ayat (3) huruf a meliputi:
   a. materiil sandi;
   b. tempat kegiatan sandi; dan
   c. alat pendukung utama (APU) Persandian.

(5) Pemeliharaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksudkan pada ayat (3) 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.

(6) Perbaikan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksudkan pada ayat (3) huruf c dilakukan melalui perbaikan umum, yang merupakan perbaikan yang tidak berkaitan dengan aspek kriptografis, dilakukan oleh Dinas dengan berkoordinasi dengan BSSN.

(7) Pendistribusian aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksudkan pada ayat (3) 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).

(8) Pengawasan dan pengendalian aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksudkan pada ayat (3) huruf e harus dilakukan secara menyeluruh, terus menerus, dan berkesinambungan.

Pasal 22

(1) Dinas bertanggung jawab dalam penghapusan aset keamanan teknologi informasi dan komunikasi.
(2) Perangkat Daerah berkewenangan untuk melakukan pengajuan terkait penghapusan aset keamanan teknologi informasi dan komunikasi.
(3) Penghapusan aset keamanan teknologi informasi dan komunikasi dilakukan berdasarkan prinsip kehati-hatian dan ketepatan.
(4) Penghapusan aset keamanan teknologi informasi dan komunikasi meliputi:
    a. penghapusan dari daftar barang pengguna dan/atau daftar barang kuasa pengguna terkait aset keamanan teknologi informasi dan komunikasi Pemerintah Daerah; dan
    b. penghapusan dari daftar barang milik Pemerintah Daerah terkait aset keamanan teknologi informasi dan komunikasi Pemerintah Daerah.

Pasal 23

(1) Penghapusan dari daftar barang pengguna dan/atau daftar barang kuasa pengguna terkait aset keamanan teknologi Informasi dan komunikasi Pemerintah Daerah sebagaimana dimaksud dalam pasal 22 ayat (4) huruf a dilakukan dalam hal barang milik daerah sudah tidak berada dalam penguasaan Pemerintah Daerah.
(2) Penghapusan sebagaimana dimaksud pada ayat (1) dilakukan dengan menerbitkan keputusan Penghapusan dari Dinas setelah mendapatkan persetujuan dari Bupati untuk barang milik daerah dan BSSN untuk barang milik negara.
(3) Penghapusan aset keamanan teknologi Informasi dan komunikasi dilakukan karena:
    a. pengalihan status penggunaan;
    b. pemindahtanganan; atau
    c. pemusnahan.

(4) Bupati melalui Dinas dapat mendelegasikan persetujuan Penghapusan aset keamanan teknologi Informasi dan komunikasi kepada BSSN.
(5) Pelaksanaan penghapusan aset keamanan teknologi Informasi dan komunikasi dilaporkan kepada BSSN.

Pasal 24

(1) Penghapusan dari daftar barang milik Pemerintah Daerah terkait aset keamanan teknologi Informasi dan komunikasi Pemerintah Daerah sebagaimana dimaksud dalam pasal 22 ayat (2) huruf b dilakukan dalam hal barang milik daerah sudah beralih kepemilikannya, terjadi pemusnahan, atau karena sebab lain.
(2) Penghapusan sebagaimana pada ayat (1) dilakukan berdasarkan keputusan dan/atau laporan penghapusan dari Pemerintah Daerah melalui Dinas.

Pasal 25

Ketentuan lebih lanjut terkait teknis pengelolaan aset keamanan teknologi Informasi dan komunikasi yang meliputi perencanaan, pengadaan, pemanfaatan, dan penghapusan di lingkungan Pemerintah Daerah ditetapkan oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Paragraf 2

Pengelolaan Sumber Daya Manusia

Pasal 26

(1) Dinas melakukan pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 17 ayat (2) huruf b.
(2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses sebagai berikut:
    a. pengembangan kompetensi;
    b. pembinaan karir;
    c. pendayagunaan; dan
    d. pemberian tunjangan pengamanan persandian.

Pasal 27

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 26 ayat (2) 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 26 ayat (2) 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 26 ayat (2) huruf c dilaksanakan agar seluruh sumber daya manusia yang bertugas di Dinas melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan.

(4) Pemberian tunjangan pengamanan persandian sebagaimana dimaksudkan dalam pasal 26 ayat (2) huruf d meliputi Tunjangan Pengamanan Persandian dan Tunjangan Jabatan Fungsional Sandiman.

Paragraf 3

Manajemen Pengetahuan

Pasal 28

(1) Dinas melakukan manajemen pengetahuan sebagaimana dimaksud dalam Pasal 17 ayat (2) huruf c.
(2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan untuk meningkatkan kualitas Layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait Keamanan Informasi.
(3) Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi Pemerintah Daerah.
(4) Manajemen pengetahuan sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi Pemerintah Daerah.
(5) Dalam pelaksanaan manajemen pengetahuan, Dinas berkoordinasi dan dapat melakukan konsultasi dengan BSSN.

Pasal 29

(1) Pengumpulan pengetahuan 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 yang dihasilkan dalam pelaksanaan Keamanan Informasi dilakukan melalui serangkaian proses untuk mengetahui aset pengetahuan yang dimiliki Pemerintah Daerah, aset ini bisa berupa produk / layanan, portfolio proyek, data, *database* kompetensi

organisasi, literatur (buku, majalah, laporan), dan sebagainya.

(5) Pengetahuan yang telah teridentifikasi kemudian diprioritaskan implementasinya, sehingga menjadi ruang lingkup.

Pasal 30

(1) Pengolahan pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi dilakukan dengan mengintegrasikan dengan pengetahuan lainnya.

(2) Pengolahan pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi juga dapat dilakukan dengan membagi pengetahuan berdasarkan kompetensi atau kategori tertentu sesuai dengan yang telah ditentukan oleh Pemerintah Daerah.

Pasal 31

(1) Pengetahuan yang telah teridentifikasi direkam dan disimpan ke dalam database pengetahuan organisasi atau *knowledge repository*.

(2) Setiap Perangkat Daerah wajib mendokumentasikan pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi yang kemudian akan dilakukan penyimpanan oleh Dinas.

Pasal 32

(1) Penggunaan pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi diwujudkan dalam prosedur atau peraturan untuk mengarahkan ke perilaku pada masa yang akan datang.

(2) Pada saat penggunaan pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi dapat melakukan aktivitas pengembangan dan penyempurnaan lebih lanjut dari pengetahuan yang telah didapatkan.

Pasal 33

(1) Kegiatan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi dapat berlangsung secara tradisional maupun dengan menggunakan teknologi pendukung.
(2) Pemerintah Daerah wajib menjamin terjadinya alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi antar perangkat daerah yang membutuhkan.
(3) Kegiatan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi dilakukan melalui:
    a. pendidikan dan pelatihan kerja sesuai dengan kualifikasi jabatan yang diduduki; dan
    b. pelaksanaan pelatihan atau pengajaran dalam jangka waktu tertentu.

Pasal 34

Ketentuan lebih lanjut terkait teknis pelaksanaan manajemen pengetahuan yang meliputi proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi Pemerintah Daerah ditetapkan oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Bagian Keempat

Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik

Pasal 35

Dinas melaksanakan pengamanan Sistem Elektronik dan pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf c sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 36

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 35 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) Dalam melaksanakan Pengelolaan aset dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 36, Dinas melakukan:
    a. identifikasi;
    b. deteksi;
    c. proteksi; dan
    d. penanggulangan dan pemulihan.
(2) Identifikasi sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui kegiatan analisis kerawanan dan risiko terhadap Sistem Elektronik.
(3) Deteksi sebagaimana dimaksud pada ayat (1) huruf b dilakukan melalui kegiatan analisis untuk menentukan adanya ancaman atau kejadian insiden pada Sistem Elektronik.
(4) Proteksi sebagaimana dimaksud pada ayat (1) huruf c dilakukan dengan kegiatan 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 kegiatan penanganan yang tepat dan perbaikan terhadap adanya insiden pada Sistem Elektronik agar penyelenggaraan pemerintahan berbasis elektronik berfungsi kembali dengan baik.

Pasal 38

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 36, Dinas 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) Untuk mendapatkan Sertifikat elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 39

(1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik Dinas dapat menyelenggarakan 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 terkait teknis penyelenggaraan pusat operasi Pengamanan Informasi sebagaimana dimaksud pada ayat (1) di lingkungan Pemerintah Daerah ditetapkan oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 40

(1) Dalam mendukung pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 35 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi nonelektronik.
(2) Ketentuan lebih lanjut terkait teknis pengamanan informasi nonelektronik sebagaimana dimaksud pada ayat (1) di lingkungan Pemerintah Daerah ditetapkan oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 41

(1) Dinas melaksanakan audit Keamanan Informasi di lingkup Pemerintah Daerah.
(2) Audit Keamanan Informasi meliputi audit keamanan Sistem Elektronik dan audit pelaksanaan sistem manajemen.
(3) Ketentuan lebih lanjut terkait teknis pelaksanaan audit Keamanan Informasi sebagaimana dimaksud pada ayat (1) di lingkungan Pemerintah Daerah ditetapkan oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Bagian Kelima
Penyediaan Layanan Keamanan Informasi
Pasal 42

(1) Dinas melaksanakan Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf d.
(2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:
    a. Bupati dan Wakil;
    b. Perangkat Daerah;

c. pegawai atau aparatur sipil negara pada Pemerintah Daerah; dan
d. pihak lainnya.

Pasal 43

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 42 ayat (1) 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) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 43 Dinas melaksanakan 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 terkait teknis pelaksanaan manajemen layanan keamanan informasi sebagaimana dimaksud pada ayat (3) di lingkungan Pemerintah Daerah ditetapkan oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB III

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH

Pasal 45

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

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

(5) Jaring komunikasi sandi internal Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar Pengguna Layanan di lingkup internal Perangkat Daerah.

(6) Jaring komunikasi sandi pimpinan daerah sebagaimana dimaksud pada ayat (3) 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) Bupati menetapkan hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (4) sebagai pola hubungan komunikasi sandi antar Perangkat Daerah, dengan Keputusan Bupati.

(6) Keputusan 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 sebagaimana dimaksud pada ayat (6) disampaikan oleh Bupati kepada Gubernur sebagai wakil Pemerintah Pusat dan ditembuskan kepada Kepala BSSN.

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

BAB IV
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) Dinas melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) setiap 1 (satu) tahun sekali.

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

Pasal 48

Ketentuan lebih lanjut terkait teknis pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah di lingkungan Pemerintah Daerah ditetapkan oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB V

PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 49

(1) Pemerintah Daerah mendapatkan pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dari BSSN dan Gubernur sebagai wakil Pemerintah Pusat sesuai dengan kewenangannya.

(2) Dinas sesuai dengan kewenangannya melakukan pembinaan dan pengawasan teknis terhadap perangkat daerah terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.

Pasal 50

(1) Pemerintah Daerah mendapatkan pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sesuai dengan ketentuan peraturan perundang-undangan.

(2) Ketentuan lebih lanjut terkait teknis pelaksanaan pembinaan dan pengawasan teknis terhadap perangkat daerah sebagaimana dimaksud dalam pasal 49 ayat (2) ditetapkan oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB VI

PENDANAAN

Pasal 51

Pendanaan pelaksanaan penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah 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 VII

KETENTUAN PENUTUP

Pasal 52

Pada saat Peraturan Bupati ini mulai berlaku:

a. Kebijakan pemerintah dan semua peraturan perundang-undangan yang mengatur mengenai pelaksanaan Persandian untuk Pengamanan Informasi Pemerintah Daerah yang telah ditetapkan dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan Peraturan Bupati ini; dan
b. Kebijakan pemerintah dan semua peraturan perundang-undangan yang mengatur mengenai pelaksanaan Persandian untuk Pengamanan Informasi Pemerintah Daerah yang telah ditetapkan wajib menyesuaikan dengan ketentuan dalam Peraturan Bupati ini paling lama 1 (satu) tahun terhitung sejak Peraturan Bupati ini diundangkan.

Pasal 53

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan. Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Lembaran Daerah Kabupaten Madiun.

Ditetapkan di Madiun
pada tanggal 23 September 2020

BUPATI MADIUN

ttd

AHMAD DAWAMI RAGIL SAPUTRO

Diundangkan di Madiun
pada tanggal 23 September 2020
SEKRETARIS DAERAH
KABUPATEN MADIUN,

ttd
TONTRO PAHLAWANTO

BERITA DAERAH KABUPATEN MADIUN TAHUN 2020 NOMOR 46

SALINAN
Sesuai dengan aslinya
KEPALA BAGIAN HUKUM,

ttd
ALIF MARGIANTO
NIP. 197805252002121006