GUBERNUR JAWA TENGAH

PERATURAN GUBERNUR JAWA TENGAH

NOMOR 25 TAHUN 2021

TENTANG

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH PROVINSI JAWA TENGAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR JAWA TENGAH,

Menimbang :

a. bahwa dalam rangka pengamanan informasi di Provinsi Jawa Tengah telah ditetapkan Peraturan Gubernur Jawa Tengah Nomor 10 Tahun 2018 tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi Di Lingkungan Pemerintah Provinsi;

b. bahwa berdasarkan dinamika perkembangan teknologi informasi dan tantangan serta ancaman dunia siber dan berdasarkan peninjauan kembali terhadap penyelenggaraan persandian untuk pengamanan informasi di Lingkungan Pemerintah Daerah, maka Peraturan Gubernur Jawa Tengah Nomor 10 Tahun 2018 tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi Di Lingkungan Pemerintah Provinsi perlu diganti;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, serta berdasarkan Peraturan Kepala Badan Siber Dan Sandi Negara Nomor 10 Tahun 2019 Tentang Pelaksanaan Persandian Untuk Pengamanan Informasi Di Pemerintah Daerah, perlu menetapkan Peraturan Gubernur tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi Di Lingkungan Pemerintah Provinsi Jawa Tengah;

Mengingat :

1. Undang-Undang Nomor 10 Tahun 1950 tentang Pembentukan Provinsi Jawa Tengah (Himpunan Peraturan-Peraturan Negara Tahun 1950 Nomor 86-92);

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);

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

4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia tahun 2014 Nomor 244, Tambahan Lembaran

Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);

5. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik;
6. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 8 Tahun 2019 Tentang Penyelenggaraan Urusan Pemerintahan Konkuren Bidang Komunikasi dan Informatika;
7. Peraturan Kepala Badan Siber Dan Sandi Negara Nomor 10 Tahun 2019 Tentang Pelaksanaan Persandian Untuk Pengamanan Informasi Di Pemerintah Daerah;
8. Peraturan Kepala Badan Siber Dan Sandi Negara Nomor 4 Tahun 2021 Tentang Pedoman Managemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik;

MEMUTUSKAN :

Menetapkan : PERATURAN GUBERNUR TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH PROVINSI JAWA TENGAH.

BAB I
KETENTUAN UMUM

Bagian Kesatu
Pengertian

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Daerah adalah Provinsi Jawa Tengah.
2. Pemerintah Daerah adalah Pemerintah Provinsi Jawa Tengah.
3. Kabupaten/Kota adalah kabupaten/kota di Jawa Tengah.
4. Sekretaris Daerah adalah Sekretaris Daerah Provinsi Jawa Tengah.
5. Dinas adalah Perangkat Daerah yang mempunyai tugas pokok dan fungsi dalam penyelenggaraan Komunikasi dan Informatika.
6. Kepala Dinas adalah Kepala Perangkat Daerah yang mempunyai tugas pokok dan fungsi dalam penyelenggaraan Komunikasi dan Informatika.
7. 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.
8. Materiil Sandi yang selanjutnya disebut Matsan adalah barang persandian negara yang memiliki klasifikasi rahasia dan berfungsi sebagai alat pengamanan informasi atau alat analisis sinyal atau bahan/perangkat yang berhubungan dengan proses penyelenggaraan pengamanan informasi.

9. Jaring Komunikasi Sandi yang selanjutnya disebut JKS adalah keterhubungan antar pengguna persandian melalui jaring telekomunikasi.
10. Alat Pendukung Utama Persandian yang selanjutnya disebut APU Persandian adalah peralatan pendukung yang digunakan dalam kegiatan pengamanan persandian.
11. *Jamming* adalah kegiatan untuk mengacak sinyal di waktu dan tempat tertentu.
12. Operasi Siaga Kontra Penginderaan yang selanjutnya disebut Kontra Penginderaan adalah kegiatan yang dibatasi waktu untuk melakukan pencegahan terhadap pengawasan pihak lain, termasuk metode-metode yang melibatkan peralatan elektronik seperti *bugsweeping* dan mendeteksi adanya peralatan pengawasan (*surveillance*).
13. *Penetration Test* yang selanjutnya disingkat PENTEST adalah pengujian keamanan informasi dimana seorang asesor meniru serangan yang biasa sering terjadi untuk mengidentifikasi metode peretasan fitur keamanan aplikasi, sistem, atau jaringan.
14. *Security Operation Center* yang selanjutnya disingkat SOC adalah kegiatan pengamanan informasi dengan melakukan proses pengawasan, perlindungan, dan penanggulangan insiden keamanan informasi dengan memperhatikan aspek personil, proses pelaksanaan, dan ketersediaan teknologi.
15. *Computer Security Insident Response Team* yang selanjutnya disingkat CSIRT adalah kegiatan penanggulangan dan pemulihan terhadap insiden keamanan siber pada sektor pemerintah daerah.
16. 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.
17. Informasi publik adalah 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 ini serta informasi lain yang berkaitan dengan kepentingan publik.
18. Informasi berklasifikasi adalah informasi publik yang dikecualikan menurut peraturan perundang-undangan yang berlaku.
19. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan Informasi.
20. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
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 penyelenggara sertifikasi elektronik.
23. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.

24. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
25. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.
26. Dinas Komunikasi dan Informatika Provinsi Jawa Tengah yang selanjutnya disebut Dinas adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang persandian dan keamanan siber.
27. Perangkat Daerah adalah perangkat daerah dilingkungan Pemerintah Provinsi Jawa Tengah.

Bagian Kedua
Maksud, Tujuan dan Ruang Lingkup

Pasal 2

Peraturan Gubernur ini dimaksudkan untuk memberikan pedoman dalam melaksanakan kebijakan, program, dan kegiatan penyelenggaraan persandian untuk pengamanan informasi di lingkungan Pemerintah Daerah.

Pasal 3

Pelaksanaan persandian untuk pengamanan informasi di lingkungan Pemerintah Daerah bertujuan untuk :

a. menciptakan harmonisasi dalam pembagian urusan pemerintahan bidang Persandian;
b. memfasilitasi Pemerintah Kabupaten/Kota dalam melaksanakan penyelenggaraan persandian untuk pengamanan informasi;
c. meningkatkan efektivitas pelaksanaan kebijakan, program dan kegiatan penyelenggaraan persandian untuk pengamanan informasi; dan
d. memberikan pedoman bagi Pemerintah Daerah dalam menetapkan pola hubungan komunikasi sandi antar perangkat daerah.

Pasal 4

Ruang lingkup Peraturan Gubernur ini meliputi:

a. perencanaan;
b. pelaksanaan;
c. Forum Komunikasi Persandian Daerah;
d. pemantauan, evaluasi dan pelaporan;
e. pembinaan dan pengawasan teknis kabupaten/kota; dan
f. pembiayaan.

BAB II
PERENCANAAN

Pasal 5

(1) Perencanaan Persandian Untuk Pengamanan Informasi Di Lingkungan Pemerintah Provinsi Jawa Tengah dituangkan dalam bentuk Rencana Strategis Pengamanan Informasi.

(2) Rencana Strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) disusun oleh Dinas dan dikoordinasikan dengan Perangkat Daerah yang membidangi perencanaan pembangunan daerah.

(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 sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Gubernur.

Pasal 6

(1) Rencana strategis Pengamanan Informasi yang telah disusun sebagaimana dimaksud dalam Pasal 5 ayat (1) diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah (RPJMD).

(2) Penyusunan rencana strategis sebagaimana dimaksud pada ayat (1) dikoordinasikan dan dikonsultasikan oleh Dinas kepada BSSN.

BAB III
PELAKSANAAN

Bagian Kesatu
Umum

Pasal 7

(1) Pelaksanaan persandian untuk pengamanan informasi di Lingkungan Pemerintah Daerah meliputi :

a. penyelenggaraan Persandian untuk Pengamanan Informasi;

b. penetapan pola hubungan komunikasi sandi antar Perangkat Daerah;

c. penyelenggaraan Sertifikat Elektronik di Lingkungan Pemerintah Daerah untuk mendukung Sistem Pemerintahan Berbasis Elektronik.

(2) Pelaksanaan persandian untuk pengamanan infomasi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Gubernur melalui :

a. penguatan kapasitas kelembagaan, SDM dan sarana prasarana;

b. mengoordinasikan kegiatan antar Perangkat Daerah;

c. kerjasama dengan kabupaten/kota, provinsi lain, dan/atau kabupaten/kota di provinsi lain

Pasal 8

(1) Pelaksanaan persandian untuk pengamanan informasi meliputi :

a. penyediaan analisis kebutuhan penyelenggaraan persandian untuk pengamanan informasi;

b. penyediaan kebijakan penyelenggaraan persandian untuk pengamanan informasi;

c. pengelolaan dan perlindungan informasi;
d. pengelolaan sumber daya persandian meliputi sumber daya manusia, materiil sandi dan jaring komunikasi sandi serta anggaran;
e. penyelenggaraan operasional dukungan persandian untuk pengamanan informasi;
f. pengawasan dan evaluasi penyelenggaraan pengamanan informasi melalui persandian di seluruh Perangkat Daerah;
g. koordinasi dan konsultasi penyelenggaraan persandian untuk pengamanan informasi.

(2) Pengamanan informasi sebagaimana dimaksud pada ayat (1) mencakup pengamanan fisik, pengamanan logis dan perlindungan secara administrasi.

Bagian Kedua
Penyelenggaraan Persandian Untuk Pengamanan Informasi

Paragraf 1
Umum

Pasal 9

Penyelenggaraan Persandian untuk Pengamanan Informasi 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.

Paragraf 2
Penyusunan Kebijakan Pengamanan Informasi

Pasal 10

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 9 huruf a dilaksanakan dengan :

a. menyusun rencana strategis Pengamanan Informasi;
b. menetapkan arsitektur Keamanan Informasi; dan
c. menetapkan aturan mengenai tata kelola Keamanan Informasi.

Pasal 11

Penyusunan rencana strategis pengamanan informasi sebagaimana dimaksud dalam Pasal 10 huruf a dilaksanakan sesuai ketentuan Pasal 5 dan Pasal 6 Peraturan Gubernur ini.

Pasal 12

(1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 10 huruf b disusun oleh Dinas.

(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) Penyusunan Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) dikoordinasikan dan dikonsultasikan oleh Dinas kepada BSSN.

(4) Arsitektur Keamanan Informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.

(5) Arsitektur Keamanan Informasi dilakukan evaluasi pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu waktu sesuai dengan kebutuhan.

Pasal 13

(1) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 10 huruf c dituangkan dalam Standar Operasional Prosedur yang ditetapkan dengan Keputusan Kepala Dinas.

(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) Penyusunan aturan mengenai tata kelola Keamanan Informasi dilaksanakan oleh Dinas dan dikoordinasikan kepada Unit Kerja Perangkat Daerah yang membidangi urusan pemerintahan dibidang hukum.

(4) Penyusunan aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) dikoordinasikan dan dikonsultasikan oleh Dinas kepada BSSN.

Paragraf 3
Pengelolaan Sumber Daya Keamanan Informasi

Pasal 14

(1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 9 huruf b dilaksanakan oleh Perangkat Daerah terkait.

(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.

Pasal 15

(1) Pengelolaan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf a dilakukan oleh Dinas dan berkoordinasi dengan Perangkat Daerah yang membidangi urusan aset daerah.

(2) Pengelolaan aset keamanan teknologi Informasi dan komunikasi dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.

(3) 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 16

(1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf b dilakukan oleh Dinas dan berkoordinasi dengan Perangkat Daerah yang membidangi urusan kepegawaian dan Perangkat Daerah yang membidangi urusan pengembangan sumber daya manusia.

(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 17

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 16 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 masing-masing; dan
   c. memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi di bidang Keamanan Informasi.

(2) Pembinaan karir sebagaimana dimaksud dalam Pasal 16 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 16 ayat (2) huruf c dilaksanakan dengan ketentuan :

a. seluruh sumber daya manusia yang bertugas di bidang Keamanan Informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan;
b. untuk memenuhi kebutuhan dan mengantisipasi keterbatasan sumber daya manusia persandian, pegawai yang telah memiliki sertifikasi, keahlian dan atau pernah mengikuti pendidikan dan pelatihan sandi yang diselenggarakan oleh BSSN sebagai pembina dan penyelenggara persandian nasional, tetap ditugaskan secara penuh di bidang persandian dan tidak dimutasi kebidang tugas lain kecuali promosi jabatan.

Pasal 18

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf c dilakukan untuk meningkatkan kualitas Layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait Keamanan Informasi.

(2) Manajemen pengetahuan 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 (3) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi pemerintah daerah.

(4) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.

(5) Dalam pelaksanaan manajemen pengetahuan, Dinas berkoordinasi dan berkonsultasi dengan BSSN.

Paragraf 4
Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik

Pasal 19

Pengamanan Sistem Elektronik dan pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 9 huruf c dilaksanakan oleh Dinas.

Pasal 20

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 19 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 21

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 20, 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 dimaksudpada 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 22

(1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 21 ayat (1) Pemerintah Daerah 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.

Pasal 23

(1) Pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 19 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi nonelektronik.
(2) Pengamanan Informasi nonelektronik sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 24

(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) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Paragraf 5
Penyediaan Layanan Keamanan Informasi

Pasal 25

(1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 9 huruf d dilaksanakan oleh Dinas.

(2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:

a. Kepala Daerah dan Wakil Kepala Daerah;

b. Perangkat Daerah;

c. pegawai atau Aparatur Sipil Negara pada Pemerintah Daerah; dan

d. pihak lainnya.

Pasal 26

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 25 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 Keamanan Informasi dan/atau persandian;
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 27

(1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 26, 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) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen Layanan Keamanan Informasi.

Bagian Ketiga
Penetapan Pola Hubungan Komunikasi Sandi Antar Perangkat Daerah

Pasal 28

(1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 7 ayat (1) huruf b ditetapkan oleh Gubernur.

(2) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dan kabupaten/kota 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 Gubernur, Wakil Gubernur, dan Kepala Perangkat Daerah.

Pasal 29

(1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 28 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 (2) huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (3).

(4) Pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 19 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi nonelektronik.

(5) Pengamanan Informasi nonelektronik sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan

(6) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (4) 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, infrastruktur komunikasi, serta fasilitasi lainnya yang dibutuhkan; dan

d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.

(7) Hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (5) ditetapkan sebagai pola hubungan komunikasi sandi antar perangkat daerah Provinsi oleh Gubernur dalam bentuk Keputusan Gubernur.

(8) 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.

(9) Salinan keputusan sebagaimana dimaksud pada ayat (6) disampaikan oleh Gubernur kepada Kepala BSSN.

Bagian Keempat

Penyelenggaraan Sertifikat Elektronik Di Lingkungan Pemerintah Daerah Guna Mendukung Sistem Pemerintahan Berbasis Elektronik

Pasal 30

(1) Dalam melaksanakan Pengamanan Sistem Elektronik, wajib menggunakan Sertifikat Elektronik pada setiap layanan publik dan layanan pemerintahan berbasis elektronik.

(2) Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) diterbitkan oleh Balai Sertifikasi Elektronik.

(3) Penyelenggaraan Sertifikat Elektronik di lingkungan Pemerintah Daerah bertujuan:

a. meningkatkan kapabilitas dan tata kelola Keamanan Informasi dalam penyelenggaraan Sistem Elektronik;

b. meningkatkan Keamanan Informasi dalam Sistem Elektronik;

c. meningkatkan kepercayaan, kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan terhadap implementasi Sistem Elektronik; dan
d. meningkatkan efisiensi dan efektifitas penyelenggaraan pemerintahan dan pelayanan publik.

(4) Untuk mendapatkan Sertifikat elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan oleh Otoritas Pendaftaran (OP) yang bertanggung jawab melakukan pemeriksaan, pemberian persetujuan atau penolakan atas setiap permintaan penerbitan, pembaruan, dan pencabutan Sertifikat Elektronik yang diajukan oleh pemilik atau calon Pemilik Sertifikat Elektronik.

(5) Dinas berkedudukan sebagai Otoritas Pendaftaran (OP).

BAB IV
FORUM KOMUNIKASI PERSANDIAN DAERAH

Pasal 31

(1) Dalam mendukung penyelenggaraan jaring komunikasi sandi yang efektif, efisien dan komprehensif dilingkungan Pemerintah Daerah, perlu dibentuk Forum Komunikasi Sandi Daerah.

(2) Forum Komunikasi Sandi sebagaimana dimaksud pada ayat (1) dapat beranggotakan Instansi dilingkungan Pemerintah Daerah, Pemerintah Kabupaten/Kota dan Instansi vertikal di Daerah serta Badan Usaha Milik Daerah/Daerah yang memiliki tugas pokok dan fungsi pengelola persandian dan keamanan informasi daerah.

(3) Forum Komunikasi Sandi sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Gubernur.

BAB V
PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 32

(1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penatepan pola hubungan komunikasi sandi antar perangkat daerah.

(2) Kepala Dinas melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) setiap 1 (satu) tahun sekali dan menyampaikan laporannya kepada Gubernur.

(3) Gubernur menyampaikan laporan pelaksanaan penyelenggaraan sebagaimana dimaksud pada ayat (1) Kepala BSSN sebagai pembina tunggal persandian negara dengan tembusan kepada Menteri Dalam Negeri.

(4) Guna kelancaran pelaksanaan tugas sebagaimana dimaksud pada ayat (1) Gubernur dapat membentuk tim yang susunan keanggotaannya terdiri dari unsur instansi terkait sesuai kebutuhan.

Pasal 33

Pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi pemerintah daerah provinsi dan penetapan pola hubungan komunikasi sandi antar perangkat daerah provinsi dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI
PEMBINAAN DAN PENGAWASAN TEKNIS KEPADA PEMERINTAH KABUPATEN/KOTA

Pasal 34

Gubernur sebagai wakil Pemerintah Pusat melaksanakan pembinaan dan pengawasan teknis terhadap penyelenggaraan persandian untuk Pengamanan Informasi Pemerintah Daerah Kabupaten/Kota dan penetepan pola hubungan komunikasi sandi antar Perangkat Daerah Kabupaten/Kota.

Pasal 35

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah Kabupaten/Kota dan penetepan pola hubungan komunikasi sandi antar Perangkat Daerah Kabupaten/Kota dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 36

(1) Dalam melaksanakan pembinaan dan pengawasan teknis sebagaimana dimaksud dalam Pasal 34 Gubernur sesuai dengan kewenangannya menyelenggarakan rapat koordinasi urusan Persandian.

(2) Rapat koordinasi sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam setahun.

BAB VII
PEMBIAYAAN

Pasal 37

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 Provinsi; dan/atau
b. sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perindang-undangan.

BAB VIII
KETENTUAN PENUTUP

Pasal 38

Pada saat Peraturan Gubernur ini mulai berlaku, Peraturan Gubernur Jawa Tengah Nomor 10 Tahun 2019 tentang Pedoman Penyelenggaraan Persandian Untuk Pengamanan Informasi di Lingkungan Pemerintahan Daerah Provinsi danKabupaten/Kota (Berita Negara Republik Indonesia Tahun 2017 Nomor 758), dicabut dan dinyatakan tidak berlaku.

Pasal 39

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur Jawa Tengah ini dengan penempatannya dalam Berita Daerah Provinsi Jawa Tengah.

Ditetapkan di Semarang
pada tanggal 1 Oktober 2021

GUBERNUR JAWA TENGAH,

Ttd

GANJAR PRANOWO

Diundangkan di Semarang
pada tanggal 1 Oktober 2021

Pj. SEKRETARIS DAERAH PROVINSI
JAWA TENGAH,

Ttd

PRASETYO ARIBOWO

BERITA DAERAH PROVINSI JAWA TENGAH TAHUN 2021 NOMOR 25

Salinan sesuai dengan aslinya
KEPALA BIRO HUKUM

IWANUDIN ISKANDAR
Pembina Utama Muda
NIP. 19711207 199503 1 003