SALINAN

GUBERNUR DAERAH KHUSUS
IBUKOTA JAKARTA

PERATURAN GUBERNUR DAERAH KHUSUS
IBUKOTA JAKARTA

NOMOR 15 TAHUN 2025

TENTANG

PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR DAERAH KHUSUS IBUKOTA JAKARTA,

Menimbang : a. bahwa dalam rangka optimalisasi pelaksanaan persandian di daerah yang berfungsi sebagai pengamanan informasi perlu pedoman penggunaan persandian;

b. bahwa sesuai ketentuan Pasal 8 ayat (1) Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, Gubernur menetapkan aturan mengenai tata kelola keamanan informasi;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Gubernur tentang Pelaksanaan Persandian untuk Pengamanan Informasi;

Mengingat : 1. Undang-Undang Nomor 29 Tahun 2007 tentang Pemerintahan Provinsi Daerah Khusus Ibukota Jakarta sebagai Ibukota Negara Kesatuan Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 93, Tambahan Lembaran Negara Republik Indonesia Nomor 4744);

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);

3. 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 beberapa kali diubah terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);

4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

5. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);

6. Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 99);

7. 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);

8. 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);

9. 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);

10. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber (Berita Negara Republik Indonesia Tahun 2024 Nomor 43);

11. Peraturan Gubernur Nomor 43 Tahun 2022 tentang Pembangunan dan Pengembangan Aplikasi Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Provinsi Daerah Khusus Ibukota Jakarta Tahun 2022 Nomor 71019);

12. Peraturan Gubernur Nomor 68 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Provinsi Daerah Khusus Ibukota Jakarta Tahun 2022 Nomor 71026);

MEMUTUSKAN:

Menetapkan : PERATURAN GUBERNUR TENTANG PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Provinsi Daerah Khusus lbukota Jakarta yang selanjutnya disebut Provinsi DKI Jakarta adalah provinsi yang mempunyai kekhususan dalam penyelenggaraan pemerintahan daerah karena kedudukannya sebagai Ibukota Negara Kesatuan Republik Indonesia.

2. Pemerintah Provinsi DKI Jakarta adalah Gubernur dan perangkat daerah Provinsi DKI Jakarta sebagai unsur penyelenggara pemerintahan Provinsi DKI Jakarta.

3. Gubernur adalah Kepala Daerah Provinsi DKI Jakarta yang karena jabatannya berkedudukan juga sebagai wakil Pemerintah di wilayah Provinsi DKI Jakarta.

4. Sekretaris Daerah adalah Sekretaris Daerah Provinsi DKI Jakarta.

5. Perangkat Daerah adalah Perangkat Daerah Provinsi DKI Jakarta.

6. Unit Kerja pada Perangkat Daerah adalah Unit Kerja pada Perangkat Daerah Provinsi DKI Jakarta.

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. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.

9. Data adalah catatan atas kumpulan fakta atau deskripsi berupa angka, karakter, simbol, gambar, peta, tanda, isyarat, tulisan, suara, dan/atau bunyi yang mempresentasikan keadaan sebenarnya atau menunjukkan suatu ide, objek, kondisi, atau situasi.

10. 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.

11. 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.

12. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan Informasi.

13. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.

14. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi elektronik.

15. Keamanan Siber adalah upaya adaptif dan inovatif untuk melindungi seluruh lapisan ruang siber termasuk aset Informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik bersifat teknis maupun sosial.

16. Keamanan Sandi adalah kegiatan dan tindakan pencegahan atau penanggulangan yang dilakukan secara terencana, terarah, dan berkesinambungan untuk melindungi kelangsungan Persandian dari segala hakikat ancaman dan gangguan.

17. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik.

18. Tim Tanggap Insiden Siber adalah tim yang bertanggung jawab menangani Insiden Siber di lingkungan Pemerintah Provinsi DKI Jakarta.

19. 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.

20. Layanan Keamanan adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan urusan pemerintahan bidang Persandian dan yang memiliki nilai manfaat.

21. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang Keamanan Siber dan Persandian

22. Pusat Operasi Pengamanan Siber adalah pusat operasi yang memiliki tugas penyusunan, pelaksanaan, evaluasi, dan pelaporan kendali operasi Keamanan Siber.

23. Sumber Daya Manusia adalah pegawai negeri sipil dan pegawai pemerintah dengan perjanjian kerja Pemerintah Provinsi DKI Jakarta yang diangkat dalam jabatan oleh pejabat pembina kepegawaian dan diserahi tugas dalam suatu jabatan pemerintahan dalam urusan pengelolaan pemerintahan di bidang Persandian untuk Pengamanan Informasi dan diberikan penghasilan berdasarkan ketentuan peraturan perundang-undangan.

Pasal 2

Pelaksanaan Persandian untuk Pengamanan Informasi bertujuan:

a. menciptakan harmonisasi dalam penyelenggaraan urusan pemerintahan di bidang Persandian;

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/Unit Kerja pada Perangkat Daerah.

Pasal 3

(1) Pelaksanaan Persandian untuk Pengamanan Informasi meliputi:

a. penyelenggaraan Persandian untuk Pengamanan Informasi; dan

b. penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.

(2) Pelaksanaan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Sekretaris Daerah.

(3) Penanggung jawab pelaksanaan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.

Pasal 4

Pelaksana Persandian untuk Pengamanan Informasi terdiri dari:

a. Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian; dan

b. Perangkat Daerah/Unit Kerja pada Perangkat Daerah.

BAB II

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

Bagian Kesatu

Umum

Pasal 5

(1) Penyelenggaraan Persandian untuk Pengamanan Informasi sebagaimana dimaksud dalam Pasal 3 ayat (1) 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) Penyelenggaraan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

(3) Dalam penyelenggaraan Persandian untuk Pengamanan Informasi, Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian melakukan koordinasi dan konsultasi kepada lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang Keamanan Siber dan Persandian.

(4) Penyelenggaraan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 6

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf a meliputi:

a. penyusunan kebijakan Keamanan Sandi; dan

b. penyusunan kebijakan Keamanan Siber.

Bagian Kedua

Penyusunan Kebijakan Pengamanan Informasi

Paragraf 1

Penyusunan Kebijakan Keamanan Sandi

Pasal 7

(1) Penyusunan kebijakan Keamanan Sandi sebagaimana dimaksud dalam Pasal 6 huruf a meliputi:

a. rencana strategis Keamanan Sandi; dan

b. tata kelola Keamanan Sandi.

(2) Penyusunan kebijakan Keamanan Sandi sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

(3) Dalam melakukan penyusunan dan penetapan aturan mengenai rencana strategis dan tata kelola Keamanan Sandi, Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian melakukan koordinasi dan konsultasi kepada lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang Keamanan Siber dan Persandian.

Pasal 8

(1) Penyusunan rencana strategis Keamanan Sandi sebagaimana dimaksud dalam Pasal 7 ayat (1) huruf a memuat:

a. tujuan, sasaran, program, kegiatan, dan target pelaksanaan Keamanan Sandi; dan

b. peta rencana penyelenggaraan Keamanan Sandi yang merupakan penjabaran dari tahapan rencana strategis.

(2) Penyusunan rencana strategis Keamanan Sandi sebagaimana dimaksud pada ayat (1) untuk jangka waktu 5 (lima) tahun dilakukan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

(3) Hasil penyusunan rencana strategis Keamanan Sandi dan peta rencana penyelenggaraan Keamanan Sandi sebagaimana dimaksud pada ayat (2) diintegrasikan dalam rencana pembangunan jangka menengah daerah.

Pasal 9

(1) Tata kelola Keamanan Sandi sebagaimana dimaksud dalam Pasal 7 ayat (1) huruf b paling sedikit mengatur tentang standar teknis dan prosedur Keamanan Sandi untuk:

a. Jaringan Intra Pemerintah Provinsi DKI Jakarta;

b. komunikasi intra Pemerintah Provinsi DKI Jakarta; dan

c. persuratan elektronik.

(2) Tata kelola Keamanan Sandi sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Kepala Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian atas nama Gubernur.

Paragraf 2

Penyusunan Kebijakan Keamanan Siber

Pasal 10

(1) Penyusunan Kebijakan Keamanan Siber sebagaimana dimaksud dalam Pasal 6 huruf b meliputi:

a. rencana strategis Keamanan Siber;

b. arsitektur Keamanan Siber; dan

c. tata kelola Keamanan Siber.

(2) Penyusunan kebijakan Keamanan Siber sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

(3) Dalam melakukan penyusunan dan penetapan aturan mengenai rencana strategis, arsitektur dan tata kelola Keamanan Siber, Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian melakukan koordinasi dan konsultasi kepada lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang Keamanan Siber dan Persandian.

Pasal 11

(1) Penyusunan rencana strategis Keamanan Siber sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf a memuat:

a. tujuan, sasaran, program, kegiatan, dan target pelaksanaan Keamanan Siber; dan

b. peta rencana penyelenggaraan Keamanan Siber yang merupakan penjabaran dari tahapan rencana strategis.

(2) Program kerja Keamanan Siber sebagaimana dimaksud pada ayat (1) huruf a paling sedikit memuat:

a. edukasi kesadaran Keamanan Siber;

b. penilaian kerentanan Keamanan Siber;

c. peningkatan Keamanan Siber;

d. penanganan insiden Keamanan Siber; dan

e. audit Keamanan Siber.

(3) Penyusunan rencana strategis Keamanan Siber sebagaimana dimaksud pada ayat (1) untuk jangka waktu 5 (lima) tahun dilakukan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

(4) Hasil penyusunan rencana strategis Keamanan Siber dan peta rencana penyelenggaraan Keamanan Siber sebagaimana dimaksud pada ayat (3) diintegrasikan dalam rencana pembangunan jangka menengah daerah.

Pasal 12

(1) Arsitektur Keamanan Siber sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf b memuat:

a. infrastruktur;

b. desain dan aplikasi keamanan perangkat teknologi Informasi; dan

c. keamanan jaringan.

(2) Arsitektur Keamanan Siber sebagaimana dimaksud pada ayat (1) diintegrasikan dalam dokumen arsitektur SPBE.

Pasal 13

(1) Tata kelola Keamanan Siber sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf c minimal mengatur tentang standar teknis dan prosedur Keamanan Siber untuk:

a. keamanan Sumber Daya Manusia;

b. keamanan perangkat teknologi informasi dan komunikasi;

c. keamanan Jaringan Intra;

d. keamanan pusat data;

e. keamanan sistem penghubung layanan;

f. keamanan Data dan Informasi;

g. keamanan akses;

h. keamanan operasional;

i. keamanan komunikasi;

j. keamanan aplikasi;

k. pengendalian terhadap pihak ketiga;

l. penanganan insiden Keamanan Siber;

m. pengelolaan keberlangsungan layanan Teknologi Informasi dan Komunikasi;

n. audit internal Keamanan Siber; dan

o. aspek pengendalian Keamanan Siber lainnya.

(2) Pelaksanaan standar teknis dan prosedur Keamanan Siber sebagaimana dimaksud pada ayat (1) huruf a dikoordinasikan oleh tim koordinasi SPBE.

(3) Pelaksanaan standar teknis dan prosedur Keamanan Siber sebagaimana dimaksud pada ayat (1) huruf c, huruf d, huruf e, huruf n, dan huruf o dikoordinasikan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

(4) Pelaksanaan standar teknis dan prosedur Keamanan Siber sebagaimana dimaksud pada ayat (1) huruf b, huruf f, huruf g, huruf h, huruf i, huruf j, huruf k, huruf l dan huruf m dilaksanakan oleh Perangkat Daerah.

(5) Dalam hal Perangkat Daerah belum dapat melaksanakan ketentuan sebagaimana dimaksud pada ayat (4) secara mandiri, Perangkat Daerah berkoordinasi dengan Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang persandian.

(6) Penerapan standar teknis dan prosedur Keamanan Siber sebagaimana dimaksud pada ayat (1) disesuaikan dengan asas risiko kategori Sistem Elektronik meliputi:

a. Sistem Elektronik strategis;

b. Sistem Elektronik tinggi; dan

c. Sistem Elektronik rendah.

(7) Sistem Elektronik strategis sebagaimana dimaksud pada ayat (6) huruf a merupakan Sistem Elektronik yang berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara.

(8) Sistem Elektronik tinggi sebagaimana dimaksud pada ayat (6) huruf b merupakan Sistem Elektronik yang berdampak terbatas pada kepentingan sektor dan/atau daerah tertentu.

(9) Sistem Elektronik rendah sebagaimana dimaksud pada ayat (6) huruf c merupakan Sistem Elektronik lainnya yang tidak termasuk pada ayat (7) dan ayat (8).

(10) Kategori Sistem Elektronik menjadi pedoman dalam penguatan pelindungan infrastruktur Informasi vital.

(11) Penguatan pelindungan infrastruktur Informasi vital sebagaimana dimaksud pada ayat (10) meliputi:

a. penyelenggaraan pelindungan infrastruktur Informasi vital;

b. peningkatan pembinaan dan pengawasan penyelenggaraan pelindungan infrastruktur Informasi vital; dan

c. pelaksanaan pengukuran tingkat kematangan Keamanan Siber dan Keamanan Sandi.

(12) Pelindungan infrastruktur Informasi vital sebagaimana dimaksud pada ayat (11) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

(13) Tata kelola Keamanan Siber sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Kepala Dinas yang menyelenggarakan urusan pemerintahan di bidang Persandian atas nama Gubernur.

Pasal 14

(1) Dalam penyelenggaraan Keamanan Siber Perangkat Daerah menyusun dokumen manajemen risiko Keamanan Siber.

(2) Dokumen manajemen risiko Keamanan Siber sebagaimana dimaksud pada ayat (1) diintegrasikan dengan dokumen manajemen risiko SPBE.

Bagian Ketiga

Pengelolaan Sumber Daya Keamanan Informasi

Pasal 15

Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf b meliputi:

a. pengelolaan sumber daya Keamanan Sandi; dan

b. pengelolaan sumber daya Keamanan Siber.

Paragraf 1

Pengelolaan Sumber Daya Keamanan Sandi

Pasal 16

(1) Pengelolaan sumber daya Keamanan Sandi sebagaimana dimaksud dalam Pasal 15 huruf a meliputi:

a. pengelolaan aset Keamanan Sandi;

b. pengelolaan Sumber Daya Manusia Keamanan Sandi; dan

c. manajemen pengetahuan Keamanan Sandi.

(2) Pengelolaan aset Keamanan Sandi sebagaimana dimaksud pada ayat (1) huruf a, meliputi perangkat yang digunakan untuk pelindungan Informasi pada:

a. kegiatan penting Pemerintah Provinsi DKI Jakarta; dan

b. aset/fasilitas penting milik atau yang akan digunakan Pemerintah Provinsi DKI Jakarta.

(3) Pengelolaan aset Keamanan Sandi sebagaimana dimaksud pada ayat (1) huruf a dikoordinasikan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

(4) Pengelolaan Sumber Daya Manusia Keamanan Sandi sebagaimana dimaksud pada ayat (1) huruf b dikoordinasikan oleh:

a. Perangkat Daerah yang membidangi pengelolaan kepegawaian terkait perencanaan, pengadaan, pembinaan jabatan fungsional dan pendayagunaan Sumber Daya Manusia; dan

b. Perangkat Daerah yang membidangi pendidikan dan pelatihan terkait pengembangan kompetensi Sumber Daya Manusia.

(5) Manajemen pengetahuan Keamanan Sandi sebagaimana dimaksud pada ayat (1) huruf c dikoordinasikan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang pendidikan dan pelatihan.

Paragraf 2

Pengelolaan Sumber Daya Keamanan Siber

Pasal 17

(1) Pengelolaan sumber daya Keamanan Siber sebagaimana dimaksud dalam Pasal 15 huruf b meliputi:

a. pengelolaan aset teknologi Keamanan Siber;

b. pengelolaan Sumber Daya Manusia Keamanan Siber; dan

c. manajemen pengetahuan Keamanan Siber.

(2) Pengelolaan aset teknologi Keamanan Siber sebagaimana dimaksud pada ayat (1) huruf a, meliputi perangkat yang digunakan untuk:

a. mengidentifikasi;

b. mendeteksi;

c. memproteksi;

d. menganalisis;

e. menanggulangi; dan/atau

f. memulihkan insiden Keamanan Siber.

(3) Pengelolaan aset teknologi Keamanan Siber sebagaimana dimaksud pada ayat (1) huruf a dikoordinasikan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

(4) Pengelolaan Sumber Daya Manusia Keamanan Siber sebagaimana dimaksud pada ayat (1) huruf b dikoordinasikan oleh:

a. Perangkat Daerah yang membidangi pengelolaan kepegawaian terkait perencanaan, pengadaan, pembinaan jabatan fungsional dan pendayagunaan Sumber Daya Manusia; dan

b. Perangkat Daerah yang membidangi pendidikan dan pelatihan terkait pengembangan kompetensi Sumber Daya Manusia.

(5) Manajemen pengetahuan Keamanan Siber sebagaimana dimaksud pada ayat (1) huruf c dikoordinasikan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang pendidikan dan pelatihan.

Bagian Keempat

Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik

Paragraf 1

Pengamanan Sistem Elektronik

Pasal 18

(1) Pengamanan Sistem Elektronik meliputi penjaminan terhadap:

a. kerahasiaan, keutuhan, ketersediaan, keaslian, dan nirsangkal terhadap Data dan Informasi;

b. ketersediaan infrastruktur elektronik; dan

c. keutuhan, ketersediaan, dan keaslian aplikasi Sistem Elektronik.

(2) Pelaksanaan Pengamanan Sistem Elektronik sebagaimana dimaksud pada ayat (1) dilengkapi dengan pemenuhan ketentuan perundangan yang mengatur tentang penerapan manajemen risiko SPBE.

(3) Pengamanan Sistem Elektronik dilaksanakan pada tahapan:

a. sebelum terjadi insiden;

b. saat terjadi insiden; dan

c. setelah terjadi insiden.

(4) Pengamanan Sistem Elektronik pada tahapan sebelum terjadi insiden sebagaimana dimaksud pada ayat (3) huruf a dilaksanakan melalui:

a. edukasi Keamanan Siber;

b. simulasi penanganan Insiden Siber;

c. pencegahan insiden Keamanan Siber; dan

d. peningkatan keamanan Sistem Elektronik dilaksanakan paling sedikit melalui:

1. menerapkan standar teknis dan prosedur keamanan Sistem Elektronik; dan
2. menguji fungsi keamanan terhadap aplikasi dan infrastruktur Sistem Elektronik.

(5) Pengamanan Sistem Elektronik sebagaimana dimaksud pada ayat (3) dikoordinasikan oleh Tim Tanggap Insiden Siber.

(6) Penerapan pengamanan Sistem Elektronik sebagaimana dimaksud pada ayat (4) dilaksanakan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

(7) Dalam penerapan pengamanan Sistem Elektronik, Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian melakukan koordinasi dan konsultasi kepada BSSN.

Pasal 19

(1) Dalam melaksanakan pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 18 melalui:

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.

(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.

Pasal 20

(1) Dalam melaksanakan pengamanan Sistem Elektronik, setiap layanan publik dan layanan pemerintahan berbasis elektronik pada Pemerintah Provinsi DKI Jakarta wajib menggunakan Sertifikat Elektronik yang dimohonkan kepada BSSN melalui Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

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

(3) Fasilitasi pengelolaan Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

(4) Ketentuan lebih lanjut mengenai fasilitasi pengelolaan Sertifikat Elektronik sebagaimana dimaksud pada ayat (3) ditetapkan dengan Keputusan Gubernur.

Paragraf 2

Tim Tanggap Insiden Siber dan Pusat Operasi Keamanan Siber

Pasal 21

(1) Tim Tanggap Insiden Siber memiliki tugas untuk melakukan paling sedikit:

a. penanggulangan dan pemulihan Insiden Siber;

b. penyampaian Informasi Insiden Siber kepada pihak terkait; dan

c. diseminasi Informasi untuk mencegah dan/atau mengurangi dampak dari Insiden Siber.

(2) Struktur organisasi dan susunan keanggotaan Tim Tanggap Insiden Siber sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Sekretaris Daerah.

Pasal 22

(1) Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian membentuk Pusat Operasi Keamanan Siber.

(2) Pusat Operasi Keamanan Siber sebagaimana dimaksud pada ayat (1) dilengkapi dengan:

a. ruang kendali;

b. sarana dan prasarana pendukung layanan; dan

c. Sumber Daya Manusia Keamanan Siber.

(3) Pengelolaan Pusat Operasi Keamanan Siber sebagaimana dimaksud pada ayat (2) dilaksanakan oleh tim Pusat Operasi Keamanan Siber.

(4) Tim Pusat Operasi Keamanan Siber sebagaimana dimaksud pada ayat (3) memiliki tugas untuk melakukan paling sedikit:

a. pencegahan insiden Keamanan Siber;

b. melakukan uji coba kerentanan Keamanan Siber;

c. pemantauan dan pendeteksian serangan Keamanan Siber; dan

d. penanggulangan dan pemulihan insiden Keamanan Siber.

(5) Struktur organisasi dan susunan keanggotaan tim Pusat Operasi Keamanan Siber sebagaimana dimaksud pada ayat (3) ditetapkan dengan Keputusan Kepala Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

Pasal 23

Mekanisme pengamanan Sistem Elektronik pada tahapan sebelum, saat, dan sesudah Insiden Siber oleh Tim Tanggap Insiden Siber dan tim Pusat Operasi Keamanan Siber sebagaimana dimaksud dalam Pasal 21 dan Pasal 22 ditetapkan dengan Keputusan Sekretaris Daerah selaku Ketua Tim Koordinasi SPBE.

Paragraf 3

Pengamanan Informasi Nonelektronik

Pasal 24

(1) Pengamanan Informasi nonelektronik 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.

Bagian Kelima

Penyediaan Layanan Keamanan Informasi

Pasal 25

Penyediaan layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf d meliputi:

a. penyediaan layanan Keamanan Sandi; dan

b. penyediaan layanan Keamanan Siber.

Paragraf 1

Penyediaan Layanan Keamanan Sandi

Pasal 26

(1) Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian menyediakan layanan Keamanan Sandi terhadap:

   a. unsur pimpinan Pemerintah Provinsi DKI Jakarta;

   b. aparatur sipil negara Pemerintah Provinsi DKI Jakarta; dan

   c. pegawai non aparatur sipil negara yang bertugas di lingkungan Pemerintah Provinsi DKI Jakarta.

(2) Layanan Keamanan Sandi sebagaimana dimaksud pada ayat (1) meliputi:

a. pelindungan Informasi pada kegiatan penting Pemerintah Provinsi DKI Jakarta melalui teknik pengamanan gelombang frekuensi atau sinyal;

b. pelindungan Informasi pada aset/fasilitas penting milik atau yang akan digunakan Pemerintah Provinsi DKI Jakarta melalui kegiatan kontra penginderaan; dan

c. jenis layanan Keamanan Sandi lainnya.

(3) Dalam penyediaan layanan Keamanan Sandi, Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian melakukan koordinasi dan konsultasi kepada lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang Keamanan Siber dan Persandian.

(4) Mekanisme penyediaan layanan Keamanan Sandi sebagaimana dimaksud pada ayat (3) ditetapkan dengan Keputusan Kepala Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

Paragraf 2

Penyediaan Layanan Keamanan Siber

Pasal 27

(1) Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian menyediakan layanan Keamanan Siber terhadap:

a. unsur pimpinan Pemerintah Provinsi DKI Jakarta;

b. aparatur sipil negara Pemerintah Provinsi DKI Jakarta; dan

c. pegawai non aparatur sipil negara yang bertugas di lingkungan Pemerintah Provinsi DKI Jakarta.

(2) Layanan Keamanan Siber sebagaimana dimaksud pada ayat (1) meliputi:

a. identifikasi kerentanan dan penilaian risiko terhadap Sistem Elektronik;

b. peningkatan keamanan Sistem Elektronik;

c. penerapan Sertifikat Elektronik;

d. literasi Keamanan Siber;

e. koordinasi dan konsultasi peningkatan kompetensi Sumber Daya Manusia di bidang Keamanan Siber dan/atau Persandian;

f. penanganan Insiden Siber; dan

g. jenis layanan Keamanan Siber lainnya.

(3) Dalam penyediaan layanan Keamanan Siber, Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian melakukan koordinasi dan konsultasi kepada lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang Keamanan Siber dan Persandian.

(4) Mekanisme penyediaan layanan Keamanan Siber sebagaimana dimaksud pada ayat (3) ditetapkan dengan Keputusan Kepala Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

BAB III

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH

Pasal 28

(1) Pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf b meliputi:

a. jaring komunikasi sandi antar Perangkat Daerah;

b. jaring komunikasi sandi internal Perangkat Daerah; dan

c. jaring komunikasi sandi pimpinan Pemerintah Provinsi DKI Jakarta.

(2) Pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Gubernur.

BAB IV

STRATEGI KESIAPSIAGAAN DAN KETAHANAN KEAMANAN SIBER

Pasal 29

Kesiapsiagaan dan ketahanan Keamanan Siber meliputi:

a. pembangunan kapabilitas tanggap Insiden Siber yang efektif dan efisien;

b. perumusan dan penetapan rencana kontingensi untuk pengelolaan Insiden Siber;

c. penyelenggaraan penanganan Insiden Siber; dan

d. penguatan pertukaran pengelolaan Insiden Siber.

BAB V

KERJA SAMA DAN KOLABORASI

Pasal 30

Kerja sama dan kolaborasi pengamanan siber meliputi:

a. peningkatan inisiatif kerja sama dan kolaborasi dalam rangka pengamanan siber; dan

b. peningkatan kerja sama praktis, berbagi Informasi, dan praktik terbaik dalam menghadapi Insiden Siber.

BAB VI

PEMANTAUAN DAN EVALUASI

Pasal 31

(1) Pemantauan dan evaluasi pelaksanaan Persandian untuk Pengamanan Informasi dilaksanakan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

(2) Perangkat Daerah menyampaikan laporan hasil pelaksanaan pemantauan dan evaluasi Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1) disampaikan kepada Gubernur melalui Sekretaris Daerah dan Kepala BSSN.

Pasal 32

Pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Provinsi DKI Jakarta dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VII

PENDANAAN

Pasal 33

Pembiayaan pelaksanaan Persandian untuk Pengamanan Informasi dapat bersumber dari:

a. anggaran pendapatan dan belanja daerah; dan

b. sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB VIII

KETENTUAN PERALIHAN

Pasal 34

(1) Sertifikat Elektronik yang telah dikeluarkan sebelum berlakunya Peraturan Gubernur ini tetap berlaku sampai dengan habis masa berlakunya.

(2) Terhadap permohonan Sertifikat Elektronik yang sedang dalam proses pada Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian harus menyesuaikan dengan Peraturan Gubernur ini.

BAB IX

KETENTUAN PENUTUP

Pasal 35

Pada saat Peraturan Gubernur ini mulai berlaku:

a. Peraturan Gubernur Nomor 11 Tahun 2018 tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi (Berita Daerah Provinsi Daerah Khusus Ibukota Jakarta Tahun 2018 Nomor 12004); dan
b. Peraturan Gubernur Nomor 69 Tahun 2018 tentang Penggunaan Sertifikat Elektronik (Berita Daerah Provinsi Daerah Khusus Ibukota Jakarta Tahun 2018 Nomor 72029),

dicabut dan dinyatakan tidak berlaku.

Pasal 36

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur ini dengan penempatannya dalam Berita Daerah Provinsi Daerah Khusus Ibukota Jakarta.

Ditetapkan di Jakarta
pada tanggal 2 Mei 2025

GUBERNUR DAERAH KHUSUS
IBUKOTA JAKARTA,

ttd

PRAMONO ANUNG

Diundangkan di Jakarta
pada tanggal 6 Mei 2025

SEKRETARIS DAERAH PROVINSI DAERAH KHUSUS
IBUKOTA JAKARTA,

ttd

MARULLAH MATALI

BERITA DAERAH PROVINSI DAERAH KHUSUS IBUKOTA JAKARTA
TAHUN 2025 NOMOR 71004

Salinan sesuai dengan aslinya
KEPALA BIRO HUKUM SEKRETARIAT DAERAH
PROVINSI DAERAH KHUSUS IBUKOTA JAKARTA,

SIGIT PRATAMA YUDHA
NIP 197612062002121009