



WALIKOTA MAKASSAR
PROVINSI SULAWESI SELATAN

PERATURAN WALIKOTA MAKASSAR
NOMOR 53 TAHUN 2021

TENTANG

PENERAPAN SERTIFIKAT ELEKTRONIK
PADA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALIKOTA MAKASSAR,

- Menimbang :
- a. bahwa berdasarkan ketentuan dalam Pasal 2 ayat (1) dan ayat (2) serta Pasal 51 ayat (1) Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang menyatakan Penyelenggaraan Sistem Elektronik dilaksanakan oleh Penyelenggara Sistem Elektronik (PSrE) yang meliputi Penyelenggara Sistem Elektronik lingkup Publik dan lingkup Privat yang wajib memiliki sertifikat elektronik;
 - b. bahwa Balai Sertifikasi Elektronik (BsrE) merupakan unit pelaksana teknis di Badan Siber dan Sandi Negara (BSSN) yang mempunyai tugas melaksanakan penyelenggaraan sertifikasi elektronik guna mendukung sistem pemerintahan berbasis elektronik, yang dibentuk oleh Lembaga Sandi Negara yang pada Surat Keputusan Nomor 936 Tahun 2019 oleh Kementerian Komunikasi dan Informatika sebagai Penyelenggara Sistem Elektronik (PSrE) dengan status Pengakuan Terdaftar per tanggal 12 November 2019;
 - c. bahwa Pemerintah Daerah menginginkan pelaksanaan pemerintahan yang berbasis elektronik untuk lebih menunjang penyelenggaraan pemerintahan daerah yang efektif, efisien dan akuntabel, serta mempercepat pelayanan publik, maka untuk melindungi segala informasi dari risiko kebocoran data, modifikasi data, pemalsuan data, dan penyangkalan terhadap data yang ditransaksikan serta perlindungan sistem elektronik milik Pemerintah Daerah, dipandang perlu adanya pedoman dalam Penerapan Sertifikat Elektronik bagi hal tersebut;
 - d. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a, huruf b dan huruf c, maka perlu menetapkan Peraturan Walikota Makassar tentang Penerapan Sertifikat Elektronik pada Sistem Pemerintahan Berbasis Elektronik.
- Mengingat :
1. Undang-Undang Nomor 29 Tahun 1959 tentang Pembentukan Daerah Tingkat II di Sulawesi (Lembaran Negara Tahun 1959 Nomor 74, Tambahan Lembaran Negara Republik Indonesia Nomor 1822);
 2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);

3. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234) sebagaimana telah diubah dengan Undang-Undang Republik Indonesia Nomor 15 Tahun 2019 tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 183, Tambahan Lembaran Negara Republik Indonesia Nomor 6398);
4. Undang-Undang Nomor 5 Tahun 2014 tentang Aparatur Sipil Negara (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 6, Tambahan Lembaran Negara Republik Indonesia Nomor 5494);
5. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
6. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601) sebagaimana telah diubah 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);
7. Peraturan Pemerintah Nomor 51 Tahun 1971 tentang Perubahan Batas-batas Daerah Kotamadya Makassar Dan Kabupaten-kabupaten Gowa, Maros Dan Pangkajene dan Kepulauan Dalam Lingkungan Daerah Propinsi Sulawesi Selatan (Lembaran Negara Republik Indonesia Tahun 1971 Nomor 65, Tambahan Lembaran Negara Republik Indonesia Nomor 2970);
8. Peraturan Pemerintah Nomor 86 Tahun 1999 tentang Perubahan Nama Kota Ujung Pandang menjadi Kota Makassar dalam wilayah Propinsi Sulawesi Selatan (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 193);
9. Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 114, Tambahan Lembaran Negara Republik Indonesia Nomor 5887) sebagaimana telah diubah dengan Peraturan Pemerintah Nomor 72 Tahun 2019 tentang Perubahan Atas Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 187, Tambahan Lembaran Negara Republik Indonesia Nomor 6402);
10. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 71, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
11. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

12. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036) sebagaimana telah diubah terakhir dengan Peraturan Menteri Dalam Negeri Nomor 120 Tahun 2018 tentang Perubahan Atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2018 Nomor 157);
13. Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik (Berita Negara Republik Indonesia Tahun 2018 Nomor 1238).

MEMUTUSKAN:

Menetapkan : **PERATURAN WALIKOTA MAKASSAR TENTANG PENERAPAN SERTIFIKAT ELEKTRONIK PADA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.**

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Walikota ini yang dimaksud dengan:

1. Daerah adalah Kota Makassar
2. Pemerintah Daerah adalah Pemerintah Kota Makassar.
3. Walikota adalah Walikota Makassar.
4. Perangkat Daerah adalah unsur pembantu Kepala Daerah dan DPRD dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan daerah.
5. Dinas Komunikasi dan Informatika yang selanjutnya disebut Diskominfo adalah Dinas Komunikasi dan Informatika Kota Makassar.
6. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah suatu sistem tata kelola pemerintahan yang memanfaatkan teknologi informasi secara menyeluruh dan terpadu dalam pelaksanaan administrasi pemerintahan dan penyelenggaraan pelayanan publik pada Pemerintah Daerah.
7. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi elektronik.
8. Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.
9. Informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode Akses, simbol, atau peforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh yang mampu memahaminya.
10. Dokumen elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memilki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
11. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subyek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik.
12. 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.

13. Pemilik sertifikat elektronik adalah individu atau badan hukum yang telah menyetujui perjanjian penggunaan Sertifikat Elektronik
14. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
15. Pasangan kunci kriptografi adalah kunci privat dan kunci publik yang saling berasosiasi.
16. Kunci privat adalah salah satu kunci dari pasangan kunci kriptografi yang hanya disimpan dan dirahasiakan oleh pengguna serta digunakan untuk melakukan Tanda Tangan Elektronik atau untuk membuka pesan yang disandi menggunakan Kunci publik pada Sertifikat elektronik.
17. Kunci publik adalah salah satu kunci dari Pasangan kunci kriptografi yang dimiliki oleh pihak tertentu dan dapat dipergunakan oleh pihak lain untuk melakukan pertukaran informasi secara aman dengan pemilik kunci tersebut.
18. *Passphrase* adalah serangkaian angka dan/atau huruf dan/atau karakter tertentu yang digunakan sebagai alat autentikasi untuk melakukan akses ke pasangan Kunci privat dan Sertifikat elektronik.
19. Keamanan informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan Nir penyangkalan informasi.
20. Otoritas Sertifikat Digital yang selanjutnya disingkat OSD adalah sistem elektronik yang berfungsi sebagai layanan Sertifikasi elektronik di Badan Siber dan Sandi Negara.
21. Balai Sertifikasi Elektronik yang selanjutnya disingkat BSrE merupakan unit pelaksana teknis penyelenggara OSD yang berada di bawah dan bertanggung jawab kepada Kepala Badan Siber dan Sandi Negara.
22. Otoritas Pendaftaran yang selanjutnya disingkat OP adalah unit 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.
23. Verifikator adalah personil yang bertanggung jawab melakukan pemeriksaan, persetujuan atau penolakan atas setiap pengajuan berkas permohonan penerbitan, pembaruan dan pencabutan sertifikat elektronik yang diajukan oleh pemilik (atau calon pemilik) sertifikat elektronik.
24. Auditor keamanan adalah personel yang bertanggung jawab dalam mengaudit kesesuaian dan keamanan OSD serta otoritas pendaftaran.
25. *Certificate Policy* yang selanjutnya disingkat CP adalah ketentuan dan kebijakan yang mengatur semua pihak yang terkait dengan penggunaan Sertifikat elektronik yang dikeluarkan oleh BSrE.
26. *Certificate Practice Statement* yang selanjutnya disingkat CPS adalah pernyataan tentang bagaimana prosedur terkait penerbitan, penggunaan, pengaturan, penarikan, dan pembaruan Sertifikat elektronik oleh BSrE.
27. Aplikasi adalah komponen sistem informasi yang digunakan untuk menjalankan fungsi, proses, dan mekanisme kerja yang mendukung pelaksanaan pelayanan publik.
28. Insiden keamanan informasi adalah merupakan satu atau serangkaian kejadian Keamanan Informasi yang memiliki peluang signifikan bagi pelemahan dan/atau gangguan bisnis proses dan peningkatan ancaman Keamanan Informasi.

BAB II MAKSUD DAN TUJUAN

Pasal 2

Peraturan Walikota ini dimaksudkan sebagai pedoman bagi seluruh Perangkat Daerah dalam penyelenggaraan dan penerapan Sertifikat Elektronik untuk pengamanan informasi pada transaksi elektronik yang dilaksanakan dan dikembangkan pada SPBE di lingkungan Pemerintah Daerah.

Pasal 3

Peraturan Walikota ini bertujuan untuk:

- a. menjamin keutuhan, kerahasiaan, otentikasi dan nir penyangkalan Dokumen elektronik di Pemerintah Daerah;
- b. meningkatkan kapabilitas dan tata kelola keamanan informasi dalam penyelenggaraan Sistem elektronik di Daerah;
- c. meningkatkan efisiensi dan efektifitas penyelenggaraan pemerintahan dan layanan publik di lingkungan Pemerintah Daerah;
- d. menciptakan hubungan komunikasi yang baik dan aman pada seluruh Perangkat Daerah;
- e. membantu Perangkat Daerah dalam pengamanan informasi milik Pemerintah Daerah;
- f. meningkatkan kinerja Perangkat Daerah dalam pelaksanaan pada SPBE;
- g. menjamin integritas informasi untuk memastikan bahwa informasi tidak diubah/dimodifikasi selama penyimpanan atau pada saat dikirimkan; dan
- h. meningkatkan kepercayaan dan penerimaan masyarakat terhadap implementasi sistem elektronik.

BAB III RUANG LINGKUP

Pasal 4

Ruang lingkup penerapan Sertifikat elektronik di lingkungan Pemerintah Daerah ini meliputi:

- a. penyelenggaraan Sertifikat Elektronik;
- b. pemanfaatan dan layanan Sertifikat elektronik pada SPBE;
- c. tanggung jawab, kewajiban, larangan, ketentuan penyimpanan bagi Pemilik Sertifikat elektronik dan konsekuensi hukum atas persetujuan perjanjian Pemilik Sertifikat elektronik; dan
- b. penyelenggaraan operasional dukungan Sertifikat elektronik untuk pengamanan informasi.

BAB IV PENYELENGGARAAN SERTIFIKAT ELEKTRONIK

Pasal 5

- (1) Penyelenggaraan sertifikat elektronik di Pemerintah Daerah dilaksanakan sesuai ketentuan yang ditetapkan oleh BSrE yang tidak bertentangan dengan ketentuan peraturan perundang-undangan.
- (2) Pihak yang terlibat dalam penyelenggaraan Sertifikasi elektronik sebagaimana dimaksud pada ayat (1) terdiri dari:
 - a. Penyelenggara Sertifikat Elektronik yaitu BSrE atau penyelenggara Sertifikat Elektronik lain sesuai dengan ketentuan peraturan perundang-undangan;
 - b. OP; dan
 - c. Pemilik Sertifikat Elektronik.

Pasal 6

OP sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b memiliki tugas dan fungsi sebagai berikut:

- a. melakukan identifikasi dan analisis kebutuhan sertifikat elektronik;
- b. melakukan pengembangan atau memberikan masukan kepada Perangkat Daerah yang membidangi aplikasi untuk membuat sistem/aplikasi pendukung penggunaan Sertifikat Elektronik;

- c. memberikan rekomendasi yang ditujukan kepada BSrE terkait permohonan penerbitan, pembaruan, dan pencabutan sertifikat elektronik;
- d. menyediakan serta menjaga keamanan infrastruktur yang dibutuhkan pada pemanfaatan sertifikat elektronik;
- e. menyusun SOP pemanfaatan sertifikat elektronik dengan asistensi dari BSrE;
- f. memberikan dukungan kepada BSrE dalam rangka sosialisasi dan bimbingan teknis terkait penyiapan dan pemanfaatan Sertifikat Elektronik yang diselenggarakan Pemerintah Daerah; dan
- g. membuat laporan hasil pemanfaatan sertifikat elektronik kepada BSrE minimal 1 (satu) tahun sekali.

Pasal 7

- (1) Pemilik Sertifikat Elektronik sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf c harus memenuhi persyaratan dan kriteria dalam melindungi Kunci Privat serta menyetujui ketentuan penggunaan Sertifikat Elektronik sebelum Sertifikat Elektronik diterbitkan.
- (2) Persyaratan dan kriteria sebagaimana dimaksud pada ayat (1), berpedoman kepada CP.

Pasal 8

- (1) Pengajuan permohonan penerbitan Sertifikat elektronik dapat dilakukan kepada OP dengan melampirkan sekurang-kurangnya:
 - a. fotokopi/scan Kartu Tanda Penduduk;
 - b. fotokopi/scan Surat Keputusan Pengangkatan Jabatan Terakhir;
 - c. email instansi yang menggunakan domain @makassar.go.id;
 - d. surat persetujuan Perjanjian Pemilik Sertifikat Elektronik;
 - e. surat permohonan kepada Diskominfo;
 - f. surat rekomendasi/pengantar untuk melakukan pendaftaran Sertifikat Elektronik; dan
 - g. Formulir pendaftaran Sertifikat Elektronik.
- (2) Terhadap permohonan sebagaimana dimaksud pada ayat (1) dilakukan verifikasi oleh Verifikator sebagai dasar permohonan untuk dapat diterima atau ditolak.
- (3) Dalam hal permohonan ditolak, OP memberikan jawaban disertai alasan secara tertulis kepada pemohon.
- (4) Dalam hal permohonan diterima, OP mengeluarkan surat rekomendasi permohonan penerbitan Sertifikat Elektronik yang diteruskan kepada BSrE.
- (5) OP melakukan pengarsipan berkas permohonan pendaftaran Sertifikat Elektronik baik dalam bentuk *hardfile* dan *softfile*.

BAB V

PEMANFAATAN LAYANAN SERTIFIKAT ELEKTRONIK PADA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Pasal 9

Pemanfaatan Layanan Sertifikat Elektronik pada SPBE, berupa:

- a. Tanda Tangan Elektronik;
- b. Perlindungan e-mail;
- c. Perlindungan dokumen;
- d. *Security socket layer server*, dan/atau
- e. *Security socket layer client*.

Pasal 10

Penggunaan Sertifikat Elektronik pada SPBE, meliputi:

- a. penyelenggaraan sistem dan transaksi elektronik;
- b. sistem naskah dinas secara digital;
- c. penggunaan aplikasi atau sistem informasi yang ditentukan dan/atau disediakan oleh Diskominfo dan/atau sistem informasi SKPD terkait di lingkungan Pemerintah Daerah; dan
- d. layanan pada SPBE lainnya yang ditentukan dan/atau disediakan oleh Pemerintah Daerah;

BAB VI TANGGUNG JAWAB, KEWAJIBAN, LARANGAN, PENYIMPANAN DAN KONSEKUENSI HUKUM BAGI PEMILIK SERTIFIKAT ELEKTRONIK

Bagian Kesatu Tanggung Jawab Pemilik Sertifikat Elektronik

Pasal 11

Pemilik Sertifikat Elektronik bertanggung jawab terhadap pengelolaan pasangan kunci kriptografi dan telah menyetujui untuk menggunakan kunci kriptografi dan Sertifikat Elektronik sesuai dengan kebijakan BSrE.

Bagian Kedua Kewajiban Pemilik Sertifikat Elektronik

Pasal 12

Pemilik Sertifikat Elektronik berkewajiban:

- a. memastikan semua informasi yang diberikan ke Diskominfo adalah benar;
- b. melindungi Sertifikat Elektronik agar tidak digunakan oleh orang lain;
- c. tidak menyerahkan/menguasakan penggunaan Sertifikat Elektronik kepada orang lain;
- d. mengajukan permohonan pencabutan Sertifikat Elektronik, jika mengetahui atau mencurigai bahwa sertifikat yang dimiliki digunakan oleh orang lain atau adanya kesalahan informasi atau kehilangan atau kebocoran kunci privat;
- e. melindungi kerahasiaan kunci privat, *Passphrase* atau hal lain yang digunakan untuk mengaktifkan kunci privat;
- f. tidak mengubah, mengganggu atau melakukan *reverse-engineering* dan berusaha untuk membocorkan layanan keamanan yang disediakan Diskominfo; dan
- g. bertanggung jawab atas penggunaan, penyimpanan, pembaruan, dan pemusnahan Sertifikat Elektronik dan kunci privat.

Bagian Ketiga Larangan Pemilik Sertifikat Elektronik

Pasal 13

Pengguna Sertifikat Elektronik dilarang:

- a. mengakses sistem yang bukan merupakan haknya;
- b. mengabaikan prinsip kehati-hatian guna menghindari penggunaan secara tidak sah terhadap data terkait pembuatan Tanda Tangan Elektronik;
- c. menunda-nunda untuk segera memberitahukan kepada seseorang yang oleh penanda tangan dianggap memercayai Tanda Tangan Elektronik atau kepada pihak pendukung layanan Tanda Tangan Elektronik jika:
 1. penanda tangan mengetahui bahwa data pembuatan Tanda Tangan Elektronik telah dibobol; dan/atau
 2. keadaan yang diketahui oleh penanda tangan dapat menimbulkan risiko yang berarti. kemungkinan akibat bobolnya data pembuatan Tanda Tangan Elektronik;

- d. menyampaikan fotokopi dokumen yang tidak sesuai dengan aslinya dan/atau dokumen yang dengan sengaja dipalsukan sebagai persyaratan permohonan Sertifikat Elektronik.

Bagian Keempat
Penyimpanan Data Sertifikat Elektronik

Pasal 14

Data yang terkait dengan penandatanganan Sertifikat Elektronik harus tersimpan di tempat atau sarana penyimpanan data, yang menggunakan sistem terpercaya milik penyelenggara Tanda Tangan Elektronik atau pendukung layanan Tanda Tangan Elektronik yang dapat mendeteksi adanya perubahan dengan memenuhi persyaratan:

- a. hanya orang yang diberi wewenang yang dapat memasukkan data baru, mengubah, menukar, atau mengganti data;
- b. informasi identitas penanda tangan dapat diperiksa keautentikannya;
- c. perubahan teknis lainnya yang melanggar persyaratan keamanan dapat dideteksi atau diketahui oleh penyelenggara; dan
- d. penandatanganan wajib menjaga kerahasiaan dan bertanggung jawab atas data pembuatan tanda tangan elektronik.

Pasal 15

Setiap Tanda Tangan Elektronik yang dibubuhkan pada Dokumen Elektronik menggunakan pasangan Kunci Privat dan Sertifikat Elektronik memiliki konsekuensi hukum yang sah, setara dengan tanda tangan basah sesuai ketentuan peraturan perundang-undangan.

BAB VII
PENYELENGGARAAN OPERASIONAL DUKUNGAN
SERTIFIKAT ELEKTRONIK UNTUK
PENGAMANAN INFORMASI

Pasal 16

Kegiatan operasional dukungan Sertifikat Elektronik melalui sistem OSD merupakan kegiatan operasional yang terkait dengan kriptografi untuk mendukung terciptanya keamanan informasi di Lingkungan Pemerintah Daerah.

Pasal 17

Dalam penyelenggaraan operasional Sertifikat Elektronik melalui sistem OSD sebagaimana dimaksud dalam Pasal 16, Diskominfo berkoordinasi dengan BsrE, Badan Siber dan Sandi Negara sebagai Instansi Pembina Teknis urusan Persandian, maupun kementerian atau instansi terkait.

Pasal 18

Dinas Komunikasi dan Informatika melaksanakan pengawasan dan evaluasi penggunaan Sertifikat elektronik seluruh Perangkat Daerah meliputi:

- a. mekanisme pengawasan dan evaluasi Penggunaan Sertifikat elektronik untuk memberikan umpan balik dalam rangka memastikan adanya perbaikan berkesinambungan;
- b. pengawasan dan evaluasi yang bersifat rutin dan insidental dilakukan paling rendah 1 (satu) kali dalam 6 (bulan) bulan; dan
- c. laporan hasil pengawasan dan evaluasi paling rendah disusun sekali dalam 1 (satu) tahun yang terdiri atas laporan untuk Walikota, Gubernur, Kepala Badan Siber dan Sandi Negara dan Kepala BSrE.

Pasal 19

- (1) Dalam hal terdapat insiden keamanan informasi dalam Penggunaan Sertifikat elektronik di lingkungan Pemerintah Daerah, Diskominfo segera menyampaikan laporan kepada Kepala Badan Siber dan Sandi Negara dan Kepala BSrE.
- (2) Insiden keamanan informasi sebagaimana dimaksud pada ayat (1) diantaranya terdiri atas:
 - a. kejadian hilang/rusak/tidak dapat diaksesnya pasangan kunci privat dan Sertifikat Elektronik; dan
 - b. permasalahan dalam penggunaan Sertifikat Elektronik terkait otentikasi, keaslian data, dan penyangkalan dalam Penggunaan Sertifikat Elektronik di lingkungan Pemerintah Daerah.

Pasal 20

- (1) Dalam hal terjadi permasalahan dalam Penggunaan Sertifikat Elektronik terkait otentikasi, keaslian data, dan penyangkalan dalam penggunaan Sertifikat Elektronik di lingkungan Pemerintah Daerah, pengguna atau Pemilik Sertifikat Elektronik berkoordinasi dan melaporkannya kepada Diskominfo.
- (2) Permasalahan sebagaimana dimaksud pada ayat (1), Diskominfo meminta bantuan teknis kepada BSrE.

Pasal 21

- (1) Dinas Komunikasi dan Informatika dapat mengembangkan sistem informasi atau aplikasi untuk membantu kelancaran tugas pengelolaan Sertifikat Elektronik di lingkungan Pemerintah Daerah.
- (2) Sistem informasi atau sebagaimana dimaksud pada ayat (1) harus memenuhi standar keamanan informasi sesuai ketentuan Peraturan Perundang-undangan dan harus dapat diperiksa kesesuaian fungsinya melalui proses audit.

BAB VIII PEMBIAYAAN

Pasal 22

Pembiayaan Penggunaan Sertifikat Elektronik di lingkungan Pemerintah Daerah bersumber dari Anggaran Pendapatan dan Belanja Daerah dan/atau sumber lain yang sah dan tidak mengikat sesuai peraturan perundang-undangan.

BAB IX PEMBINAAN DAN PENGAWASAN

Pasal 23

- (1) Setiap pengguna atau pemilik Sertifikat Elektronik yang tidak memenuhi kewajiban sebagaimana dimaksud dalam Pasal 12 dan melanggar ketentuan dalam Pasal 13 dan Pasal 14 serta bertentangan dengan Peraturan Walikota ini dilakukan pembinaan sesuai ketentuan peraturan perundang-undangan.
- (2) Apabila selama dalam pembinaan dan pengawasan ternyata pengguna atau pemilik Sertifikat Elektronik tidak melakukan upaya perbaikan, maka dikenakan pengenaan sanksi sesuai peraturan perundang-undangan.

BAB X
KETENTUAN PENUTUP

Pasal 24

Peraturan Walikota ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Makassar
pada tanggal 2 September 2021

WALIKOTA MAKASSAR,

MOH. RAMDHAN POMANTO

Diundangkan di Makassar
pada tanggal 3 September 2021

SEKRETARIS DAERAH KOTA MAKASSAR,

M ANSAR

BERITA DAERAH KOTA MAKASSAR TAHUN 2021 NOMOR 53