WALIKOTA DUMAI
PROVINSI RIAU

PERATURAN WALIKOTA DUMAI
NOMOR 44 TAHUN 2019

TENTANG

PEMANFAATAN SERTIFIKAT ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALIKOTA DUMAI ,

Menimbang :

a. bahwa dalam rangka melindungi informasi dari resiko pencurian data, modifikasi data, pemalsuan data dan penyangkalan terhadap data yang ditransaksikan serta perlindungan sistem elektronik milik pemerintah dalam pelaksanaan Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kota Dumai diperlukan upaya pengamanan yang memadai dan andal;
b. bahwa upaya pengamanan sebagaimana dimaksud dalam huruf a dapat dilakukan melalui skema kriptografi infrastruktur kunci publik yang diwujudkan dalam bentuk pemanfaatan Sertifikat Elektronik;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Walikota tentang Pemanfaatan Sertifikat Elektronik.

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 16 Tahun 1999, tentang Pembentukan Kotamadya Daerah Tingkat II Dumai (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 50, Tambahan Lembaran Negara Republik Indonesia Nomor 3829);
3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4846), 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);
4. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);
5. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Publik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);

6. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 6 Tahun 2011 tentang Pedoman Umum Tata Naskah Dinas Elektronik di Lingkungan Instansi Pemerintah (Berita Negara Republik Indonesia Tahun 2011);
7. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 Tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036), sebagaimana telah diubah dengan Peraturan Menteri Dalam Negeri Nomor 120 Tahun 2018 tentang Perubahan atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 50 tentang Pembentukan Produk Hukum Daerah (Berita Negara Tahun 2019 Nomor 157);
8. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
9. Peraturan Daerah Kota Dumai Nomor 12 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kota Dumai (Lembaran Pemerintah Kota Dumai Tahun 2016 Nomor 1 Seri D), sebagaimana telah diubah dengan Peraturan Daerah Kota Dumai Nomor 4 Tahun 2018 tentang Perubahan Peraturan Daerah Kota Dumai Nomor 12 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kota Dumai (Lembaran Pemerintah Kota Dumai Tahun 2018 Nomor 1 Seri D);
10. Peraturan Walikota Dumai Nomor 59 Tahun 2018 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi serta tata Kerja Dinas Komunikasi dan Informatika Kota Dumai (Berita Daerah Kota Dumai Tahun 2018 Nomor 14 Seri D).

MEMUTUSKAN:

Menetapkan : PERATURAN WALIKOTA TENTANG PEMANFAATAN SERTIFIKAT ELEKTRONIK.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Walikota ini yang dimaksud dengan:
1. Daerah adalah Kota Dumai
2. Pemerintah Daerah adalah Walikota dan Perangkat daerah sebagai unsur Penyelenggara Pemerintahan Daerah.
3. Walikota adalah Kepala Daerah Kota Dumai
4. Organisasi Perangkat Daerah yang selanjutnya disingkat OPD adalah Organisasi Perangkat Daerah di lingkungan Pemerintah Daerah.
5. Dinas Komunikasi dan Informatika adalah Dinas Komunikasi dan Informatika Kota Dumai.
6. Unit Kerja pada OPD yang selanjutnya disebut Unit Kerja adalah bagian atau subordinat pada OPD yang melaksanakan satu atau beberapa program.
7. Aparatur Sipil Negara yang selanjutnya disingkat ASN adalah Aparatur Sipil Negara di lingkungan Pemerintah Daerah.
8. 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.
9. 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 terikat pada etika profesi sandi.

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. 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.
12. Sertifikat elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan digital dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik.
13. Sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
14. Pemilik sertifikat elektronik adalah individu hukum baik pejabat atau staf pegawai yang telah menyetujui perjanjian penggunaan sertifikat elektronik pada instansi di lingkungan Pemerintah Daerah yang memanfaatkan sertifikat elektronik.
15. Otoritas Sertifikat Digital yang selanjutnya disingkat OSD adalah sistem elektronik yang berfungsi sebagai layman sertifikasi elektronik di Badan Siber dan Sandi Negara.
16. Balai Sertifikasi Elektronik yang selanjutnya di sebut BSrE adalah unit pelaksana teknis penyelenggara OSD yang berada di bawah dan bertanggung jawab kepada Kepala Badan Siber dan Sandi Negara.
17. *Certificate Policy* yang selanjutnya disingkat CP adalah ketentuan dan kebijakan yang mengatur semua pihak yang terkait dengan penggunaan sertifikat elektronik yang dikeluarkan oleh BSrN Badan Siber dan Sandi Negara.
18. 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 OSD.
19. Auditor Keamanan adalah personel yang bertanggung jawab dalam mengaudit kesesuaian dan keamanan OSD serta otoritas pendaftaran.
20. Standar Operasional Prosedur yang selanjutnya disingkat SOP adalah pernyataan tentang bagaimana prosedur terkait penerbitan, penggunaan, pengaturan, penarikan dan pembaruan Sertifikat Elektronik oleh BsrE.
21. Pasangan kunci kriptografi adalah kunci privat dan kunci publik yang saling berasosiasi.
22. Sistem informasi adalah serangkaian perangkat dan prosedur yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan informasi yang dikelola di lingkungan Pemerintah Daerah.
23. Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer dan/atau media elektronik lainnya.

24. 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, 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.
25. Tanda tangan elektronik adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
26. 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.
27. 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.
28. *Passphrase/Password* 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.
29. *Reverse engineering*/rekayasa adalah sebuah proses untuk mencari dan menemukan sistem teknologi, fungsi dan operasi yang bekerja di balik suatu desain, komponen atau objek melalui sebuah proses analisa yang mendalam pada setiap komponen struktur dari desain atau objek yang diteliti.

BAB II
MAKSUD DAN TUJUAN

Pasal 2

Peraturan Walikota ini dimaksudkan sebagai pedoman bagi seluruh Perangkat Daerah dalam penyelenggaraan dan pemanfaatan 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. menciptakan hubungan komunikasi yang baik dan aman pada seluruh OPD;
b. membantu OPD dalam pengamanan informasi milik Pemerintah Daerah;
c. meningkatkan kinerja OPD dalam pelaksanaan pada SPBE;
d. menjamin integritas informasi untuk memastikan bahwa informasi tidak diubah/dimodifikasi selama penyimpanan atau pada saat dikirimkan
e. menjamin keautentikan pemilik informasi untuk memastikan bahwa informasi dikirimkan dan diterima oleh pihak yang benar (keaslian pengirim/penerima informasi);
f. menjamin nir-penyangkalan untuk memastikan bahwa pemilik informasi tidak dapat menyangkal bahwa informasi tersebut adalah miliknya atau telah disahkan olehnya;
g. menjaga kerahasiaan untuk memastikan bahwa informasi hanya dapat diakses oleh pihak yang sah;

h. meningkatkan kepercayaan dan penerimaan terhadap implementasi sistem elektronik; dan
i. meningkatkan efisiensi dan efektivitas penyelanggaraan pemerintahan dan layanan publik.

BAB III
RUANG LINGKUP

Pasal 4

Ruang lingkup pemanfaatan Sertifikat Elektronik di lingkungan Pemerintah Daerah meliputi:
a. penyelenggaraan sertifikat elektronik;
b. pemanfaatan layanan sertifikat elektronik dan bentuk tanda tangan digital pada sistem pemerintahan berbasis elektronik;
c. tata cara permohonan dan pencabutan sertifikat elektronik;
d. masa berlaku sertifikat elektronik;
e. kewajiban, larangan, ketentuan penyimpanan bagi pemilik sertifikat elektronik dan konsekuensi hukum atas persetujuan perjanjian pemilik sertifikat elektronik; dan
f. penyelenggaraan operasional dukungan sertifikat elektronik untuk pengamanan informasi.

BAB IV
PENYELENGGARAAN SERTIFIKAT ELEKTRONIK

Pasal 5

Pihak yang terlibat dalam penyelenggaraan sertifikasi elektronik terdiri atas:
a. penyelenggara sertifikat Elektronik yaitu BSrE;
b. RA yaitu Dinas Komunikasi dan Informatika; dan
c. pemilik sertifikat elektronik adalah individu hukum pejabat atau staf pegawai.

Pasal 6

(1) OP dilaksanakan oleh Dinas Komunikasi dan Informatika sebagai instansi pemilik sertifikat elektronik yang sudah mendapat delegasi dari Walikota dan BsrE serta dilaksanakan berdasarkan uji kelayakan.
(2) OP sebagaimana dimaksud pada ayat (1) harus melaksanakan tugas dan fungsinya sesuai dengan ketentuan yang diatur dalam CP.

Pasal 7

(1) Pemilik sertifikat elektronik 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) diatur di dalam CP.

Pasal 8

Penyelenggaraan sertifikat elektronik terdiri atas:
a. permohonan sertifikat elektronik;
b. penerbitan sertifikat elektronik;
c. penggunaan sertifikat elektronik;
d. pembaruan sertifikat elektronik; dan
e. pencabutan sertifikat elektronik.

Pasal 9

(1) Permohonan sertifikat elektronik sebagaimana dimaksud dalam pasal 8 huruf a, merupakan proses permintaan sertifikat elektronik yang diajukan oleh OPD calon pengguna sertifikat elektronik kepada Dinas Komunikasi dan Informatika.

(2) Penerbitan sertifikat elektronik sebagaimana dimaksud dalam Pasal 8 huruf b, merupakan proses persetujuan permohonan dan penandatanganan sertifikat elektronik oleh Dinas Komunikasi dan Informatika.

(3) Penggunaan sertifikat elektronik sebagaimana dimaksud dalam Pasal 8 huruf c, merupakan proses pemanfaatan sertifikat elektronik oleh pemilik sertifikat.

(4) Pembaruan sertifikat elektronik sebagaimana dimaksud dalam Pasal 8 huruf d, merupakan proses membuat sertifikat elektronik baru untuk memperpanjang masa penggunaan sertifikat elektronik.

(5) Pencabutan sertifikat elektronik sebagaimana dimaksud dalam Pasal 8 huruf e, merupakan proses penghentian penggunaan sertifikat elektronik oleh BSrE berdasarkan evaluasi atau permintaan pemilik sertifikat elektronik.

Pasal 10

(1) Setiap ASN wajib memiliki sertifikat elektronik yang digunakan selama melaksanakan tugas kedinasan.

(2) Aplikasi dan sistem elektronik di lingkungan Pemerintah Daerah harus memanfaatkan sertifikat elektronik dalam rangka pengamanan informasi.

(3) Pengajuan permohonan kepemilikan sertifikat elektronik dapat dilakukan oleh Kepala OPD melalui RA sesuai dengan syarat dan ketentuan peraturan perundang-undangan.

Pasal 11

Tugas kedinasan sebagaimana dimaksud dalam Pasal 10 ayat (1) adalah:

a. pembuatan dan pengiriman dokumen melalui email OPD;
b. pembuatan dokumen secara elektronik; dan
c. pembuatan dokumen elektronik lainnya yang menggunakan aplikasi dan sistem elektronik.

BAB V

PEMANFAATAN LAYANAN SERTIFIKAT ELEKTRONIK DAN BENTUK TANDA TANGAN DIGITAL PADA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Pasal 12

Pemanfaatan layanan sertifikat elektronik pada SPBE, berupa:

a. tanda tangan digital/elektronik;
b. pengarnanan dokumen elektronik; dan
c. pengamanan email.

Pasal 13

Pemanfaatan layanan 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 Dinas Komunikasi dan Informatika dan/atau dari sistem informasi OPD terkait di lingkungan Pemerintah Daerah; dan

d. layanan pada SPBE lainnya yang ditentukan dan/atau disediakan oleh Pemerintah Daerah.

Pasal 14

Bentuk tanda tangan digital terdiri atas:
a. bagian kiri logo daerah;
b. bagian kanan logo BsrE; dan
c. bagian tengah menyebutkan Jabatan, Nama, Nomor Induk Pegawai (NIP).

BAB VI
TATA CARA PERMOHONAN, PENERBITAN
DAN PENCABUTAN SERTIFIKAT ELEKTRONIK

Bagian Kesatu
Permohonan Penerbitan Sertifikat Elektronik

Pasal 15

Pengajuan permohonan penerbitan sertifikat elektronik dapat dilakukan oleh OPD kepada Dinas Komunikasi dan Informatika dengan menyampaikan:
a. surat permohonan penerbitan sertifikat elektronik dan Kepala OPD kepada Kepala Dinas Komunikasi dan Informatika;
b. surat rekomendasi dan Kepala OPD, untuk melakukan pendaftaran sertifikat elektronik;
c. mengisi formulir pendaftaran sertifikat elektronik untuk individu;
d. potokopi/scan Kartu Tanda Penduduk;
e. potokopi/scan Keputusan Pengangkatan Jabatan Terakhir;
f. email instansi individu pengguna yang menggunakan domain @dumai.go.id; dan
g. memahami dan menyetujui Perjanjian Pemilik Sertifikat Elektronik.

Pasal 16

(1) Permohonan penerbitan sertifikat elektronik dilakukan secara langsung oleh Kepala OPD melalui aplikasi yang telah ditetapkan oleh BSrE.

(2) Dalam rangka menjaga keamanan dan kerahasiaan, pemilik sertifikat elektronik harus menjaga keamanan *passphrase/password* dan pasangan kunci privat dan sertifikat elektronik yang dimiliki.

(3) Setiap tanda tangan elektronik yang dibubuhkan pada dokumen elektronik menggunakan pasangan kunci privat dan sertifikat elektronik memiliki konsekuensi hukum sehingga pemilik sertifikat dilarang menguasakan tanda tangan elektronik kepada pihak lain.

(4) Dalam hal pasangan kunci privat dan sertifikat elektronik hilang/ rusak/tidak dapat diakses, maka pemilik sertifikat elektronik menyampaikan permohonan penerbitan kembali dengan melampirkan surat keterangan yang ditandatangani oleh atasan langsung.

(5) Dalam hal masa berlaku sertifikat elektronik akan habis, maka pemilik sertifikat elektronik dapat mengajukan kembali permohonan sertifikat elektronik dengan mengikuti tata cara pemohonan.

Pasal 17

(1) RA dilaksanakan oleh Dinas Komunikasi dan Informatika.

(2) RA sebagaimana dimaksud pada ayat (1) memiliki tugas dan kewenangan sebagai berikut:
   a. melakukan identifikasi dan analisis kebutuhan sertifikat elektronik;
   b. melakukan pengembangan atau memberikan masukan kepada satuan unit kerja yang membidangi aplikasi untuk membuat sistem/aplikasi pendukung penggunaan sertifikat elektronik;
   c. membuat rekomendasi penggunaan sertifikat elektronik dan/atau aplikasi pendukung penggunaan sertifikat elektronik;
   d. melakukan sosialisasi dan bimbingan teknis terkait penggunaan sertifikat elektronik;
   e. melakukan edukasi kepada pemilik sertifikat elektronik yang setidaknya meliputi hak, kewajiban dan tanggung jawab, serta prosedur pengajuan komplain;
   f. melakukan verifikasi pendaftaran, pembaharuan dan pencabutan sertifikat elektronik; dan
   g. melakukan pengawasan dan evaluasi penggunaan sertifikat elektronik.

(3) RA sebagaimana dimaksud pada ayat (1) menyusun SOP dan melakukan sosialisasi kepada pihak terkait.

(4) Petugas RA adalah pegawai pada Dinas Komunikasi dan Informatika yang ditunjuk dan telah mendapatkan sertifikat elektronik sebagai petugas RA yang diberikan oleh BSrE.

(5) Dalam hal data yang diajukan oleh pegawai tidak lengkap/tidak sesuai dengan ketentuan dan persyaratan, petugas RA memiliki hak untuk menolak permohonan yang diajukan oleh pemohon.

(6) Dalam hal petugas RA tidak menjalankan tugasnya sesuai dengan ketentuan yang berlaku maka petugas RA dapat dilaporkan ke BSrE.

Bagian Kedua
Pencabutan Sertifikat Elektronik

Pasal 18

(1) OPD dapat meminta pencabutan sertifikat elektronik ke Dinas Komunikasi dan Informatika, jika:
   a. pengguna sudah tidak menjabat/mutasi/rotasi; dan
   b. pengguna pensiun.

(2) Pencabutan sertifikat elektronik dilakukan setelah surat permohonan dan dokumen kelengkapan memenuhi syarat yang ditentukan dalam Peraturan Walikota ini.

(3) Syarat dan ketentuan pencabutan sertifikat elektronik adalah surat permintaan pencabutan sertifikat elektronik harus ditandatangani dan disampaikan oleh Kepala OPD yang bersangkutan.

(4) Sertifikat Elektronik yang telah dicabut oleh Dinas Komunikasi dan Informatika tidak dapat digunakan kembali.

(5) Dalam hal permintaan pencabutan sertifikat elektronik telah disetujui oleh Dinas Komunikasi dan Informatika, maka OPD terkait menerima pemberitahuan dari Dinas Komunikasi dan Informatika yang dikirim melalui jawaban surat atau email yang tercantum dalam surat permintaan pencabutan sertifikat elektronik.

(6) Dalam hal OPD memerlukan kembali sertifikat elektronik, maka OPD dapat meminta Sertifikat Elektronik sesuai dengan ketentuan di dalam Peraturan Walikota ini.

(7) Permohonan pencabutan sertifikat elektronik yang telah diterima dari OPD, kemudian Dinas Komunikasi dan Informatika sebagai RA meneruskan ke BsrE.

BAB VII
MASA BERLAKU SERTIFIKAT ELEKTRONIK

Pasal 19

(1) Masa berlaku sertifikat elektronik selama 2 (dua) tahun dihitung sejak tanggal sertifikat elektronik diterbitkan atau sejak diterbitkan sertifikat elektronik baru.

(2) Sebelum masa berlaku sertifikat elektronik berakhir, pengguna sertifikat elektronik dapat meminta sertifikat elektronik baru.

(3) Tata cara permintaan sertifikat elektronik baru sebagaimana dimaksud pada ayat (2) mengikuti syarat dan ketentuan permintaan sertifikat elektronik sebagaimana diatur dalam Peraturan Walikota ini.

BAB VIII
KEWAJIBAN, LARANGAN DAN PENYIMPANAN BAGI PEMILIK SERTIFIKAT ELEKTRONIK

Pasal 20

Pemilik Sertifikat Elektronik berkewajiban:
a. memastikan semua informasi yang diberikan ke Dinas Komunikasi dan Informatika adalah benar;
b. melindungi sertifikat elektronik agar tidak digunakan oleh orang lain;
c. tidak menyerahkan 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/password* atau hal lain yang digunakan untuk mengaktifkan kunci privat;
f. tidak mengubah, mengganggu atau melakukan *reverse engineering*/ rekayasa dan berusaha untuk membocorkan layanan keamanan yang disediakan Dinas Komunikasi dan Informatika; dan
g. bertanggung jawab atas penggunaan, penyimpanan, pembaruan dan pemusnahan sertifikat elektronik dan kunci privat.

Pasal 21

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 mempercayai 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. pengguna sertifikat elektronik menyampaikan potokopi dokumen yang tidak sesuai dengan aslinya dan/atau dokumen yang dengan sengaja dipalsukan sebagai persyaratan permintaan sertifikat elektronik.

Pasal 22

Data yang terkait dengan penanda tangan 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. penanda tangan wajib menjaga kerahasiaan dan bertanggung jawab atas data pembuatan tanda tangan elektronik.

Pasal 23

Setiap ASN yang tidak menjalankan kewajiban atau melanggar larangan dalam Peraturan Walikota ini dikenakan sanksi berupa pencabutan Sertifikat elektronik dan sanksi sesuai ketentuan peraturan perundang-undangan.

BAB IX
PENYELENGGARAAN OPERASIONAL DUKUNGAN SERTIFIKAT ELEKTRONIK UNTUK PENGAMANAN INFORMASI

Pasal 24

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 25

Dalam penyelenggaraan operasional sertifikat elektronik melalui sistem OSD sebagaimana dimaksud dalam Pasal 23, Dinas Komunikasi dan Informatika berkoordinasi dengan Badan Siber dan Sandi Negara sebagai Instansi Pembina Persandian.

Pasal 26

Dinas Komunikasi dan Informatika melaksanakan pengawasan dan evaluasi penggunaan sertifikat elektronik seluruh OPD, meliputi:
a. pengawasan dan evaluasi yang bersifat rutin dan insidentil yang dilakukan paling sedikit satu kali dalam 6 (bulan) bulan atau sesuai kebutuhan; dan/atau
b. pengawasan dan evaluasi yang bersifat tahunan.

Pasal 27

Dalam rangka penggunaan sertifikat elektronik dan pernyataan tentang SOP di lingkungan Pemerintah Daerah, Dinas Komunikasi dan Informatika dapat melaksanakah koordinasi dan/atau konsultasi kepada Badan Siber dan Sandi Negara, maupun kementerian atau instansi terkait.

BAB X
KETENTUAN PENUTUP

Pasal 28

Peraturan Walikota ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Dumai
pada tanggal 29 Agustus 2019

WALIKOTA DUMAI,

dto

ZULKIFLI AS

Diundangkan di Dumai
pada tanggal 29 Agustus 2019

Pj. SEKRETARIS DAERAH KOTA DUMAI,

dto

HAMDAN KAMAL

BERITA DAERAH KOTA DUMAI TAHUN 2019 NOMOR 36 SERI E