



WALI KOTA TERNATE
PROVINSI MALUKU UTARA

PERATURAN WALI KOTA TERNATE
NOMOR 28 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN
BERBASIS ELEKTRONIKDILINGKUP PEMERINTAH KOTA TERNATE

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA TERNATE,

- Menimbang : a. bahwa untuk menindaklanjuti ketentuan Pasal 30 ayat (5) Peraturan Daerah Nomor 2 Tahun 2023 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kota Ternate, pengamanan pada sistem elektronik perlu diatur dengan Peraturan Wali Kota;
- b. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Kota Ternate, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;
- c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Wali Kota tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Di Lingkup Pemerintah Kota Ternate;
- Mengingat : 1. Undang-Undang Nomor 11 Tahun 1999 tentang Pembentukan Daerah Kotamadya Tingkat II Ternate (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 45, Tambahan Lembaran Negara Republik Indonesia Nomor 3824)
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 Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
6. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
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 2010 Nomor 1054);
8. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
9. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);
10. 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);
11. Peraturan Daerah Kota Ternate Nomor 2 Tahun 2023 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kota Ternate (Lembaran Daerah Kota Ternate Tahun 2023 Nomor 217, Tambahan Lembaran Daerah Kota Ternate Nomor 154);
12. Peraturan Wali Kota Ternate Nomor 48.A Tahun 2023 tentang Penyelenggaraan Satu Data Indonesia Kota Ternate (Berita Daerah Kota Ternate Tahun 2023 Nomor 555.A);

MEMUTUSKAN:

Menetapkan : PERATURAN WALI KOTA TENTANG MENAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KOTA TERNATE.

BAB I KETENTUAN UMUM

Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:

1. Daerah adalah Kota Ternate.
2. Pemerintah Daerah adalah Kepala Daerah sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan Daerah otonom.
3. Wali Kota adalah Wali Kota Ternate.
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Ternate.
5. Perangkat Daerah yang selanjutnya disingkat PD adalah unsur pembantu Kepala Daerah dan DPRD dalam penyelenggaraan urusan Pemerintahan yang menjadi kewenangan Daerah.
6. Dinas Komunikasi, Informatika, dan Persandian Kota Ternate yang selanjutnyadisebut Dinasadalah Perangkat Daerah yang menyelenggarakan urusanKomunikasi, Informatika, danPersandian.
7. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna Sistem Pemerintahan Berbasis Elektronik.
8. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan Informasi antar media.
9. Keamanan Informasi adalah suatu kondisi untuk melindungi aset yang dimiliki organisasi dari berbagai ancaman pihak internal maupun eksternal untuk menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, serta terjaganya aspek kerahasiaan, keutuhan dan ketersediaan dari informasi.
- 10.Keamanan Sistem Pemerintahan Berbasis Elektronik mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian dan kenirsangkalan sumber daya terkait data dan informasi, infrastruktur Sistem Pemerintahan Berbasis Elektronik, dan Aplikasi Sistem Pemerintahan Berbasis Elektronik.
- 11.Manajemen Keamanan Sistem Pemerintahan Berbasis Elektronikadalah serangkaian proses untuk mencapai penerapan keamanan Sistem Pemerintahan Berbasis Elektronikyang efektif, efisien, dan berkesinambungan, serta mendukung layanan Sistem Pemerintahan Berbasis Elektronikyang berkualitas.

12. Aplikasi Sistem Pemerintahan Berbasis Elektronik adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan Sistem Pemerintahan Berbasis Elektronik.
13. Infrastruktur Sistem Pemerintahan Berbasis Elektronik adalah semua perangkat keras, perangkat lunak dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung dan perangkat elektronik lainnya.

BAB II MAKSUD DAN TUJUAN

Pasal 2

Maksud dan tujuan ditetapkan Peraturan Wali Kota ini adalah sebagai pedoman manajemen keamanan informasi sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Kota Ternate.

BAB III MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Bagian Kesatu Umum

Pasal 3

Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik meliputi:

- a. penetapan ruang lingkup;
- b. penetapan penanggung jawab;
- c. perencanaan;
- d. dukungan pengoperasian;
- e. evaluasi kinerja; dan
- f. perbaikan berkelanjutan.

Pasal 4

Ketentuan lain untuk mendukung kebijakan internal Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud dalam Pasal 3, dapat menerapkan pengendalian teknis keamanan yang meliputi:

- a. manajemen risiko;
- b. penetapan prosedur pengendalian keamanan informasi Sistem Pemerintahan Berbasis Elektronik; dan
- c. pengelolaan pihak ketiga.

Bagian Kedua
Kebijakan Internal Manajemen Keamanan Informasi
Sistem Pemerintahan Berbasis Elektronik

Paragraf 1
Penetapan Ruang Lingkup

Pasal 5

- (1) Penetapan ruang lingkup Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud dalam Pasal 3 huruf a meliputi:
 - a. data dan informasi Sistem Pemerintahan Berbasis Elektronik;
 - b. aplikasi Sistem Pemerintahan Berbasis Elektronik; dan
 - c. aset infrastruktur Sistem Pemerintahan Berbasis Elektronik.
- (2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Daerah yang harus diamankan dalam Sistem Pemerintahan Berbasis Elektronik.

Paragraf 2
Penetapan Penanggung Jawab

Pasal 6

- (1) Wali Kota menetapkan penanggung jawab sebagaimana dimaksud dalam Pasal 3 huruf b.
- (2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah yang mempunyai tugas sebagai Koordinator Sistem Pemerintahan Berbasis Elektronik di Daerah.

Pasal 7

- (1) Dalam melaksanakan tugas sebagai penanggung jawab dan koordinator Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud dalam Pasal 6, Sekretaris Daerah menetapkan Pelaksana Teknis Keamanan Sistem Pemerintahan Berbasis Elektronik.
- (2) Pelaksana Teknis Keamanan Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud pada ayat (1), terdiri atas:
 - a. Ketua Tim; dan
 - b. Anggota tim.
- (3) Ketua Tim sebagaimana dimaksud pada ayat (2) huruf a adalah pimpinan Perangkat Daerah yang membidangi urusan pemerintahan di bidang komunikasi, informatika dan persandian.
- (4) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh pimpinan Perangkat Daerah lainnya yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan infrastruktur Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Daerah.

Pasal 8

- (1) Ketua Tim sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Daerah yang meliputi:
 - a. menetapkan prosedur pengendalian keamanan informasi Sistem Pemerintahan Berbasis Elektronik Pemerintah Daerah Kota Ternate;
 - b. mengevaluasi penerapan prosedur pengendalian keamanan informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Daerah Kota Ternate;
 - c. memastikan penerapan keamanan Aplikasi Sistem Pemerintahan Berbasis Elektronik dan Infrastruktur Sistem Pemerintahan Berbasis Elektronik sesuai dengan standar teknis dan prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan;
 - d. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan Sistem Pemerintahan Berbasis Elektronik;
 - e. memutuskan dan merancang langkah kelangsungan layanan teknologi informasi dan komunikasi dalam bentuk dokumen *business continuity* dan *disaster recovery plans*; dan
 - f. melaporkan pelaksanaan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik pada Koordinator Sistem Pemerintahan Berbasis Elektronik.
- (2) Anggota Tim sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf b mempunyai tugas:
 - a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian keamanan informasi Sistem Pemerintahan Berbasis Elektronik pada Perangkat Daerah masing-masing;
 - b. memastikan penerapan keamanan Aplikasi dan Infrastruktur Sistem Pemerintahan Berbasis Elektronik pada Perangkat Daerah masing-masing sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan;
 - c. melaksanakan dan mengelola langkah kelangsungan layanan teknologi informasi dan komunikasi yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan
 - d. melaksanakan koordinasi dengan Ketua Tim terkait penerapan keamanan Aplikasi Sistem Pemerintahan Berbasis Elektronik dan Infrastruktur Sistem Pemerintahan Berbasis Elektronik.

Paragraf 3 Perencanaan

Pasal 9

- (1) Perencanaan sebagaimana dimaksud dalam Pasal 3 huruf c ditetapkan oleh Ketua Tim Pelaksana Teknis Keamanan Sistem Pemerintahan Berbasis Elektronik.

- (2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
- a. program kerja keamanan Sistem Pemerintahan Berbasis Elektronik; dan
 - b. target realisasi program kerja Keamanan Sistem Pemerintahan Berbasis Elektronik.

Pasal 10

- (1) Program kerja Keamanan Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud pada Pasal 9 ayat (2) huruf a meliputi:
- a. edukasi kesadaran keamanan Sistem Pemerintahan Berbasis Elektronik;
 - b. penilaian kerentanan keamanan Sistem Pemerintahan Berbasis Elektronik;
 - c. peningkatan keamanan Sistem Pemerintahan Berbasis Elektronik;
 - d. penanganan insiden keamanan Sistem Pemerintahan Berbasis Elektronik; dan
 - e. audit keamanan Sistem Pemerintahan Berbasis Elektronik.
- (2) Target realisasi program kerja Keamanan Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf b ditetapkan berdasarkan kebutuhan Pemerintah Daerah.

Pasal 11

Edukasi kesadaran Keamanan Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf a dilaksanakan melalui kegiatan:

- a. sosialisasi; dan
- b. pelatihan.

Pasal 12

Penilaian kerentanan keamanan Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf b dilaksanakan melalui:

- a. menginventarisasi seluruh aset Sistem Pemerintahan Berbasis Elektronik meliputi data dan informasi, aplikasi dan infrastruktur;
- b. mengidentifikasi kerentanan dan ancaman terhadap aset Sistem Pemerintahan Berbasis Elektronik; dan
- c. mengukur tingkat risiko keamanan Sistem Pemerintahan Berbasis Elektronik.

Pasal 13

- (1) Peningkatan keamanan Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf c dilaksanakan berdasarkan hasil dari penilaian kerentanan keamanan Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud dalam Pasal 12.
- (2) Peningkatan keamanan Sistem Pemerintahan Berbasis Elektronik dilaksanakan paling sedikit melalui:
- a. menerapkan standar teknis dan prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik; dan
 - b. menguji fungsi keamanan terhadap aplikasi dan infrastruktur Sistem Pemerintahan Berbasis Elektronik.

Pasal 14

Penanganan insiden keamanan Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf d dilaksanakan paling sedikit melalui:

- a. mengidentifikasi sumber serangan;
- b. menganalisis informasi yang berkaitan dengan insiden selanjutnya;
- c. memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
- d. mendokumentasi bukti insiden yang terjadi; dan
- e. memitigasi atau mengurangi dampak risiko keamanan Sistem Pemerintahan Berbasis Elektronik.

Pasal 15

Audit Keamanan Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf e dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

Paragraf 4

Dukungan Pengoperasian

Pasal 16

- (1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 3 huruf d dilakukan oleh Koordinator Sistem Pemerintahan Berbasis Elektronik.
- (2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:
 - a. sumber daya manusia keamanan Sistem Pemerintahan Berbasis Elektronik;
 - b. teknologi keamanan Sistem Pemerintahan Berbasis Elektronik; dan
 - c. anggarankeamanan Sistem Pemerintahan Berbasis Elektronik.
- (3) Koordinator Sistem Pemerintahan Berbasis Elektronik melalui dukungan pengoperasian memastikan pelaksanaan manajemen keamanan informasi Sistem Pemerintahan Berbasis Elektronik diberikan alokasi sumber daya yang sesuai.

Pasal 17

- (1) Sumber daya manusia keamanan Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf a paling sedikit berjumlah 5 (lima) orang dengan ketentuan harus memiliki kompetensi:
 - a. keamanan teknologi, informasi dan komunikasi; dan
 - b. keamananaplikasi.
- (2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), paling sedikit harus adanya dukungan kegiatan:
 - a. pelatihan dan/atau sertifikat kompetensi keamanan aplikasi dan TIK; dan
 - b. Bimbingan teknis mengenai standar teknis dan prosedur keamanan Sistem Pemerintahan Berbasis Elektronik.

- (3) Pemenuhan kompetensi sebagaimana dimaksud pada ayat (2) dilakukan agar sumber daya manusia keamanan Sistem Pemerintahan Berbasis Elektronik memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan keamanan Sistem Pemerintahan Berbasis Elektronik.

Pasal 18

Teknologi keamanan Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud pada Pasal 16 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

Pasal 19

Anggaran keamanan Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Paragraf 5 Evaluasi Kinerja

Pasal 20

- (1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 3 huruf e dilakukan oleh Koordinator Sistem Pemerintahan Berbasis Elektronik.
- (2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan manajemen keamanan informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Daerah.
- (3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
 - a. menganalisis efektifitas pelaksanaan keamanan Sistem Pemerintahan Berbasis Elektronik; dan
 - b. mendukung dan merealisasikan program audit keamanan Sistem Pemerintahan Berbasis Elektronik.
- (4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Paragraf 6 Perbaikan Berkelanjutan Terhadap Keamanan Sistem Pemerintahan Berbasis Elektronik

Pasal 21

- (1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 3 huruf f dilakukan oleh Pelaksana Teknis Keamanan Sistem Pemerintahan Berbasis Elektronik.
- (2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja yang dilakukan dengan:
 - a. mengatasi permasalahan dalam pelaksanaan keamanan Sistem Pemerintahan Berbasis Elektronik;
 - b. memperbaiki pelaksanaan keamanan Sistem Pemerintahan Berbasis Elektronik secara periodik; dan
 - c. tindak lanjut hasil audit Keamanan Sistem Pemerintahan Berbasis Elektronik.

Bagian Ketiga
Pengendalian Teknis Keamanan
Sistem Pemerintahan Berbasis Elektronik

Paragraf 1
Manajemen Risiko

Pasal 22

- (1) Manajemen risiko sebagaimana dimaksud dalam Pasal 4 huruf a dilakukan oleh setiap Perangkat Daerah.
- (2) Manajemen risiko sebagaimana dimaksud pada ayat (1) dilakukan dengan menyusun daftar risiko (*risk register*) dengan ketentuan substansi meliputi:
 - a. inventarisasi aset Sistem Pemerintahan Berbasis Elektronik;
 - b. identifikasi ancaman dan kerentanan keamanan terhadap aset Sistem Pemerintahan Berbasis Elektronik;
 - c. penilaian risiko keamanan terhadap aset Sistem Pemerintahan Berbasis Elektronik;
 - d. penentuan prioritas risiko;
 - e. analisa dampak jika terjadi risiko;
 - f. analisa kontrol keamanan yang bisa diterapkan; dan
 - g. rekomendasikontrol keamanan.

Paragraf 2
Penetapan Prosedur Pengendalian Keamanan Informasi
Sistem Pemerintahan Berbasis Elektronik

Pasal 23

- (1) Penetapan prosedur pengendalian keamanan informasi Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud dalam Pasal 4 huruf b ditetapkan oleh Ketua Tim Pelaksana Teknis Keamanan Sistem Pemerintahan Berbasis Elektronik.
- (2) Penetapan prosedur pengendalian keamanan informasi Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan manajemen keamanan informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Daerah Kota Ternate dengan cakupan aspek meliputi:
 - a. keamanan perangkat teknologi informasi komunikasi;
 - b. keamanan jaringan;
 - c. keamanan pusat data;
 - d. keamanan perangkat *end point*;
 - e. keamanan *remote working*;
 - f. Keamanan penyimpanan elektronik;
 - g. pengelolaan akses control;
 - h. pengendalian keamanan dari ancaman virus dan *malware*;
 - i. persyaratan keamananan terkait pembangunan dan pengembangan aplikasi Sistem Pemerintahan Berbasis Elektronik;
 - j. pengelolaan aset;

- k. keamanan migrasi data;
 - l. konfigurasi perangkat IT *Security*;
 - m. perlingungan data pribadi;
 - n. keamanan komunikasi;
 - o. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
 - p. pengendalian keamanan informasi terhadap pihak ketiga;
 - q. penerapan *kriptografi*;
 - r. penanganan insiden keamanan informasi;
 - s. kelangsungan bisnis atau layanan TIK (*business continuity*);
 - t. perencanaan pemulihan bencana terhadap layanan;
 - u. TIK (*Disaster Recovery Plans*);
 - v. audit internal keamanan Sistem Pemerintahan Berbasis Elektronik; dan/atau
 - w. aspek prosedur pengendalian keamanan informasi Sistem Pemerintahan Berbasis Elektronik lainnya.
- (3) Ketentuan lebih lanjut mengenai penetapan prosedur pengendalian keamanan informasi Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud pada ayat (2) ditetapkan dengan Keputusan Wali Kota.
- (4) Perangkat Daerah melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud pada ayat (3) dan bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian keamanan informasi Sistem Pemerintahan Berbasis Elektronik.

Paragraf 3 Pengelolaan Pihak Ketiga

Pasal 24

- (1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 4 huruf c dilakukan oleh setiap Perangkat Daerah.
- (2) Perangkat Daerah harus memastikan seluruh pembangunan atau pengembangan Aplikasi dan Infrastruktur Sistem Pemerintahan Berbasis Elektronik yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur keamanan Sistem Pemerintahan Berbasis Elektronik yang telah ditetapkan.
- (3) Perangkat Daerah harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi Infrastruktur Sistem Pemerintahan Berbasis Elektronik beserta kode sumbernya.
- (4) Perangkat Daerah harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan Informasi dalam hubungan kerjasama dengan pihak ketiga.
- (5) Perangkat Daerah harus memuat laporan secara berkala tentang pencapaian sasaran tingkatan layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB III
KETENTUAN PENUTUP

Pasal 25

Peraturan Wali Kota ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Ternate
pada tanggal 30 Agustus 2024

WALI KOTA TERNATE,

ttd

M. TAUHID SOLEMAN

Diundangkan di Ternate
pada tanggal 30 Agustus 2024

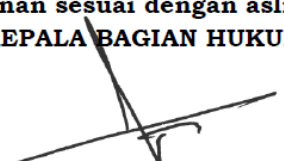
SEKRETARIS DAERAH KOTA TERNATE,

ttd

RIZAL MARSAOLY

BERITA DAERAH KOTA TERNATE TAHUN 2024 NOMOR 590

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM



TOTO SUNARTO, S.H

PEMBINA IV/a

NIP: 19830627 2008 03 1 001