BUPATI WAKATOBI
PROVINSI SULAWESI TENGGARA

PERATURAN BUPATI WAKATOBI
NOMOR: 43 TAHUN 2022

TENTANG

PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI
DI LINGKUNGAN PEMERINTAH KABUPATEN WAKATOBI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI WAKATOBI,

Menimbang : a. bahwa berdasarkan ketentuan Pasal 4 ayat (2) Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintahan Daerah, Bupati sesuai dengan kewenangannya bertanggung jawab terhadap Penyelenggaraan Persandian untuk Pengamanan Informasi;

b. bahwa setiap pemerintah daerah wajib mengelola informasi yang dimilikinya dan untuk melindungi informasi perlu dilakukan upaya pengamanan informasi melalui penyelenggaraan persandian;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Penyelenggaraan Persandian dalam Pengamanan Informasi di Lingkungan Pemerintah Kabupaten Wakatobi;

Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 29 Tahun 2003 tentang Pembentukan Kabupaten Bombana, Kabupaten Wakatobi, dan Kabupaten Kolaka Utara di Provinsi Sulawesi Tenggara (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 144, Tambahan Lembaran Negara Republik Indonesia Nomor 4339);

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

4. Undang-Undang Nomor 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 Nomor 15 Tahun 2019

tentang Perubahan Atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 183, Tambahan Lembaran Negara Republik Indonesia Nomor 6398);

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 1 Tahun 2022 tentang Hubungan Keuangan Antara Pemerintah Pusat dan Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6757);
6. Peraturan Pemerintah Nomor 12 Tahun 2017 tentang Pembinaan dan Pengawasan Penyelenggaraan Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 73, Tambahan Lembaran Negara Republik Indonesia Nomor 6041);
7. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah;
8. Peraturan Daerah Nomor 5 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Wakatobi (Lembaran Daerah Kabupaten Wakatobi Tahun 2016 Nomor 5) sebagaimana telah diubah dengan Peraturan Daerah Nomor 5 Tahun 2020 tentang Perubahan Atas Peraturan Daerah Nomor 5 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Wakatobi (Lembaran Daerah Kabupaten Wakatobi Tahun 2020 Nomor 8);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH KABUPATEN WAKATOBI.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini, yang dimaksud dengan:

1. Daerah adalah Kabupaten Wakatobi.

2. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Bupati adalah Bupati Wakatobi.
4. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
5. Perangkat Daerah yang membidangi urusan persandian adalah Dinas Komunikasi, Informatika, Statistik dan Persandian Kabupaten Wakatobi.
6. Surat Elektronik adalah yang selanjutnya disebut email adalah sarana komunikasi yang didalamnya mampu untuk mengirim, menerima, dan menyimpan pesan melalui fasilitas jaringan internet.
7. Persandian adalah kegiatan di bidang pengamanan data/informasi yang dilaksanakan dengan menerapkan konsep, teori, seni dan ilmu kripto beserta ilmu pendukung lainnya secara sistematis, metodologis dan konsisten serta terkait pada etika profesi sandi.
8. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan Informasi.
9. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
10. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
11. 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.
12. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
13. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
14. 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.

15. 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.
16. Badan Siber dan Sandi Negara, yang selanjutnya disebut BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.

Pasal 2

Pelaksanaan persandian untuk pengamanan informasi bertujuan untuk:

a. meningkatkan komitmen, efektivitas, dan kinerja Pemerintah Daerah dalam melaksanakan kebijakan, program, dan kegiatan pelaksanaan Persandian untuk pengamanan informasi;
b. menciptakan hubungan komunikasi yang baik dan aman pada seluruh Perangkat Daerah; dan
c. meningkatkan kinerja Dinas Komunikasi, Informatika, Statistik dan Persandian Kabupaten Wakatobi dalam menangani urusan pemerintah bidang persandian untuk pengamanan informasi.

Pasal 3

Pelaksanaan persandian untuk pengamanan informasi sebagaimana dimaksud dalam Pasal 2 meliputi:

a. penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah; dan
b. penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.

BAB II
PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

Bagian Kesatu
Umum

Pasal 4

Penyelenggaraan Persandian untuk Pengamanan Informasi sebagaimana dimaksud dalam Pasal 3 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.

Bagian Kedua
Penyusunan Kebijakan Pengamanan Informasi

Pasal 5

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 4 huruf a dilakukan dengan:

a. menyusun rencana strategis pengamanan informasi;

b. menetapkan arsitektur keamanan informasi; dan

c. menetapkan aturan mengenai tata kelola keamanan informasi.

Pasal 6

(1) Penyusunan rencana strategis pengamanan informasi sebagaimana dimaksud pada Pasal 5 huruf a dilakukan oleh Perangkat Daerah.

(2) Rencana Strategis sebagaimana dimaksud pada ayat (1) terdiri atas:

a. tujuan, sasaran, program, kegiatan, dan target pelaksanaan pengamanan informasi setiap tahun untuk jangka waktu 5 (lima) tahun; dan

b. peta rencana penyelenggaraan pengamanan informasi yang merupakan penjabaran dari tahapan rencana strategis yang akan dicapai setiap tahun untuk jangka waktu 5 (lima) tahun.

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

Pasal 7

(1) Arsitektur keamanan informasi sebagaimana dimaksud dalam Pasal 5 huruf b memuat:

a. infrastruktur teknologi informasi;

b. desain keamanan perangkat teknologi informasi dan keamanan jaringan; dan

c. aplikasi keamanan perangkat teknologi informasi dan keamanan jaringan.

(2) Arsitektur keamanan informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.

Pasal 8

Aturan mengenai tata kelola keamanan informasi sebagaimana dimaksud dalam Pasal 5 huruf c paling sedikit terdiri atas:

a. keamanan sumber daya teknologi informasi;

b. keamanan akses kontrol;

c. keamanan data dan informasi;

d. keamanan sumber daya manusia;

e. keamanan jaringan;

f. keamanan surat elektronik;

g. keamanan pusat data; dan/atau

h. keamanan komunikasi.

Bagian Ketiga
Pengelolaan Sumber Daya Keamanan Informasi

Pasal 9

(1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 4 huruf b dilaksanakan oleh Perangkat Daerah.

(2) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas:

a. pengelolaan aset keamanan teknologi informasi dan komunikasi;

b. pengelolaan sumber daya manusia; dan

c. manajemen pengetahuan.

Pasal 10

(1) Pengelolaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf a dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.

(2) Aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (1) merupakan perangkat yang digunakan untuk mengidentifikasi, mendeteksi, memproteksi, menganalisis, menanggulangi, dan/atau memulihkan insiden Keamanan Informasi dalam Sistem Elektronik.

Pasal 11

(1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf b dilakukan oleh Perangkat Daerah.

(2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses sebagai berikut:

a. pengembangan kompetensi;

b. pembinaan karir;

c. pendayagunaan; dan

d. pemberian tunjangan pengamanan persandian.

Pasal 12

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a dilaksanakan dengan ketentuan:

a. melalui tugas belajar, pendidikan dan pelatihan pembentukan dan penjenjangan fungsional, pendidikan dan pelatihan teknis, bimbingan teknis, asistensi, *workshop*, seminar, dan kegiatan lainnya yang terkait pengembangan kompetensi sumber daya manusia di bidang keamanan informasi;

b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, pihak lainnya, atau pemerintah daerah masing-masing; dan

c. memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi bidangnya.

(2) Pembinaan karir sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b dilaksanakan dengan ketentuan:

a. pembinaan jabatan fungsional di bidang Keamanan Informasi; dan

b. pengisian formasi jabatan pimpinan tinggi, jabatan administrator, dan jabatan pengawas sesuai dengan standar kompetensi yang ditetapkan.

(3) Pendayagunaan sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf c dilaksanakan agar seluruh sumber daya manusia yang bertugas di bidang keamanan informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan.

Pasal 13

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf c dilakukan oleh Perangkat Daerah.

(2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan untuk meningkatkan kualitas layanan keamanan informasi dan mendukung proses pengambilan keputusan terkait keamanan informasi.

(3) Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi pemerintah daerah.

(4) Manajemen pengetahuan sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi pemerintah daerah.

Bagian Keempat
Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik

Pasal 14

Pengamanan Sistem Elektronik dan pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf c dilaksanakan oleh Perangkat Daerah sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 15

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 14 terdiri atas:

a. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan nirsangkal terhadap data dan informasi;

b. penjaminan ketersediaan infrastruktur yang terdiri atas pusat data, jaringan intra pemerintah, dan sistem penghubung layanan penyelenggaraan pemerintahan berbasis elektronik; dan

c. penjaminan keutuhan, ketersediaan, dan keaslian aplikasi.

Pasal 16

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 15 Perangkat Daerah melakukan:

a. identifikasi;

b. deteksi;

c. proteksi; dan

d. penanggulangan dan pemulihan.

(2) Identifikasi sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui kegiatan analisis kerawanan dan risiko terhadap Sistem Elektronik.

(3) Deteksi sebagaimana dimaksud pada ayat (1) huruf b dilakukan melalui kegiatan analisis untuk menentukan adanya ancaman atau kejadian insiden pada Sistem Elektronik.

(4) Proteksi sebagaimana dimaksud pada ayat (1) huruf c dilakukan dengan kegiatan mitigasi risiko dan penerapan pelindungan terhadap Sistem Elektronik untuk menjamin keberlangsungan penyelenggaraan pemerintahan berbasis elektronik.

(5) Penanggulangan dan pemulihan sebagaimana dimaksud pada ayat (1) huruf d dilakukan dengan kegiatan penanganan yang tepat dan perbaikan terhadap adanya insiden pada Sistem Elektronik agar penyelenggaraan pemerintahan berbasis elektronik berfungsi kembali dengan baik.

Pasal 17

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 15 Pemerintah Daerah wajib menggunakan Sertifikat Elektronik pada setiap layanan publik dan layanan pemerintahan berbasis elektronik.

(2) Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) diterbitkan oleh BSSN dan/atau lembaga penyelenggara Sertifikasi Elektronik dalam negeri yang telah diakui.

(3) Untuk mendapatkan Sertifikat elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 18

(1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 17 ayat (1) Pemerintah Daerah dapat menyelenggarakan pusat operasi Pengamanan Informasi sesuai standar yang ditetapkan oleh BSSN.

(2) Pusat operasi Pengamanan Informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk pengamanan sistem elektronik dengan melakukan proses pengawasan, penanggulangan, dan pemulihan atas insiden keamanan sistem elektronik dengan memperhatikan aspek personel, proses pelaksanaan, dan ketersediaan teknologi.

Pasal 19

(1) Pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 14 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi nonelektronik.

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

Pasal 20

(1) Perangkat Daerah melaksanakan audit keamanan informasi di lingkup pemerintah daerah.

(2) Audit keamanan informasi meliputi audit keamanan sistem elektronik dan audit pelaksanaan sistem manajemen.

(3) Audit keamanan informasi sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima
Penyediaan Layanan Keamanan Informasi

Pasal 21

(1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf d dilaksanakan oleh Perangkat Daerah.

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

a. Bupati dan wakil Bupati Wakatobi;

b. perangkat daerah;

c. pegawai atau aparatur sipil negara pada pemerintah daerah; dan

d. pihak lainnya.

Pasal 22

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 21 ayat (1) meliputi:

a. identifikasi kerentanan dan penilaian risiko terhadap sistem elektronik;

b. asistensi dan fasilitasi penguatan keamanan sistem elektronik;

c. penerapan sertifikat elektronik untuk melindungi sistem elektronik dan dokumen elektronik;

d. perlindungan informasi melalui penyediaan perangkat teknologi keamanan informasi dan jaring komunikasi sandi;

e. fasilitasi sertifikasi penerapan manajemen pengamanan sistem elektronik;

f. audit keamanan sistem elektronik;

g. audit keamanan pelaksanaan sistem manajemen;

h. literasi keamanan informasi dalam rangka peningkatan kesadaran keamanan informasi dan pengukuran tingkat kesadaran keamanan informasi di lingkungan pemerintah daerah dan publik;

i. peningkatan kompetensi sumber daya manusia di bidang keamanan informasi dan/atau persandian;

j. pengelolaan pusat operasi pengamanan informasi;

k. penanganan insiden keamanan sistem elektronik;

l. forensik digital;

m. perlindungan informasi pada kegiatan penting pemerintah daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;

n. perlindungan informasi pada aset/fasilitas penting milik atau yang akan digunakan pemerintah daerah melalui kegiatan kontra penginderaan;

o. konsultasi keamanan informasi bagi pengguna layanan; dan/atau

p. jenis layanan keamanan informasi lainnya.

Pasal 23

(1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 22 Perangkat Daerah melaksanakan manajemen Layanan Keamanan Informasi.

(2) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan Keamanan Informasi kepada Pengguna Layanan.

(3) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) merupakan penanganan terhadap keluhan, gangguan, masalah, permintaan, dan/atau perubahan Layanan Keamanan Informasi dari Pengguna Layanan.

(4) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen Layanan Keamanan Informasi.

BAB III
PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH

Pasal 24

(1) Penetapan pola hubungan komunikasi sandi antar perangkat daerah untuk menentukan jaring komunikasi sandi internal pemerintah daerah.

(2) Jaring komunikasi sandi internal pemerintah daerah sebagaimana dimaksud pada ayat (1) terdiri atas:

a. jaring komunikasi sandi antar perangkat daerah;

b. jaring komunikasi sandi internal perangkat daerah; dan

c. jaring komunikasi sandi pimpinan daerah.

(3) Jaring komunikasi sandi antar perangkat daerah sebagaimana dimaksud pada ayat (2) huruf a menghubungkan seluruh perangkat daerah.

(4) Jaring komunikasi sandi internal perangkat daerah sebagaimana dimaksud pada ayat (2) huruf b menghubungkan antar Pengguna Layanan di lingkup internal perangkat daerah.

(5) Jaring komunikasi sandi pimpinan daerah sebagaimana dimaksud pada ayat (2) huruf c menghubungkan antara Bupati, Wakil Bupati dan kepala perangkat daerah.

Pasal 25

(1) Penetapan pola hubungan komunikasi sandi antar perangkat daerah sebagaimana dimaksud dalam Pasal 24 ayat (1) dilaksanakan melalui:

a. identifikasi pola hubungan komunikasi sandi; dan

b. analisis pola hubungan komunikasi sandi.

(2) Identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf a, dilakukan terhadap:

a. pola hubungan komunikasi pimpinan dan pejabat structural internal pemerintah daerah;

b. alur informasi yang dikomunikasikan antar perangkat daerah dan internal perangkat daerah;

c. teknologi informasi dan komunikasi;

d. infrastruktur komunikasi; dan

e. kompetensi personil.

(3) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (2).

(4) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (3) memuat:

a. pengguna Layanan yang akan terhubung dalam jaring komunikasi sandi;

b. topologi atau bentuk atau model keterhubungan jaring komunikasi sandi antar Pengguna Layanan;

c. perangkat keamanan teknologi Informasi dan komunikasi, dan infrastruktur komunikasi, serta fasilitas lainnya yang dibutuhkan; dan

d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.

BAB IV
PEMANTAUAN, EVALUASI DAN PELAPORAN

Pasal 26

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

(2) Perangkat Daerah melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) setiap 1 (satu) tahun sekali.

(3) Perangkat Daerah kabupaten/kota menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) kepada Bupati dan Gubernur sebagai wakil Pemerintah Pusat.

Pasal 27

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

BAB V
PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 28

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetepan pola hubungan komunikasi sandi antar perangkat daerah dilaksanakan oleh BSSN dan Gubernur sebagai wakil Pemerintah Pusat sesuai dengan kewenangannya.

Pasal 29

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

Pasal 30

(1) Dalam melaksanakan pembinaan dan pengawasan teknis sebagaimana dimaksud dalam Pasal 28 BSSN dan pemerintah daerah provinsi sesuai dengan kewenangannya menyelenggarakan rapat koordinasi urusan Persandian.

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

BAB VI
PENDANAAN

Pasal 31

Pendanaan pelaksanaan penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar perangkat daerah bersumber dari:

a. Anggaran Pendapatan dan Belanja Daerah Kabupaten Wakatobi; dan/atau

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

BAB VII
KETENTUAN PENUTUP

Pasal 32

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Wakatobi.

PARAF KOORDINASI

NO	UNIT/SATUAN KERJA	PARAF
1	SEKRETARIS DAERAH	
2	ASS. PEREKONOMIAN & PEMB	
3	KADIS. KOMINFO	
4	KABAG. HUKUM	
5		

Ditetapkan di Wangi-Wangi
pada tanggal 28-3- 2022

BUPATI WAKATOBI,

HALIANA

Diundangkan di Wangi-Wangi
pada tanggal 1-7- 2022

SEKRETARIS DAERAH KABUPATEN WAKATOBI,

LA JUMADIN

BERITA DAERAH KABUPATEN WAKATOBI TAHUN 2022 NOMOR 43