



BUPATI GARUT
PROVINSI JAWA BARAT
PERATURAN BUPATI GARUT
NOMOR 146 TAHUN 2023

TENTANG

PEDOMAN PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI
PEMERINTAH DAERAH

BUPATI GARUT,

- Menimbang : a. bahwa dalam melindungi informasi di lingkungan Pemerintah Kabupaten Garut, perlu dilakukan upaya pengamanan informasi melalui penyelenggaraan persandian;
- b. bahwa berdasarkan ketentuan Pasal 4 ayat (2) Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, Bupati sesuai dengan kewenangannya bertanggung jawab terhadap penyelenggaraan persandian untuk pengamanan informasi;
- c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah;
- Mengingat : 1. Undang-Undang Nomor 14 Tahun 1950 tentang Pembentukan Daerah-daerah Kabupaten Dalam Lingkungan Provinsi Jawa Barat (Berita Negara Tahun 1950) sebagaimana telah diubah dengan Undang-Undang Nomor 4 Tahun 1968 tentang Pembentukan Kabupaten Purwakarta dan Kabupaten Subang dengan Mengubah Undang-Undang Nomor 14 Tahun 1950 tentang Pembentukan Daerah-daerah Kabupaten Dalam Lingkungan Provinsi Jawa Barat (Lembaran Negara Republik Indonesia Tahun 1968 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 2851);
2. 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);
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. 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 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);
5. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
6. 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);
7. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);
8. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
9. Peraturan Daerah Kabupaten Garut Nomor 6 Tahun 2016 tentang Urusan Pemerintahan Konkuren Kabupaten Garut (Lembaran Daerah Kabupaten Garut Tahun 2016 Nomor 6);
10. Peraturan Daerah Kabupaten Garut Nomor 9 Tahun 2016 tentang Pembentukan dan Susunan Organisasi Perangkat Daerah Kabupaten Garut (Lembaran Daerah Kabupaten Garut Tahun 2016 Nomor 9) sebagaimana telah diubah dengan Peraturan Daerah Kabupaten Garut Nomor 10 Tahun 2021 tentang Perubahan Atas Peraturan Daerah Nomor 9 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Garut (Lembaran Daerah Kabupaten Garut Tahun 2021 Nomor 10);
11. Peraturan Bupati Garut Nomor 27 Tahun 2016 tentang Kedudukan dan Susunan Organisasi Perangkat Daerah Kabupaten Garut (Berita Daerah Kabupaten Garut Tahun 2016 Nomor 27) sebagaimana telah diubah beberapa kali, terakhir dengan Peraturan Bupati Garut Nomor 228 Tahun 2022 tentang Perubahan Kelima Atas Peraturan Bupati Nomor 27 Tahun 2016 tentang Kedudukan dan Susunan Organisasi Perangkat Daerah Kabupaten Garut (Berita Daerah Kabupaten Garut Tahun 2022 Nomor 228);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG PEDOMAN PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI PEMERINTAH DAERAH.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah Kabupaten yang selanjutnya disebut Daerah adalah Daerah Kabupaten Garut.
2. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Bupati adalah Bupati Kabupaten Garut.
4. Perangkat Daerah adalah unsur pembantu Bupati dan DPRD dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
5. Dinas adalah Perangkat Daerah yang melaksanakan urusan pemerintahan Bidang Persandian dan Keamanan Informasi.
6. Badan Siber dan Sandi Negara yang selanjutnya disebut BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.
7. 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 non elektronik.
8. 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.
9. Jaring Komunikasi Sandi yang selanjutnya disingkat JKS adalah keterhubungan antar pengguna Persandian melalui jaring telekomunikasi.
10. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan dan kenirsangkalan Informasi.
11. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
12. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
13. Pola Hubungan Komunikasi Sandi yang selanjutnya disingkat PHKS adalah bentuk atau pola hubungan antara dua entitas atau lebih dalam proses pengiriman dan penerimaan informasi/pesan/berita secara aman menggunakan Persandian;
14. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik;
15. 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.
16. 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 Balai Sertifikasi Elektronik Badan Siber dan Sandi Negara.

17. 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 memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

BAB II

MAKSUD DAN TUJUAN

Pasal 2

Peraturan ini dimaksudkan untuk memberikan acuan bagi Pemerintah Daerah dalam melaksanakan kebijakan, program dan kegiatan penyelenggaraan Persandian untuk pengamanan Informasi Pemerintah Daerah.

Pasal 3

Peraturan Bupati ini bertujuan untuk:

- a. menciptakan harmonisasi dalam melaksanakan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah Kabupaten;
- b. menjadi dasar pelaksanaan penyelenggaraan Persandian untuk pengamanan Informasi di lingkungan Pemerintah Daerah;
- c. meningkatkan komitmen, efektivitas pelaksanaan kebijakan, program dan kegiatan penyelenggaraan Persandian untuk pengamanan Informasi di lingkungan Pemerintah Daerah; dan
- d. meningkatkan kinerja penyelenggaraan Persandian di lingkungan Pemerintah Daerah; dan
- e. memberikan pedoman bagi Dinas dalam menetapkan PHKS antar Perangkat Daerah

Pasal 4

Pelaksanaan persandian untuk pengamanan informasi di Pemerintah Daerah sebagaimana dimaksud dalam Pasal 3 meliputi:

- a. penyelenggaraan Persandian untuk Pengamanan Informasi dan
- b. penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.

BAB III

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

Bagian Kesatu

Umum

Pasal 5

- (1) Penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah sebagaimana dimaksud dalam Pasal 4 huruf a dilaksanakan melalui:
 - a. penyusunan kebijakan Pengamanan Informasi;
 - b. pengelolaan sumber daya Keamanan Informasi;
 - c. pengamanan Sistem Elektronik dan pengamanan informasi non elektronik; dan

- d. penyediaan layanan Keamanan Informasi.
- (2) Bupati bertanggung jawab terhadap Penyelenggaraan Persandian untuk Pengamanan Informasi.

Bagian Kedua

Penyusunan Kebijakan Pengamanan Informasi

Pasal 6

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) 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 7

- (1) Rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 6 huruf a disusun oleh Bupati melalui Dinas.
- (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.
- (4) Dalam melakukan penyusunan rencana strategis sebagaimana dimaksud pada ayat (1) Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN.

Pasal 8

- (1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 6 huruf b ditetapkan dengan Keputusan Bupati untuk jangka waktu 5 (lima) tahun.
- (2) Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) memuat:
 - a. infrastruktur teknologi informasi;
 - b. desain keamanan perangkat teknologi informasi dan keamanan jaringan; dan
 - c. aplikasi keamanan perangkat teknologi informasi dan keamanan jaringan.
- (3) Dalam melakukan penyusunan Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1), Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN.
- (4) Arsitektur Keamanan Informasi dilakukan evaluasi oleh Bupati pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu-waktu sesuai dengan kebutuhan.

Pasal 9

- (1) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 6 huruf c paling sedikit terdiri atas:
 - a. keamanan sumber daya teknologi informasi;
 - b. keamanan akses kontrol;

- c. keamanan data dan informasi;
 - d. keamanan SDM;
 - e. keamanan Jaringan;
 - f. keamanan surat elektronik;
 - g. keamanan pusat data; dan/atau
 - h. keamanan komunikasi.
- (2) Dalam melakukan penyusunan aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1), Bupati melalui Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN.
 - (3) Ketentuan lebih lanjut mengenai tata kelola Keamanan Informasi ditetapkan dengan Standar Operasional Prosedur Dinas.

Bagian Ketiga

Pengelolaan Sumber Daya Keamanan Informasi

Pasal 10

- (1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf b dilaksanakan oleh Dinas.
- (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 11

- (1) Pengelolaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf a dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi.
- (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 12

- (1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf b dilakukan oleh Dinas.
- (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 13

- (1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 12 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 12 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 12 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 14

- (1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf c dilakukan oleh Dinas.
- (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.
- (4) Manajemen pengetahuan sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi.
- (5) Dalam pelaksanaan manajemen pengetahuan, Pemerintah Daerah berkoordinasi dan dapat melakukan konsultasi dengan BSSN.

Bagian Keempat

Pengamanan Sistem Elektronik dan Pengamanan Informasi Non Elektronik

Pasal 15

Pengamanan Sistem Elektronik dan pengamanan informasi non elektronik sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf c dilaksanakan oleh Dinas sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 16

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 15 terdiri atas:

- a. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan nirsangkalan 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 17

- (1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 16, Dinas 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 perlindungan 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 18

- (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 19

- (1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 18 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 20

- (1) Pengamanan informasi non elektronik sebagaimana dimaksud dalam Pasal 15 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi non elektronik.
- (2) Pengamanan Informasi non elektronik sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 21

- (1) Dinas 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 22

- (1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf d dilaksanakan oleh Dinas.
- (2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:
 - a. bupati dan wakil bupati;
 - b. perangkat daerah;
 - c. aparatur sipil negara pada Pemerintah Daerah; dan
 - d. pihak lainnya.

Pasal 23

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 22 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. Perlindungan informasi pada kegiatan penting pemerintah daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;
- m. perlindungan Informasi pada aset/fasilitas penting milik atau yang akan digunakan pemerintah daerah melalui kegiatan kontra penginderaan;
- n. konsultasi Keamanan Informasi bagi Pengguna Layanan; dan/atau
- o. jenis Layanan Keamanan Informasi lainnya.

Pasal 24

- (1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 23 Dinas 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 25

- (1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 4 huruf b ditetapkan oleh Bupati.
- (2) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (1) untuk menentukan jaring komunikasi sandi internal Pemerintah Daerah.
- (3) Jaring komunikasi sandi internal pemerintah daerah sebagaimana dimaksud pada ayat (2) terdiri atas:
 - a. jaring komunikasi sandi antar Perangkat Daerah;
 - b. jaring komunikasi sandi internal Perangkat Daerah;
 - c. jaring komunikasi sandi pimpinan daerah.
- (4) Jaring komunikasi sandi antar perangkat daerah sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh Perangkat Daerah.
- (5) Jaring komunikasi sandi internal perangkat daerah sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar Pengguna Layanan di lingkup internal Perangkat Daerah.
- (6) Jaring komunikasi sandi pimpinan daerah sebagaimana dimaksud pada ayat (3) huruf c menghubungkan antara Bupati, Wakil Bupati dan Kepala Perangkat Daerah.

Pasal 26

- (1) Penetapan pola hubungan komunikasi sandi antar perangkat daerah provinsi dan kabupaten/kota sebagaimana dimaksud dalam Pasal 25 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 struktural 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 personel.
- (3) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (2) huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi.
- (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.
- (5) Hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (4) merupakan pola hubungan komunikasi sandi antar Perangkat Daerah yang ditetapkan dengan Keputusan Bupati.
- (6) Keputusan sebagaimana dimaksud pada ayat (5) paling sedikit memuat :
 - a. entitas Pengguna layanan yang terhubung dalam jaring komunikasi sandi;
 - b. topologi atau bentuk atau model keterhubungan antar Pengguna Layanan;
 - c. sarana dan prasarana yang digunakan; dan
 - d. tugas dan tanggung jawab pengelola dan Pengguna Layanan
- (7) Salinan keputusan sebagaimana dimaksud pada ayat (6) disampaikan oleh Bupati kepada Gubernur dan ditembuskan kepada Kepala BSSN.

BAB IV

PEMANTAUAN, EVALUASI DAN PELAPORAN

Pasal 27

- (1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan PHKS.
- (2) Dinas melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) setiap 1 (satu) tahun sekali.
- (3) Dinas menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) kepada Bupati dan di tembuskan kepada Kepala BSSN melalui Gubernur.
- (4) Laporan hasil evaluasi sebagaimana dimaksud pada ayat (3) memuat capaian kinerja Dinas.

BAB V

KOORDINASI DAN KONSULTASI

Pasal 28

- (1) Dalam rangka pelaksanaan urusan pemerintahan bidang persandian dan Keamanan Informasi, Dinas dapat melaksanakan koordinasi dan/atau konsultasi ke BSSN, Perangkat Daerah terkait maupun antar Pemerintah Daerah lainnya.
- (2) Koordinasi dan konsultasi sebagaimana dimaksud pada ayat (1) dapat dilaksanakan dengan cara melakukan kunjungan langsung di lapangan (*on site*) dan/atau menggunakan media komunikasi lainnya.

BAB VI

PENDANAAN

Pasal 29

Pendanaan pelaksanaan penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah bersumber dari:

- a. Anggaran Pendapatan dan Belanja Daerah Kabupaten Garut; dan
- b. sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB VII

KETENTUAN PENUTUP

Pasal 30

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Garut
pada tanggal 23 - 9 - 2023
BUPATI GARUT,

t t d

RUDY GUNAWAN

Diundangkan di Garut
pada tanggal 23 - 9 - 2023

SEKRETARIS DAERAH KABUPATEN GARUT,

t t d

NURDIN YANA
BERITA DAERAH KABUPATEN GARUT
TAHUN 2023 NOMOR 146