



BUPATI GARUT  
PROVINSI JAWA BARAT  
PERATURAN BUPATI GARUT  
NOMOR 147 TAHUN 2023  
TENTANG  
MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN  
BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI GARUT,

- Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;
- b. bahwa berdasarkan ketentuan Pasal 33 ayat (3) Peraturan Bupati Garut Nomor 35 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik, manajemen keamanan informasi dilaksanakan oleh seluruh Perangkat Daerah di lingkungan Pemerintah Daerah;
- c. bahwa kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik tepat guna, maka dipandang perlu adanya pengaturan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;
- d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Bupati tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;
- 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 Nomor 2851);

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 diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
3. Undang-Undang Nomor 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 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
5. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 152, Tambahan Lembaran Negara Republik Indonesia Nomor 5071);
6. 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);
7. 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);
8. 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);
9. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
10. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
11. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);

12. 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);
13. 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)
14. 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);
15. 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);
16. Peraturan Daerah Kabupaten Garut Nomor 21 Tahun 2014 tentang Keterbukaan Informasi Publik (Lembaran Daerah Kabupaten Garut Tahun 2014 Nomor 21, Tambahan Lembaran Daerah Kabupaten Garut Nomor 252);
17. Peraturan Daerah Kabupaten Garut Nomor 6 Tahun 2016 tentang Urusan Pemerintahan Konkuren Kabupaten Garut (Lembaran Daerah Kabupaten Garut Tahun 2016 Nomor 6);
18. Peraturan Daerah Kabupaten Garut Nomor 9 Tahun 2016 tentang Pembentukan dan Susunan 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);
19. 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 beberapa kali diubah, terakhir dengan Peraturan Bupati Garut Nomor 228 Tahun 2022 tentang Perubahan Kelima Atas Peraturan Bupati Garut Nomor 27 Tahun 2016 tentang Kedudukan dan Susunan Organisasi Perangkat Daerah Kabupaten Garut (Berita Daerah Kabupaten Garut Tahun 2022 Nomor 228);
20. Peraturan Bupati Garut Nomor 22 Tahun 2018 tentang Pemanfaatan Teknologi Informasi dan Komunikasi Dalam Penyelenggaraan Pemerintahan Daerah (Berita Daerah Kabupaten Garut Tahun 2018 Nomor 22);
21. Peraturan Bupati Garut Nomor 35 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Garut Tahun 2022 Nomor 35);

## MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

## 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 Garut.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Garut.
5. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah Kabupaten dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
6. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
7. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
8. 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.
9. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
10. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan informasi, infrastruktur SPBE, dan aplikasi SPBE.
11. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasiaan (*confidentiality*) atas informasi dan komunikasi secara Elektronik.
12. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (*integrity*) atas Informasi Elektronik.
13. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (*availability*) atas Informasi Elektronik.
14. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
15. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
16. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
17. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.

18. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran Layanan SPBE.
19. Infrastruktur SPBE 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.
20. *Application Programming Interface* yang selanjutnya disingkat API adalah sekumpulan perintah, fungsi, serta protokol yang mengintegrasikan dua bagian dari aplikasi atau dengan aplikasi yang berbeda secara bersamaan.
21. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
22. Pusat Data Nasional adalah sekumpulan Pusat Data yang digunakan secara bagi pakai oleh Instansi Pusat dan Pemerintah Daerah, dan saling terhubung.

## Pasal 2

Peraturan Bupati ini dimaksudkan sebagai pedoman bagi Pemerintah Daerah dalam pelaksanaan Manajemen Keamanan Informasi SPBE.

## BAB II

### RUANG LINGKUP

#### Pasal 3

- (1) Ruang lingkup manajemen keamanan informasi SPBE meliputi:
  - a. data dan informasi SPBE;
  - b. Aplikasi SPBE; dan
  - c. Infrastruktur SPBE.
- (2) Ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan area yang menjadi prioritas terhadap pelaksanaan keamanan informasi SPBE.

## BAB III

### PENANGGUNG JAWAB

#### Pasal 4

- (1) Bupati menetapkan Sekretaris Daerah sebagai penanggung jawab Keamanan SPBE.
- (2) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan SPBE sebagaimana dimaksud pada ayat (1), Sekretaris Daerah disebut sebagai Koordinator SPBE.

#### Pasal 5

- (1) Koordinator SPBE sebagaimana dimaksud dalam Pasal 4 ayat (2) menetapkan pelaksana teknis Keamanan SPBE.
- (2) Pelaksana teknis Keamanan SPBE sebagai dimaksud pada ayat (1) terdiri atas:
  - a. ketua tim; dan
  - b. anggota tim.

- (3) Ketua Tim sebagaimana dimaksud pada ayat (2) huruf a dijabat oleh Kepala Perangkat Daerah yang melaksanakan urusan pemerintahan bidang komunikasi dan informatika.
- (4) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari Kepala Perangkat Daerah yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di Daerah.

#### Pasal 6

- (1) Ketua tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE di Daerah yang meliputi:
  - a. menetapkan prosedur pengendalian keamanan informasi SPBE;
  - b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE;
  - c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai ketentuan peraturan perundang-undangan;
  - d. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
  - e. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recovery plans*; dan
  - f. melaporkan pelaksanaan manajemen keamanan informasi SPBE pada koordinator SPBE.
- (2) Anggota tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b mempunyai tugas:
  - a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian keamanan informasi SPBE pada Perangkat Daerah masing-masing;
  - b. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai ketentuan peraturan perundang-undangan;
  - c. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan
  - d. berkoordinasi dengan ketua tim terkait penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE.

### BAB IV

#### PERENCANAAN

#### Pasal 7

- (1) Perencanaan Manajemen Keamanan SPBE dilakukan oleh pelaksana teknis Keamanan SPBE.
- (2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
  - a. program kerja Keamanan SPBE; dan
  - b. target realisasi program kerja Keamanan SPBE.

## Pasal 8

- (1) Program kerja Keamanan SPBE sebagaimana dimaksud pada Pasal 7 ayat (2) huruf a paling sedikit meliputi:
  - a. edukasi kesadaran Keamanan SPBE;
  - b. penilaian kerentanan Keamanan SPBE;
  - c. peningkatan Keamanan SPBE;
  - d. penanganan insiden Keamanan SPBE; dan
  - e. audit Keamanan SPBE.
- (2) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud pada Pasal 7 ayat (2) huruf b ditetapkan berdasarkan kebutuhan Pemerintah Daerah.

## BAB V

## DUKUNGAN PENGOPERASIAN

## Pasal 9

- (1) Dukungan pengoperasian manajemen keamanan informasi SPBE dilakukan oleh koordinator SPBE.
- (2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:
  - a. sumber daya manusia Keamanan SPBE;
  - b. teknologi keamanan SPBE; dan
  - c. anggaran keamanan SPBE.
- (3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan manajemen keamanan informasi SPBE diberikan alokasi sumber daya yang sesuai.

## Pasal 10

- (1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf a paling sedikit berjumlah 5 (lima) orang dengan ketentuan harus memiliki kompetensi:
  - a. keamanan TIK; dan
  - b. keamanan aplikasi.
- (2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), paling sedikit harus adanya dukungan kegiatan:
  - a. pelatihan dan/atau sertifikasi kompetensi keamanan aplikasi dan TIK; dan/atau
  - b. bimbingan teknis mengenai standar teknis dan prosedur Keamanan SPBE.
- (3) Pemenuhan kompetensi sebagaimana dimaksud pada ayat (2) dilakukan agar sumber daya manusia Keamanan SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan Keamanan SPBE.
- (4) Teknologi keamanan informasi sebagaimana dimaksud pada Pasal 9 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.
- (5) Anggaran Keamanan SPBE sebagaimana dimaksud pada Pasal 9 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai ketentuan ketentuan peraturan perundang-undangan.

## Pasal 11

- (1) Evaluasi kinerja manajemen keamanan informasi SPBE dilakukan oleh koordinator SPBE.
- (2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan manajemen keamanan informasi SPBE di Pemerintah Daerah.
- (3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
  - a. menganalisis efektifitas pelaksanaan Keamanan SPBE; atau
  - b. mendukung dan merealisasikan program audit Keamanan SPBE.
- (4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

## Pasal 12

- (1) Perbaikan berkelanjutan manajemen keamanan informasi SPBE dilakukan oleh pelaksana teknis Keamanan SPBE.
- (2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.
- (3) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:
  - a. mengatasi permasalahan dalam pelaksanaan Keamanan SPBE;
  - b. memperbaiki pelaksanaan Keamanan SPBE secara periodik; dan
  - c. tindak lanjut hasil audit Keamanan SPBE.

## BAB VI

## PENGENDALIAN TEKNIS KEAMANAN

## Pasal 13

- (1) Manajemen risiko manajemen keamanan informasi SPBE dilakukan oleh setiap Perangkat Daerah.
- (2) Manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko dengan ketentuan substansi meliputi:
  - a. inventarisasi aset SPBE;
  - b. identifikasi ancaman dan kerentanan keamanan terhadap aset SPBE;
  - c. penilaian risiko keamanan terhadap aset SPBE;
  - d. penentuan prioritas risiko;
  - e. analisa dampak jika terjadi risiko;
  - f. analisa kontrol keamanan yang bisa diterapkan; dan/atau
  - g. rekomendasi kontrol keamanan.
- (3) Prosedur pelaksanaan manajemen risiko mengacu sesuai ketentuan peraturan perundang-undangan.

## Pasal 14

- (1) Penetapan prosedur pengendalian keamanan informasi SPBE manajemen keamanan informasi SPBE ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE.



- (2) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan manajemen keamanan informasi SPBE di Pemerintah Daerah dengan cakupan aspek dapat 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 kontrol;
  - h. pengendalian keamanan dari ancaman virus dan *malware*;
  - i. persyaratan keamanan terkait pembangunan dan pengembangan aplikasi SPBE;
  - j. pengelolaan aset;
  - k. keamanan migrasi data;
  - l. konfigurasi perangkat *IT Security*;
  - m. perlindungan 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 TIK (*disaster recovery plans*);
  - u. audit internal keamanan SPBE; dan/atau
  - v. aspek prosedur pengendalian keamanan informasi SPBE lainnya.
- (3) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dengan surat edaran sekretaris daerah.

#### Pasal 15

- (1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 14 ayat (3).
- (2) Setiap Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian keamanan informasi SPBE.

#### Pasal 16

- (1) Pengelolaan pihak ketiga manajemen keamanan informasi SPBE dilakukan oleh setiap Perangkat Daerah.

- (2) Perangkat Daerah harus memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan.
- (3) Perangkat Daerah harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE 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 membuat laporan secara berkala tentang pencapaian Sasaran Tingkat Layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

## BAB VII

### KETENTUAN PENUTUP

#### Pasal 17

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita 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 147