SALINAN

BUPATI GARUT

PROVINSI JAWA BARAT

PERATURAN BUPATI GARUT

NOMOR 51 TAHUN 2025

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI GARUT,

Menimbang : a. bahwa untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, efisien, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya diperlukan penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Garut;

b. bahwa dalam rangka menjamin kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan sumber daya terkait data dan informasi, infrastruktur dan aplikasi sistem Pemerintahan Berbasis Elektronik, perlu melaksanakan manajemen keamanan informasi Sistem Pemerintahan Berbasis Elektronik;

c. bahwa untuk memberikan arah, landasan, dan kepastian hukum dalam menjamin keberlangsungan Sistem Pemerintahan Berbasis Elektronik dengan meminimalkan dampak risiko keamanan informasi perlu adanya pengaturan mengenai 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 Garut tentang Sistem Manajemen Keamanan Informasi;

Mengingat : 1. 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 beberapa kali 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);

2. 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);
3. Undang-Undang Nomor 110 Tahun 2024 tentang Kabupaten Garut di Provinsi Jawa Barat (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 296, Tambahan Lembaran Negara Republik Indonesia Nomor 7047);
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 Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);
7. 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);
8. 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 SISTEM MANAJEMEN KEAMANAN INFORMASI.

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. 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.
8. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang mencakup seluruh peralatan teknis untuk memproses dan menyampaikan informasi.
9. Data adalah tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange*, surat elektronik, *telegram*, *teleks*, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi.
10. Informasi Elektronik adalah satu atau sekumpulan data, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange*, surat elektronik, telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
11. Aplikasi adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan.
12. Infrastruktur 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.
13. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan keamanan informasi berdasarkan pendekatan risiko.
14. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan dan kenirsangkalan informasi.

15. Risiko adalah kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negatif terhadap pencapaian sasaran kinerja dan layanan sistem elektronik.
16. Manajemen Risiko adalah aktivitas terkoordinasi untuk identifikasi, penilaian, dan penentuan prioritas risiko yang kemudian akan dikelola, dipantau, dan dikontrol untuk mengurangi dampak dan/atau kemungkinan terjadinya risiko tersebut.
17. Rencana Tindak Lanjut risiko yang selanjutnya disebut RTL adalah respon yang direncanakan manajemen untuk menindaklanjuti hasil evaluasi risiko, seperti *mitigate/reduce*, *avoid*, *share/transfer* atau *accept*.
18. Audit adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.
19. Auditor Keamanan Informasi yang selanjutnya disebut Auditor adalah orang yang memiliki kompetensi untuk melakukan Audit Keamanan Informasi.
20. Audit Internal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi internal Pemerintah Daerah.
21. Audit Eksternal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi eksternal Pemerintah Daerah yang memiliki sertifikasi Auditor Keamanan Informasi.
22. Auditan adalah keseluruhan atau sebagian dari organisasi yang diaudit.
23. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
24. 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.
25. Insiden siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam keamanan informasi antara lain namun tidak terbatas pada *web defacement*, *malware unauthorized access*, data *breach*, dan *Distributed Denial of Service*.
26. Tim Tanggap Insiden Siber yang selanjutnya disebut TTIS adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.

27. Tim Pengelola Sistem Manajemen Keamanan Informasi yang selanjutnya disebut Tim SMKI adalah sekelompok orang yang bertanggung jawab untuk menyusun, mengkomunikasikan, memastikan, dan memantau pelaksanaan SMKI di Pemerintah Daerah.
28. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan sumber daya terkait data dan informasi, infrastruktur SPBE, dan aplikasi SPBE.
29. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
30. Enkripsi adalah proses mengubah data teks biasa menjadi bentuk yang tidak dapat dibaca atau dimengerti oleh pihak yang tidak berwenang.
31. Kriptografi adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal untuk meningkatkan Keamanan Informasi dengan menggunakan 2 (dua) prinsip yaitu enkripsi dan deskripsi.
32. Penyimpanan Awan yang selanjutnya disebut dengan *Cloud* adalah teknologi penyimpanan data digital yang memungkinkan menyimpan, mengakses, dan mengelola file di server yang terhubung melalui internet.
33. Penilaian Kerentanan adalah proses mengidentifikasi, menganalisis, dan memprioritaskan celah keamanan pada sistem, jaringan, dan aplikasi berdasarkan tingkat kritikalitas.
34. Pencatatan adalah proses penyimpanan informasi terkait kejadian, aktivitas, dan interaksi pada aplikasi dan infrastruktur SPBE.
35. Manajemen Aset TIK adalah serangkaian proses untuk merencanakan, mengakuisisi, mengelola, dan menghapus seluruh aset aplikasi dan infrastruktur SPBE.
36. Peta Rencana SPBE adalah dokumen yang mendeskripsikan arah dan langkah penyiapan dan pelaksanaan SPBE yang terintegrasi.
37. Layanan Informasi adalah layanan yang menyediakan, mengelola, dan menyajikan informasi untuk memenuhi kebutuhan pelayanan informasi.

Pasal 2

(1) Peraturan Bupati ini dimaksudkan sebagai pedoman bagi Pemerintah Daerah dalam penerapan manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah.

(2) Pedoman dalam penerapan manajemen Kemanana Informasi SPBE sebagaimana dimaksud pada ayat (1) meliputi:

a. penetapan ruang lingkup;

b. penetapan penanggung jawab SMKI;

c. perencanaan;

d. dukungan pengoperasian;

e. kendali keamanan;

f. audit Keamanan Informasi; dan

g. evaluasi kinerja dan perbaikan berkelanjutan Keamanan Informasi.

(3) Kendali keamanan sebagaimana diatur pada ayat (2) huruf e terdiri dari:

a. keamanan sumber daya manusia;

b. keamanan aset informasi;

c. keamanan akses;

d. keamanan kriptografi;

e. keamanan fisik dan lingkungan;

f. keamanan opersional;

g. keamanan komunikasi;

h. keamanan pengembangan dan pemeliharaan;

i. keamanan Pihak Ketiga;

j. manajemen insiden siber;

k. manajemen keberlangsungan layanan informasi; dan

l. pengendalian kepatuhan.

BAB II

KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI

Bagian Kesatu

Penetapan Ruang Lingkup

Pasal 3

(1) Penetapan ruang lingkup manajemen Keamanan Informasi sebagaimana dimaksud dalam pasal 2 ayat (2) huruf a meliputi:

a. data dan informasi;

b. aplikasi;

c. infrastruktur; dan

d. sumber daya manusia.

(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Daerah yang harus diamankan.

Bagian Kedua

Penanggung Jawab

Pasal 4

(1) Sekretaris Daerah selaku koordinator SPBE berperan sebagai penanggung jawab SMKI.

(2) Dalam melaksanakan tanggung jawab sebagaimana dimaksud pada ayat (1), Sekretaris Daerah dibantu oleh Tim SMKI selaku pelaksana teknis Keamanan Informasi.

(3) Penanggung jawab SMKI sebagaimana dimaksud pada ayat (1) ditetapkan oleh Bupati.

Pasal 5

(1) Tim SMKI sebagaimana dimaksud dalam Pasal 4 ayat (2) terdiri atas:

a. ketua tim; dan

b. anggota tim.

(2) Ketua Tim sebagaimana dimaksud pada ayat (1) huruf a dijabat oleh Kepala Perangkat Daerah yang melaksanakan urusan pemerintahan bidang komunikasi dan informatika.

(3) Ketua tim SMKI sebagaimana dimaksud pada ayat (2) memiliki kewenangan dalam menentukan komposisi, kualifikasi, dan jumlah anggota tim.

(4) Anggota Tim Sebagaimana dimaksud pada ayat (1) huruf b terdiri dari Kepala Perangkat Daerah yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan aplikasi dan/atau infrastruktur Teknologi Informasi dan Komunikasi di Daerah.

(5) Khusus di lingkungan Sekretariat Daerah dan Sekretariat DPRD, anggota tim sebagaimana dimaksud pada ayat (4) dilaksanakan oleh kepala unit kerja yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan aplikasi dan/atau infrastruktur Teknologi Informasi dan Komunikasi di Daerah.

(6) Tim SMKI sebagaimana dimaksud pada ayat (1) ditetapkan oleh Bupati.

Pasal 6

Dalam pengelolaan SMKI di lingkungan Pemerintah Daerah, Perangkat Daerah yang melaksanakan urusan pemerintahan bidang pengawasan berperan melaksanakan audit internal Keamanan Informasi.

Pasal 7

(1) Sekretaris Daerah bertanggung jawab untuk:

a. memastikan pelaksanaan kebijakan SMKI;

b. menyediakan sumber daya yang memadai untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan SMKI Pemerintah Daerah;

c. menetapkan kriteria penerimaan risiko dan tingkat risiko yang dapat diterima;

d. memastikan pelaksanaan audit internal Keamanan Informasi;

e. menetapkan arsitektur Keamanan Informasi;

f. menetapkan peta rencana 5 (lima) tahunan dan sasaran Keamanan Informasi setiap tahunnya;

g. melakukan tinjauan secara berkala atas pelaksanaan kebijakan SMKI; dan

h. menyampaikan kinerja pelaksanaan kebijakan SMKI kepada Bupati.

(2) Tim SMKI sebagaimana dimaksud dalam Pasal 5 bertanggung jawab untuk:

a. menyusun, mengkomunikasikan, dan memantau pelaksanaan kebijakan SMKI di Pemerintah Daerah;

b. melakukan analisis kebutuhan Keamanan Informasi;

c. merumuskan, mengkoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan Informasi;

d. memastikan seluruh pembangunan dan/atau pengembangan aplikasi dan infrastruktur informasi termasuk yang dilakukan oleh Pihak Ketiga, minimal memenuhi Standar Teknis dan Prosedur Keamanan Informasi yang ditetapkan oleh badan yang melaksanakan tugas pemerintahan dibidang keamanan siber;

e. memastikan peningkatan kesadaran, kepedulian, dan kepatuhan oleh seluruh pegawai terhadap kebijakan, prosedur, dan standar Keamanan Informasi;

f. memastikan diterapkannya perjanjian menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen perjanjian kerahasiaan;

g. mengendalikan dan menjaga kemutakhiran kebijakan, prosedur, dan standar Keamanan Informasi;

h. memfasilitasi pelaksanaan audit internal dan audit eksternal Keamanan Informasi;

i. dalam memfasilitasi pelaksanaan audit eksternal Keamanan Informasi sebagaimana dimaksud pada huruf h, Tim SMKI dapat menunjuk pihak yang berkompeten dibidang audit Keamanan Informasi sebagai konsultan;

j. memastikan diterapkannya manejemen risiko, manajemen insiden siber, dan manajemen aset dalam pelaksanaan pengamanan aset informasi;

k. mendorong perbaikan penerapan Keamanan Informasi berdasarkan hasil temuan audit internal dan audit eksternal; dan

l. menyusun laporan evaluasi penerapan Kebijakan SMKI dan menyampaikannya kepada Sekretaris Daerah.

(3) Analisis kebutuhan Keamanan Informasi sebagaimanan dimaksud pada ayat (2) huruf b diselenggarakan dengan cara:

a. mengidentifikasi aplikasi dan infrastruktur untuk Keamanan Informasi;

b. mengidentifikasi standar kompetensi personel Keamanan Informasi; dan

c. mengidentifikasi program peningkatan kompetensi Keamanan Informasi dan penanggulangan insiden siber.

(4) Perangkat Daerah yang melaksanakan urusan pemerintahan bidang pengawasan internal sebagaimana dimaksud dalam Pasal 6 bertanggung jawab untuk :

a. menyusun pedoman audit internal Keamanan Informasi;

b. menyusun perencanaan audit internal Keamanan Informasi;

c. melaksanakan kegiatan audit internal Keamanan Informasi;

d. memberikan rekomendasi perbaikan atas hasil temuan audit internal Keamanan Informasi;

e. menyusun laporan audit Keamanan Informasi;

f. menyampaikan laporan audit internal Keamanan Informasi kepada Sekretaris Daerah.

Bagian Ketiga

Perencanaan Keamanan Informasi

Pasal 8

(1) Pemerintah Daerah sebagai Penyelenggara SPBE, melakukan kategorisasi setiap sistem elektronik yang dimilikinya sebagai salah satu dasar dalam pelaksanaan Keamanan Informasi.

(2) Penentuan kategorisasi sistem elektronik dilakukan sesuai peraturan perundangan yang ditetapkan oleh badan yang menyelenggarakan tugas pemerintahan dibidang keamanan siber.

Pasal 9

(1) Pelaksanaan Keamanan Informasi dilakukan dengan memperhatikan berbagai risiko yang dapat mengakibatkan terjadinya kegagalan Keamanan Informasi di Pemerintah Daerah.

(2) Dalam melaksanakan perencanaan Keamanan Informasi, Tim SMKI melakukan manajemen risiko Keamanan Informasi yang meliputi:

a. menyusun penilaian risiko Keamanan Informasi dengan megidentifikasi ancaman, kerentanan, peluang dan dampak apabila risiko terjadi;

b. menyusun RTL bersama Perangkat Daerah pemilik aset TIK; dan

c. melakukan sosialisasi dan komunikasi RTL kepada para pemilik risiko.

(3) Proses manajemen risiko dilakukan secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan juga apabila ada perubahan aset atau proses bisnis yang berdampak signifikan terhadap profil risiko yang ditetapkan.

Pasal 10

(1) Tim SMKI menyusun program kerja Keamanan Informasi berdasarkan RTL sebagai wujud realisasi atas tindak lanjut risiko Keamanan Informasi.

(2) Program kerja sebagaimana yang dimaksud pada ayat (1) dilakukan dengan merumuskan:

a. program kerja Keamanan Informasi; dan

b. target realisasi program kerja Keamanan Informasi.

(3) Program kerja Keamanan Informasi sebagaimana dimaksud pada ayat (2) paling sedikit meliputi:

a. edukasi kesadaran Keamanan Informasi;

b. penilaian kerentanan Keamanan Informasi;

c. peningkatan Keamanan Informasi;

d. penanganan insiden siber; dan

e. audit Keamanan Informasi.

(4) Program kerja Keamanan Informasi dituangkan dalam peta rencana Keamanan Informasi yang disusun untuk periode 5 (lima) tahunan dengan sasaran Keamanan Informasi yang ditetapkan untuk setiap tahunnya.

(5) Peta rencana Keamanan Informasi sebagaimana dimaksud pada ayat (4) menjadi bagian dari peta rencana SPBE.

Bagian Keempat

Dukungan Pengoperasian

Pasal 11

(1) Sekretaris Daerah memberikan dukungan pengoperasian Keamanan Informasi dengan menyediakan:

a. sumber daya manusia Keamanan Informasi yang berkompeten;

b. teknologi Keamanan Informasi; dan

c. anggaran Keamanan Informasi.

(2) Sumber daya Keamanan Informasi sebagaimana dimaksud dalam ayat (1) huruf a paling sedikit berjumlah 5 (lima) orang dengan ketentuan harus memiliki kompetensi:

a. keamanan infrastruktur TIK; dan

b. keamanan aplikasi

(3) Dalam hal sumber daya Keamanan Informasi yang disediakan belum memiliki kompetensi memadai, maka Sekretaris Daerah memfasilitasi peningkatan kompetensi melalui kegiatan pelatihan dan/atau bimbingan teknis:

a. pelatihan dan/atau sertifikasi komptensi keamanan aplikasi dan infrastruktur; dan

b. bimbingan teknis mengenai standar teknis dan prosedur Keamanan Informasi.

(4) Teknologi Keamanan Informasi sebagaimana dimaksud ayat (1) huruf b harus tersedia sesuai kebutuhan dan tingkat prioritas dari setiap Perangkat Daerah.

(5) Sekretaris Daerah memfasilitasi penyelenggaraan kegiatan kesadaran Keamanan Informasi bagi pegawai di lingkungan Pemerintah Daerah.

(6) Sekretaris Daerah menyediakan anggaran Keamanan Informasi berdasarkan arsitektur dan peta rencana Keamanan Informasi yang telah disusun.

Bagian Kelima

Kendali Keamanan

Paragraf 1

Keamanan Sumber Daya Manusia

Pasal 12

(1) Keamanan Sumber Daya Manusia dilakukan untuk mengendalikan Sumber Daya Manusia dalam melaksanakan Kebijakan SMKI.

(2) Keamanan Sumber Daya Manusia sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Tim SMKI, dengan cara sebagai berikut:

a. mengkomunikasikan peran dan tanggung jawab pelaksanaan Kebijakan SMKI kepada seluruh pegawai dan Pihak Ketiga yang terlibat dalam pengelolaan dan pengamanan aset informasi;

b. melakukan pembagian tugas dan wewenang untuk menghindari kesalahan atau pelanggaran;

c. melakukan pemeriksaan data pribadi pegawai dan Pihak Ketiga yang terlibat dalam pengelolaan dan pengamanan aset informasi;

d. membuat perjanjian tertulis dengan pegawai dan Pihak Ketiga yang terlibat dalam penggunaan dan/atau pengelolaan informasi yang menyatakan tanggung jawab terhadap Keamanan Informasi dan sanksi atas pelanggaran Keamanan Informasi;

e. menghentikan hak penggunaan aset informasi bagi pegawai yang sedang dalam pemeriksaan terkait dengan dugaan pelanggaran Keamanan Informasi;

f. mencabut hak akses ke aset informasi yang dimiliki pegawai dan Pihak Ketiga apabila yang bersangkutan tidak lagi memiliki kepentingan terhadap aset informasi, dimutasi, atau tidak lagi bekerja di Pemerintah Daerah;

g. membuat berita acara serah terima terkait penerimaan seluruh aset informasi yang dipergunakan selama bekerja dan pengembalian seluruh aset informasi bagi pegawai yang berhenti bekerja atau mutasi;

h. memberikan edukasi kesadaran Keamanan Informasi melalui kegiatan sosialisasi, bimbingan teknis, dan/atau pelatihan mengenai Keamanan Informasi yang dilaksanakan secara berkala;

i. memelihara catatan pelatihan, kompetensi, pengalaman, dan kualifikasi pegawai yang mengelola Keamanan Informasi; dan

j. mengumpulkan dan menganalisis informasi yang berkaitan dengan ancaman Keamanan Informasi untuk menghasilkan intelijen ancaman, sehingga dapat diambil tindakan untuk mencegah ancaman serta mengurangi dampak ancaman.

Paragraf 2

Keamanan Aset Informasi

Pasal 13

(1) Keamanan aset informasi dilakukan untuk mengamankan aset informasi di Pemerintah Daerah berdasarkan tingkat kritikalitasnya.

(2) Aset Informasi sebagaimana dimaksud pada ayat (1) merupakan aset dalam bentuk:

a. fisik atau non elektronik, meliputi informasi yang tercetak, tertulis dan tersimpan dalam bentuk fisik seperti di atas kertas, papan tulis, spanduk, atau di dalam buku dan dokumen; dan

b. elektronik, meliputi informasi tercetak, tertulis dan tersimpan dalam bentuk elektronik seperti *database*, pada *file* di dalam komputer, ditampilkan pada *website*, layar komputer dan dikirimkan melalui jaringan telekomunikasi.

(3) Keamanan aset informasi dilakukan oleh Tim SMKI, dengan cara sebagai berikut:

a. mengidentifikasi aset informasi dan mendokumentasikannya dalam daftar inventaris aset informasi yang memuat tingkat kritikalitas dan penanggung jawab setiap aset;

b. memberikan label sesuai tingkat kritikalitas;

c. menetapkan pihak-pihak yang dapat mengakses aset informasi;

d. menetapkan aturan penggunaan aset informasi;

e. menetapkan mekanisme pengamanan dalam pengiriman aset informasi perangkat dan dokumen yang melibatkan pihak ketiga;

f. menempatkan aset informasi di lokasi yang aman guna mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang;

g. memberikan persetujuan terhadap penggunaan aset yang dibawa ke luar dari lingkungan Pusat Data atau tempat layanan informasi;

h. memberikan persetujuan terhadap penggunaan aset yang dibawa keluar dari lingkungan Pusat Data suatu Perangkat Daerah atau tempat pelayanan informasi;

i. melakukan sanitasi terhadap perangkat penyimpanan data yang sudah tidak digunakan lagi sebelum digunakan kembali atau dimusnahkan;

j. melaksanakan pemusnahan perangkat penyimpanan yang dilakukan secara aman sesuai Prosedur Pemusnahan Perangkat Penyimpanan;

k. mengelola peralatan mekanik (non eletronik) yang di gerakan tangan secara manual dengan media penyimpanan terdiri lemari, rak, laci, *filing cabinet*, dan perangkat non-elektronik sejenis lainnya;

l. mengelola peralatan elektronik yang bekerja secara elektronik penuh dengan menggunakan media penyimpanan *server*, *hard disk*, *flash disk*, kartu memori, dan perangkat elektronik sejenis lainnya;

m. melaksanakan pencegahan kebocoran data untuk sistem, jaringan dan peranti yang memproses, menyimpan, atau mentransmisikan informasi sensitif melalui:

   1. identifikasi dan mengklasifikasikan informasi untuk melindungi kebocoran;

   2. pengawasan saluran terjadinya kebocoran data; dan

   3. pencegahan informasi bocor melalui proses karantina alamat link yang berisi informasi sensitif.

n. mengatur akses ke situs *web* eksternal untuk mengurangi tampilan dari konten berbahaya; dan

o. melaksanakan manajemen aset TIK sesuai dengan ketentuan manajemen aset TIK yang ditetapkan oleh Kementerian yang melaksanakan tugas pemerintahan di bidang Komunikasi dan Informatika.

Paragraf 3

Keamanan Akses

Pasal 14

(1) Keamanan akses dilakukan untuk mengendalikan akses ke aset informasi yaitu memastikan perangkat pengguna yang terhubung ke aset informasi mendapatkan perlindungan keamanan dan tidak diakses oleh pihak yang tidak berhak.

(2) Keamanan akses terhadap aset informasi di Pemerintah Daerah dilakukan oleh Tim SMKI, dengan cara sebagai berikut:

a. menyusun prosedur pengelolaan hak akses pengguna yang berisi ketentuan akses ke aset informasi sesuai dengan kebutuhan Pemerintah Daerah dan Perangkat Daerah, persyaratan keamanan, dan peraturan perundang-undangan;

b. mengelola akses pengguna;

c. mengendalikan akses ke jaringan dan layanan jaringan informasi;

d. mengendalikan akses ke aplikasi dan sistem informasi;

e. mengendalikan perangkat kerja jarak jauh;

f. mengendalikan hak akses khusus diperlukan untuk mengakses sistem informasi berklasifikasi rahasia pada sistem operasi, perangkat penyimpanan, *file server*, dan aplikasi sensitif;

g. memantau akses ke aset informasi;

h. menghapus akun untuk setiap pegawai dan Pihak Ketiga yang tidak lagi memiliki kepentingan terhadap akses aset informasi, dimutasi, berhenti, atau telah berakhir kontraknya.

i. menyamarkan data untuk membatasi pemaparan data sensitif, serta untuk memenuhi persyaratan peraturan hukum, regulator dan kontraktual dengan menggunkan teknik penyamaran data, pseudonimisasi atau anonimisasi, yang dilakukan dengan cara:

1. enkripsi;

2. membatalkan atau menghapus karakter;

3. meragamkan angka dan tanggal; dan

4. substitusi.

(3) Pengelolaan akses pengguna sebagaimana dimaksud pada ayat (2) huruf b dilakukan dengan cara:

a. menggunakan akun yang unik untuk setiap pengguna;

b. memeriksa tingkat akses yang diberikan sesuai dengan tujuan penggunaan;

c. membatasi dan mengendalikan penggunaan hak akses;

d. mengatur pengelolaan kata sandi pengguna sesuai dengan ketentuan pengelolaan kata sandi di Pemerintah Daerah;

e. melaksanakan pemantauan dan evaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya;

f. memelihara catatan pengguna layanan;

g. melaksanakan penonaktifan akses pengguna yang telah berakhir penugasannya; dan

h. melaksanakan pemantauan dan evaluasi akun dan hak akses secara berkala paling sedikit 1 (satu) kali dalam 6 (enam) bulan.

(4) Pengendalian akses ke jaringan dan layanan jaringan informasi sebagaimana dimaksud pada ayat (2) huruf c dilakukan dengan cara:

a. menerapkan prosedur otorisasi pemberian akses ke jaringan dan layanan jaringan untuk setiap akses ke dalam jaringan internal;

b. mengawasi akses ke infrastruktur dan aplikasi yang digunakan untuk melakukan pemeriksaan dan hanya digunakan untuk pegawai yang bertugas untuk melakukan pengujian, pemecahan masalah, serta pengembangan sistem;

c. memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi;

d. memberikan akses jaringan kepada tamu hanya untuk akses terbatas dan waktu tertentu; dan

e. menghentikan layanan jaringan pada area jaringan yang mengalami gangguan Keamanan Informasi.

(5) Pengendalian akses ke aplikasi dan sistem informasi sebagaimana dimaksud pada ayat (2) huruf d dilakukan dengan ketentuan sebagai berikut;

a. akses terhadap aplikasi dan sistem informasi hanya diberikan kepada pengguna sesuai dengan peruntukannya dan dikontrol dengan menggunakan sistem manajemen akses pengguna;

b. setiap pengguna wajib memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya dan proses otorisasi pengguna wajib menggunakan teknik otentikasi yang sesuai untuk memvalidasi identitas pengguna;

c. menggunakan sistem pengelolaan kata sandi sesuai dengan ketentuan pengelolaan kata sandi di Pemerintah Daerah untuk memastikan kualitas kata sandi yang dibuat pengguna;

d. fasilitas *session time-out* wajib diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu;

e. membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia;

f. akses ke kode sumber aplikasi dibatasi secara ketat diperuntukkan hanya bagi pihak-pihak yang sah dan berkepentingan melalui hak akses khusus; dan

g. prinsip pengkodean yang aman sebaiknya diterapkan pada pengembangan perangkat lunak.

(6) pengendalian perangkat kerja jarak jauh sebagaimana dimaksud pada ayat (2) huruf e dilakukan dengan cara menentukan parameter-parameter keamanan yang harus dipenuhi oleh perangkat kerja jarak jauh yang digunakan dalam mengakses aset informasi, yang terdiri atas:

a. *Virtual Private Network*;

b. *Secure Socket Layer*; dan/atau

c. *Two Step Authentication*;

(7) Pemberian hak akses khusus sebagaimana dimaksud pada ayat (2) huruf f dilakukan dengan cara:

a. mengidentifikasi hak akses khusus untuk dialokasikan kepada pengguna terkait;

b. memberikan hak akses khusus hanya kepada pengguna sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu;

c. mengelola proses otorisasi dan catatan dari seluruh hak akses khusus; dan

d. memberikan hak akses khusus secara terpisah dari akun yang digunakan untuk kegiatan lainnya.

(8) Pemantauan terhadap akses ke aset informasi sebagaimana dimaksud pada ayat (2) huruf g meliputi:

a. kegagalan akses;

b. penggunaan hak akses tidak wajar;

c. alokasi dan penggunaan hak akses khusus;

d. penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan

e. penggunaan sumber daya sensitif.

Paragraf 4

Keamanan Kriptografi

Pasal 15

(1) Keamanan kriptografi untuk memastikan penggunaan kriptografi yang tepat untuk melindungi kerahasiaan, keutuhan, dan keotentikan data dan informasi rahasia dan/atau sangat rahasia yang dikelola dalam perangkat informasi.

(2) Keamanan kriptografi untuk informasi rahasia dan/atau sangat rahasia dilaksanakan oleh Tim SMKI, dengan cara sebagai berikut:

a. melakukan klasifikasi informasi yang disimpan dan dikelola dalam perangkat informasi sesuai dengan ketentuan peraturan perundang-undangan; dan

b. menerapkan keamanan kriptografi untuk informasi berklasifikasi rahasia dan/atau sangat rahasia.

(3) Penerapan keamanan kriptografi sebagaimana dimaksud pada ayat (2) huruf b dilaksanakan dengan cara berikut:

a. menerapkan jalur komunikasi aman dengan menerapkan *Secure Socket Layer* untuk proses otentikasi antara pengguna dengan aplikasi berbasis website;

b. menjaga kerahasiaan kata sandi dan menyimpannya dalam basis data dengan mekanisme *hash function*;

c. melindungi kerahasiaan data dan informasi rahasia dan/atau sangat rahasia yang dipertukarkirimkan dan disimpan dalam basis data dengan melakukan enkripsi;

d. menerapkan otentikasi berbasis tanda tangan digital dengan menggunakan sertifikat elektronik yang dikeluarkan oleh badan/Pihak Ketiga yang tersertifikasi; dan

e. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan dan/atau rekomendasi dari badan yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

Paragraf 5

Keamanan Fisik dan Lingkungan

Pasal 16

(1) Keamanan fisik dan lingkungan dilakukan untuk memberikan pelindungan, pemeliharaan, keamanan, dan ketersediaan aset informasi.

(2) Keamanan fisik dan lingkungan dilaksanakan oleh Tim SMKI, dengan cara sebagai berikut:

a. menyimpan infrastruktur di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai;

b. membatasi akses ke Pusat Data dan/atau area kerja layanan informasi yang berisi data dan/atau informasi rahasia dan/atau sangat rahasia dan hanya diberikan kepada pegawai yang memiliki akses;

c. mendampingi Pihak Ketiga yang memasuki Pusat Data dan/atau area kerja layanan informasi yang berisikan data dan/atau informasi rahasia dan/atau sangat rahasia;

d. melarang membawa makanan dan minuman untuk masuk ke atau dikonsumsi di dalam ruang *server* Pusat Data;

e. memastikan area bebas rokok untuk semua area yang digunakan untuk menyimpan aset informasi;

f. mengawasi kondisi batas minimum dan maksimum suhu dan kelembaban di dalam ruang *server* Pusat Data untuk memenuhi standar yang disyaratkan pabrikan perangkat dan senantiasa dilakukan;

g. mengamankan area Pusat Data dan area kerja layanan informasi sesuai prosedur keamanan area;

h. mengamankan kantor, ruangan, dan fasilitas kerja sesuai dengan peraturan dan standar keamanan dan keselamatan kerja, termasuk *clear screen policy* dan *clean desk policy*;

i. memelihara infrastruktur yang digunakan untuk menjalankan aplikasi sesuai dengan buku petunjuk;

j. memindahkan infrastruktur pada saat pemeliharaan yang tidak dapat dilakukan di tempat dan dilakukan berdasarkan persetujuan Kepala Perangkat Daerah yang melaksanakan urusan pemerintahan bidang komunikasi dan informatika;

k. memindahkan terlebih dahulu ke dalam media penyimpanan lain untuk pemindahan infrastruktur yang terdapat data dan/atau informasi berklasifikasi rahasia dan/atau sangat rahasia yang tersimpan pada perangkat penyimpanannya, data dan/atau informasi berklasifikasi rahasia dan/atau sangat rahasia;

l. membuat perjanjian kerja sama, paling sedikit memuat perjanjian menjaga kerahasiaan, pemeliharaan yang disediakan, dan tingkat kinerja yang harus dipenuhi Pihak Ketiga.

m. memastikan infrastruktur beserta perangkat pemulihan dan media penyimpanan data cadangan wajib diletakkan di tempat yang aman dengan struktur yang memadai untuk menghindari kerusakan dari hama atau gangguan file dan bencana;

n. memastikan semua infrastruktur mendapatkan pasokan daya yang sesuai dengan spesifikasi yang diisyaratkan oleh pabrikan infrastruktur;

o. memastikan pasokan listrik yang digunakan untuk mengoperasikan infrastruktur harus mempunyai sumber alternatif dengan daya dan jangka waktu ketersediaan atau jangka waktu pengoperasian yang cukup, yang paling sedikit mencakup generator listrik dan *Uniterruptable Power Supply* dengan daya yang cukup dan konfigurasi yang dapat memindahkan pasokan listrik tanpa gangguan terhadap infrastruktur;

p. menyimpan bahan berbahaya atau mudah terbakar di lingkungan Pusat Data pada jarak yang aman dari Pusat Data dan area kerja layanan informasi;

q. menyediakan, memelihara, dan meletakkan perangkat pemadam kebakaran di tempat yang mudah dijangkau;

r. meletakkan infrastruktur dan Pusat Data pada lokasi yang meminimalisasi akses pihak yang tidak berwenang;

s. memposisikan dan membatasi sudut pandang infrastruktur yang menangani informasi sensitif untuk mengurangi risiko informasi dilihat oleh pihak tidak berwenang;

t. menerapkan perlindungan petir untuk semua bangunan, jalur komunikasi dan listrik;

u. mengamankan kabel di Pusat Data dan/atau area kerja layanan informasi dengan mengikuti standar mekanikal/elektrikal Pusat Data yang berlaku; dan

v. memonitor keamanan fisik untuk mendeteksi dan mencegah akses fisik yang tidak diperbolehkan melalui sistem surveilans meliputi penjaga, alarm penyusup, monitoring video, serta perangkat lunak untuk keamanan fisik.

(3) Penyimpanan infrastruktur di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai sebagaimana dimaksud pada ayat (2) huruf a antara lain:

a. pintu dengan kontrol akses;

b. kamera pengawas;

c. pendeteksi asap;

d. sistem pemadam kebakaran; dan

e. perangkat pemutus aliran listrik.

Paragraf 6

Keamanan Operasional

Pasal 17

(1) Keamanan operasional dilakukan untuk memastikan implementasi, operasional, dan pemeliharaan yang aman dari aset informasi, pengelolaan layanan oleh Pihak Ketiga, meminimalkan risiko kegagalan, dan melindungi keutuhan dan ketersediaan aset informasi.

(2) Keamanan operasional di Pemerintah Daerah dilakukan oleh Tim SMKI bekerja sama dengan Perangkat Daerah yang melaksanakan urusan pemerintahan bidang komunikasi dan informatika, dengan cara sebagai berikut:

a. mendokumentasian, memeliharaan, dan menyediakan prosedur penggunaan perangkat informasi sesuai dengan peruntukannya;

b. mendokumentasikan dan mengendalikan perubahan pada aset informasi yang dapat mempengaruhi Keamanan Informasi dengan memperhatikan manajemen risiko dan persetujuan dari pemilik aset informasi;

c. menetapkan kriteria penerimaan untuk sistem informasi baru, pemutakhiran, dan versi baru serta melakukan pengujian sebelum penerimaan;

d. memantau penggunaan aset informasi yang dimiliki dan membuat proyeksi kebutuhan ke depan untuk menjamin ketersediaan aset informasi yang dibutuhkan dan untuk aset informasi yang kritikal serta senantiasa dimonitor dan dievaluasi kapasitas dan ketersediaannya;

e. memisahkan akses terhadap informasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia;

f. mencegah seorang pegawai memiliki akses terhadap seluruh aset informasi dan perangkat pengolahnya;

g. memisahkan lingkungan pengembangan, pengujian, dan operasional untuk mengurangi risiko perubahan atau akses oleh pihak yang tidak berhak terhadap sistem operasional;

h. menerapkan sistem pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman *malware*;

i. perlindungan dilakukan dengan cara pemasangan paling sedikit meliputi perangkat *firewall*, perangkat *Intrusion Prevention System*, *antivirus*, perangkat manajemen akses pengguna dan perangkat monitoring/pendukung lainnya sesuai perkembangan teknologi Keamanan Informasi;

j. membuat *backup* informasi dan aplikasi yang berada di Pusat Data dan/atau area kerja layanan informasi secara berkala sesuai dengan prosedur *backup* di Pemerintah Daerah;

k. salinan cadangan data/informasi, aplikasi, dan *image* sistem harus diambil dan diuji secara berkala dengan retensi penyalinan cadangan minimal 1 (satu) tahun dan penyalinan cadangan paling sedikit 4 (empat) kali dalam satu periode retensi;

l. mencatat setiap aktivitas administrator, aktivitas pengguna, peristiwa kegagalan, dan kejadian keamanan serta disimpan dalam periode tertentu;

m. melindungi sistem pencatatan dari pemalsuan dan akses yang tidak berwenang;

n. melakukan penilaian kerentanan terhadap perangkat informasi secara berkala dan melakukan tindakan perlindungan terhadap kerentanan dan/atau ancaman yang teridentifikasi;

o. menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindak pengamanan yang tepat;

p. memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan harus dipastikan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati; dan

q. menerapkan audit terhadap catatan yang mencatat aktivitas pengguna dan kejadian Keamanan Informasi dalam kurun waktu tertentu untuk membantu investigasi di masa mendatang.

(3) Penerapan audit terhadap catatan sebagaimana dimaksud dalam ayat (2) huruf q untuk melihat hal-hal antara lain:

a. kegagalan akses;

b. penggunaan hak akses tidak wajar;

c. alokasi dan penggunaan hak akses khusus;

d. penelusuran transaksi pengiriman *file* sistem atau dokumen tertentu yang mencurigakan; dan

e. penggunaan sumber daya sensitif.

Paragraf 7

Keamanan Komunikasi

Pasal 18

(1) Keamanan komunikasi dilakukan untuk memastikan keamanan pertukaran informasi melalui jaringan komunikasi.

(2) Keamanan komunikasi di Pemerintah Daerah dilakukan oleh Tim SMKI bekerja sama dengan Perangkat Daerah yang melaksanakan urusan pemerintahan bidang komunikasi dan informatika, sebagai berikut:

a. mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh Pihak Ketiga;

b. memberikan izin hak akses ke jaringan kepada Pihak Ketiga, maka dilakukan pemantauan serta pencatatan kegiatan selama menggunakan jaringan;

c. melindungi jaringan dari pihak yang tidak berhak mengakses;

d. menerapkan mekanisme kriptografi untuk melindungi informasi yang terdapat dalam aplikasi yang melewati jaringan publik dari upaya pengungkapan, modifikasi, dan perusakan;

e. mendeteksi dan melindungi terhadap ancaman kode berbahaya yang disisipkan pada file yang dikirim melalui sistem elektronik;

f. memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan untuk informasi elektronik berklasifikasi rahasia dan/atau sangat rahasia;

g. menetapkan prosedur pertukaran informasi yang mengatur sistem dan keamanan yang digunakan untuk pertukaran informasi;

h. menentukan dan mengatur keaamanan informasi untuk penggunaan *cloud;*

i. menghapus informasi yang disimpan dalam sistem informasi, peranti atau dimedia penyimpanan lainnya bila tidak lagi diperlukan; dan

j. memonitor jaringan, sistem, dan aplikasi untuk menemukan perilaku tidak normal dan mengambil tindakan yang tepat untuk mengevaluasi potensi insiden Keamanan Informasi.

(3) Perlindungan jaringan dari pihak yang tidak berhak mengakses sebagaimana dimaksud pada ayat (2) huruf c paling sedikit dilaksanakan dengan cara:

a. mendokumentasikan arsitektur jaringan yang meliputi seluruh komponen infrastruktur dan aplikasi jaringan;

b. menerapkan teknologi keamanan jaringan berbasis enkripsi dan otentikasi termasuk sertifikat elektronik;

c. menerapkan pemisahan jaringan untuk kelompok pengguna, layanan informasi, dan sistem informasi;

d. menerapkan parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan; dan

e. menerapkan prosedur penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau aplikasi.

(4) Penentuan dan pengaturan Keamanan Informasi untuk penggunaan *cloud* sebagaimana dimaksud pada ayat (2) huruf h paling sedikit dilaksanakan dengan cara:

a. menetapkan semua persyaratan Keamanan Informasi yang terkait dengan penggunaan layanan *cloud*;

b. menetapkan kriteria pemilihan layanan *cloud* dan ruang lingkup penggunaan layanan *cloud*;

c. menetapkan peran dan tanggung jawab penggunaan dan manajemen layanan *cloud*;

d. mendapatkan kontrol Keamanan Informasi yang diatur oleh penyedia layanan *cloud* dan diatur oleh Pemerintah Daerah sebagai pengguna layanan *cloud*;

e. mendapatkan dan memanfaatakan kapabilitas Keamanan Informasi yang disediakan oleh penyedia layanan *cloud;*

f. mendapatkan kontrol Keamanan Informasi yang diimplementasikan oleh penyedia layanan *cloud;*

g. menetapkan manajemen kontrol, antar muka, dan perubahan layanan pada saat Pemerintah Daerah menggunakan beberapa layanan *cloud*, khususnya dari penyedia layanan *cloud* yang berbeda;

h. menangani insiden Keamanan Informasi yang terjadi terakit penggunaan layanan *cloud;*

i. memonitor, mereviu dan mengevaluasi penggunaan layanan *cloud* yang sedang berlangsung untuk mengatur risiko Keamanan Informasi; dan

j. menetapkan prosedur untuk mengubah atau menghentikan penggunaan layanan *cloud* termasuk strategi keluar dari layanan *cloud.*

Paragraf 8

Keamanan Pengembangan dan Pemeliharaan

Pasal 19

(1) Keamanan pengembangan dan pemeliharaan sistem dilakukan untuk memastikan bahwa Keamanan Informasi merupakan bagian yang terintegrasi dalam daur hidup aset informasi untuk mencegah terjadinya kesalahan, eksploitasi, modifikasi, dan perusakan aset informasi oleh pihak yang tidak berwenang.

(2) Keamanan pengembangan dan pemeliharaan di Pemerintah Daerah dilakukan oleh Tim SMKI bekerja sama dengan Perangkat Daerah yang melaksanakan urusan pemerintahan bidang komunikasi dan informatika, dengan cara sebagai berikut:

a. memisahkan lingkungan pengembangan, pengujian, dan operasional aplikasi secara fisik, *logic*, dan aksesnya;

b. menjaga lingkungan pengembangan agar tidak diakses dari sistem operasional layanan;

c. mengupayakan lingkungan pengujian sama dengan lingkungan operasional layanan;

d. memilih data uji dengan hati-hati, melindungi, dan mengendalikannya;

e. mengawasi dan memantau aktivitas pembangunan/pengembangan aplikasi dan infrastruktur yang dialihdayakan pada Pihak Ketiga;

f. memastikan proses perencanaan dan pembangunan/pengembangan aplikasi dan infrastruktur termasuk yang dilakukan oleh Pihak Ketiga, telah memasukkan fitur-fitur keamanan dalam spesifikasi aplikasi dan infrastruktur yang dibangun/dikembangkan;

g. memastikan fitur-fitur keamanan yang dimasukkan sebagaimana yang dimaksud pada ayat (2) huruf f harus sesuai dengan standar keamanan relevan;

h. melaksanakan uji kelaikan aplikasi sebelum aplikasi digunakan dan sewaktu-waktu sesuai kebutuhan; dan

i. menetapkan, mendokumentasikan, mengimplementasikan, memonitor serta mengevaluasi pengaturan keamanan, perangkat keras, perangkat lunak, layanan dan jaringan.

(3) Fitur-fitur keamanan yang sesuai dengan standar keamanan relevan sebagaimana yang dimaksud pada ayat (2) huruf g mencakup :

a. standar keamanan data dan informasi;

b. standar keamanan aplikasi;

c. standar keamanan pusat data;

d. standar keamanan sistem penghubung layanan; dan

e. standar keamanan jaringan intra.

(4) Standar keamanan relevan sebagaimana dimaksud pada ayat (3) minimal memenuhi standar yang ditetapkan oleh badan yang melaksanakan tugas pemerintahan dibidang keamanan siber.

(5) Pelaksanaan uji kelaikan aplikasi sebelum aplikasi digunakan dan sewaktu-waktu sesuai kebutuhan sebagaimana dimaksud pada ayat (2) huruf h mencakup aspek:

a. uji fungsi, dilakukan untuk memastikan aplikasi yang dibangun dan/atau dikembangkan telah memenuhi fungsi-fungsi sesuai dengan dokumentasi terkait;

b. uji integrasi, dilakukan untuk yang memastikan aplikasi yang dibangun dan/atau dikembangkan telah memenuhi kebutuhan dan persyaratan integrasi dengan aplikasi, data, serta komponen-komponen lain yang terkait;

c. uji beban, dilakukan untuk yang memastikan aplikasi yang dibangun dan/atau dikembangkan dapat berfungsi sebagaimana mestinya menghadapi beban kerja yang dikenakan terhadapnya;

d. uji keamanan, dilakukan untuk memastikan aplikasi yang dibangun dan/atau dikembangkan dapat menjaga keamanan data dan informasi yang terkait dengannya.

(6) Uji kelaikan pada aspek uji fungsi, uji integrasi, dan uji beban sebagai mana dimaksud pada ayat (5) huruf a, huruf b dan huruf c dapat menggunakan pedoman dan/atau instrumen pengukuran yang ditetapkan oleh Kementerian yang menyelenggarakan tugas pemerintahan di bidang komunikasi dan informatika.

(7) Uji kelaikan pada aspek uji keamanan sebagai mana dimaksud pada ayat (5) huruf d dapat menggunakan pedoman/instrumen pengukuran yang ditetapkan oleh Badan yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

(8) Pelaksanaan pembangunan dan pengembangan aplikasi dilakukan sesuai dengan Standar Teknis dan Prosedur Pembangunan dan Pengembangan Aplikasi yang ditetapkan oleh Kementerian yang melaksanakan tugas pemerintahan di bidang Komunikasi dan Informatika.

Paragraf 9

Keamanan Pihak Ketiga

Pasal 20

(1) Keamanan Pihak Ketiga dilakukan untuk memastikan perlindungan dari aset informasi yang dapat diakses oleh Pihak Ketiga.

(2) Keamanan Pihak Ketiga di Pemerintah Daerah dilakukan oleh tim SMKI bekerja sama dengan Perangkat Daerah yang melaksanakan urusan pemerintahan bidang komunikasi dan informatika, dengan cara sebagai berikut:

a. memeriksa latar belakang Pihak Ketiga dengan tetap memperhatikan privasi dan perlindungan data pribadi;

b. membuat dan meninjau ulang secara berkala perjanjian keamanan dengan Pihak Ketiga yang terlibat dalam penggunaan dan/atau pengelolaan aset informasi yang menyatakan tanggung jawab terhadap keamanan aset informasi.

c. mengendalikan Keamanan Informasi, definisi layanan, dan tingkat layanan yang termuat dalam kesepakatan penyediaan layanan, telah diterapkan, dioperasikan, dan dipelihara oleh Pihak Ketiga harus dipastikan secara berkala;

d. memastikan *Service Level Agreement* Pihak Ketiga telah mengatur ketersediaan layanan dan penyelesaian insiden keamanan;

e. memantau kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh Pihak Ketiga dilakukan secara berkala;

f. menentukan kritikalitas proses yang terkait layanan yang disediakan oleh Pihak Ketiga dan menilai ulang risiko apabila terjadi perubahan;

g. mencatat peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan oleh Pihak Ketiga;

h. memberikan informasi tentang gangguan keamanan dan mengkaji informasi bersama Pihak Ketiga;

i. mencabut hak akses terhadap akses informasi yang dimiliki Pihak Ketiga apabila yang bersangkutan tidak lagi bekerja di Pemerintah Daerah

j. membuat berita acara serah terima terkait mengembalikan seluruh aset informasi yang dipergunakan selama bekerja bagi Pihak Ketiga yang berakhir masa kontraknya; dan

k. memastikan Pihak Ketiga dan tamu yang memasuki lingkungan Pusat Data, dan tempat layanan informasi untuk mematuhi standar keamanan fisik dan lingkungan.

(3) Perjanjian keamanan sebagaimana dimaksud pada ayat (2) huruf b disusun secara tertulis dengan paling sedikit memuat:

a. perlindungan atas informasi rahasia dan/atau sangat rahasia dan hak kekayaan intelektual setiap pihak;

b. aset informasi disediakan oleh Pihak Ketiga, harus ada jaminan tidak terdapat *malicious code* dan *backdoor*;

c. hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia dan/atau sangat rahasia;

d. pengawasan atas akses terhadap aset informasi yang diberikan pada Pihak Ketiga;

e. pelaporan terhadap penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan;

f. syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian;

g. penggunaan jalur komunikasi yang aman untuk perpindahan informasi antara Pemerintah Daerah dengan Pihak Ketiga; dan

h. Pihak Ketiga yang tidak lagi menjadi bagian dalam pengelolaan aset informasi, maka aset informasi yang dikuasainya harus diserahkan kembali kepada Tim SMKI.

Paragraf 10

Manajemen Insiden Siber

Pasal 21

(1) Manajemen insiden siber dilaksanakan untuk mengendalikan insiden siber.

(2) Manajemen insiden siber dilakukan oleh Tim SMKI, bekerja sama dengan Perangkat Daerah di lingkungan Pemerintah Daerah dan Badan yang melaksanakan urusan pemerintah bidang keamanan siber sebagai berikut:

a. membentuk TTIS yang bertugas melakukan pencegahan dan penanganan insiden siber yang terjadi di Pemerintah Daerah oleh Bupati;

b. melakukan tindakan pencegahan insiden siber;

c. melaksanakan Prosedur Penanganan Insiden Siber jika terjadi insiden siber;

d. menyusun berbagai macam skenario penanganan insiden siber;

e. melakukan simulasi skenario penanganan insiden siber secara berkala;

f. memberikan pelatihan untuk sumber daya manusia yang terlibat pada penanganan insiden siber sesuai skenario yang disusun;

g. menjalankan program kesadaran ancaman dan penanganan insiden siber, serta ajakan peran aktif pada seluruh pegawai;

h. memastikan ketersediaan kontak pelaporan insiden siber yang dapat diakses oleh seluruh pegawai di Pemerintah Daerah termasuk oleh Pihak Ketiga; dan

i. mengukur secara berkala tingkat kematangan penanganan insiden siber.

(3) Tindakan pencegahan insiden siber sebagaimana dimaksud pada ayat (2) huruf b paling sedikit meliputi :

a. melakukan penilaian kerentanan dan/atau *penetration testing* untuk menemukan celah keamanan pada aset informasi;

b. mengimplementasikan alat monitoring keamanan berupa *Security Information and Event Management*; dan

c. melakukan monitoring dan pendeteksian serangan terhadap aset informasi.

(4) Prosedur penanganan insiden sebagaimana dimaksud pada ayat (2) huruf c meliputi:

a. menerima laporan dan mencatat insiden siber;

b. melakukan pemilahan insiden siber;

c. mengidentifikasi sumber serangan;

d. menganalisis informasi yang berkaitan dengan insiden siber;

e. memprioritaskan penanganan insiden berdasarkan tingkat dampak;

f. memelihara artefak digital untuk keperluan investigasi;

g. menyusun laporan penanganan insiden siber; dan

h. mengevaluasi dan memperbaiki standar, prosedur, dan kontrol-kontrol Keamanan Informasi agar insiden siber serupa tidak terulang kembali di masa mendatang.

Paragraf 11

Manajemen Keberlangsungan Layanan Informasi

Pasal 22

(1) Manajemen keberlangsungan layanan informasi dilakukan untuk menjamin ketersediaan layanan informasi pada saat terjadi keadaan darurat.

(2) Manajemen keberlangsungan layanan informasi dilakukan oleh tim SMKI bekerja sama dengan Perangkat Daerah yang melaksanakan urusan pemerintahan bidang komunikasi dan informatika, dengan cara sebagai berikut:

a. melakukan identifikasi risiko terhadap keberlangsungan layanan informasi;

b. menyusun dan menerapkan rencana keberlangsungan proses bisnis untuk menjaga dan mengembalikan operasional aset informasi dalam jangka waktu yang disepakati dan tingkat keberlangsungan yang dibutuhkan;

c. memastikan redudansi yang cukup diperlukan untuk memenuhi ketersediaan layanan informasi jika sistem elektronik merupakan aplikasi umum dan/atau sistem elektronik berkategori strategis;

d. melakukan uji coba rencana keberlangsungan layanan informasi secara berkala;

e. merencanakan, mengimplementasikan, memelihara dan menguji kesiapan TIK berdasarkan sasaran kontinuitas bisnis dan persyaratan kontinuitas TIK; dan

f. melaksanakan pengelolaan layanan sesuai dengan pedoman manajemen layanan SPBE yang ditetapkan oleh Kementerian yang melaksanakan tugas pemerintahan di bidang Komunikasi dan Informatika.

(3) Rencana keberlangsungan proses bisnis sebagaimana dimaksud pada ayat (2) huruf b paling sedikit terdiri atas:

a. Prosedur Keberlangsungan Layanan informasi pada saat keadaan darurat, manajemen risiko, analisis dampak kegiatan, pengembalian kondisi sebelum terjadi gangguan peralihan kondisi normal, dan uji coba keberlangsungan kegiatan;

b. menetapkan peran dan penanggung jawab pegawai yang terlibat dalam pelaksanaan keberlangsungan layanan informasi;

c. melaksanakan sosialisasi dan pelatihan keberlangsungan layanan informasi.

Paragraf 12

Pengendalian Kepatuhan

Pasal 23

(1) Pengendalian kepatuhan dilaksanakan untuk memastikan kepatuhan pegawai dan Pihak Ketiga dalam melaksanakan Keamanan Informasi sesuai dengan ketentuan peraturan perundang-undangan, kontrak dan keselarasan dengan kebijakan Keamanan Informasi yang berlaku di Pemerintah Daerah.

(2) Pengendalian kepatuhan Keamanan Informasi di Pemerintah Daerah, dilakukan oleh Tim SMKI bekerja sama dengan Perangkat Daerah yang melaksanakan urusan pemerintahan bidang komunikasi dan informatika dan Perangkat Daerah lainnya sebagai berikut namun tidak terbatas pada:

a. mengidentifikasikan, mendokumentasikan, mengevaluasi, dan memelihara regulasi, standar, dan prosedur Keamanan Informasi;

b. memeriksa kepatuhan seluruh pegawai dan Pihak Ketiga terhadap regulasi, standar, dan prosedur Keamanan Informasi;

c. memastikan tidak ada pelanggaran hak cipta dengan menjamin aplikasi yang didapat hanya melalui sumber yang dikenal dan memiliki reputasi baik;

d. memeriksa kepatuhan penggunaan lisensi aplikasi dan penerapan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;

e. memelihara bukti kepemilikan lisensi, *master disk*, buku manual, dan lain sebagainya;

f. menjamin tidak ada produk bajakan yang terinstal (pelanggaran hak kekayaan intelektual) di Pemerintah Daerah;

g. menjamin rekaman terlindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah, dan rilis tidak sah sesuai dengan persyaratan peraturan perundang-undangan, kontraktual, dan bisnis harus dipastikan;

h. mengamankan privasi dan data pribadi yang dapat diidentifikasikan sesuai dengan persyaratan peraturan perundang-undangan yang berlaku harus dipastikan;

i. memastikan kesesuaian penerapan kriptografi dengan peraturan perundang-undangan yang berlaku;

j. melakukan riviu secara berkala agar sistem informasi harus sesuai dengan kebijakan dan standar Keamanan Informasi di Pemerintah Daerah.

Bagian Keenam

Audit Keamanan Informasi

Pasal 24

(1) Audit Keamanan Informasi dilaksanakan secara berkala untuk memastikan diterapkannya kebijakan, standar, dan prosedur Keamanan Informasi.

(2) Audit Keamanan Informasi dilaksanakan melalui kegiatan Audit Internal Keamanan Informasi dan Audit Eksternal Keamanan Informasi.

(3) Audit internal Keamanan Informasi sebagaimana dimaksud pada ayat (2) dilaksanakan dengan cara sebagai berikut:

a. menyelenggarakan audit internal Keamanan Informasi di Pemerintah Daerah adalah kewajiban Perangkat Daerah yang menjalankan fungsi pengawasan;

b. merencanakan, menetapkan, dan menjalankan program audit sesuai dengan pedoman Audit Internal Keamanan Informasi dilaksanakan oleh Perangkat Daerah yang melaksanakan urusan pemerintahan di bidang pengawasan internal;

c. menetapkan program audit yang memuat frekuensi, metode, kriteria, lingkup, tanggung jawab, dan mekanisme pelaporan, dengan memperhatikan pentingnya proses berjalan serta temuan audit sebelumnya;

d. melakukan Audit Internal Keamanan Informasi paling sedikit 1 (satu) kali dalam 1 (satu) tahun serta mencantumkannya dalam Peta Rencana SPBE Pemerintah Daerah;

e. melaksanakan Audit Internal Keamanan Informasi oleh auditor yang memiliki kompetensi memadai serta menjunjung tinggi objektivitas dan imparsialitas dalam pelaksanaan audit;

f. mencatat setiap temuan audit secara formal oleh Auditor dan diberikan kepada auditan;

g. melaksanakan perbaikan oleh Auditan terhadap setiap temuan yang diberikan oleh Auditor dalam jangka waktu yang disepakat;

h. melaporkan Hasil Audit Keamanan Informasi kepada Tim SMKI dan Sekretaris Daerah sebagai bahan evaluasi penerapan Kebijakan SMKI;

i. menyimpan dan mendokumentasikan proses dan hasil audit internal sebagai alat bukti dari program audit; dan

j. melaksanakan Audit Internal Keamanan Informasi dapat menggunakan instrumen penilaian Audit Keamanan SPBE yang ditetapkan oleh Kepala Badan yang melaksanakan tugas pemerintahan di bidang keamanan siber.

(4) Audit Eksternal Keamanan Informasi sebagaimana dimaksud pada ayat (2) dilaksanakan oleh badan yang melaksanakan tugas pemerintahan di bidang keamanan siber dan Pihak Ketiga yang terakreditasi sebagai lembaga audit teknologi informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Ketujuh

Evaluasi Kinerja dan Perbaikan Berkelanjutan
Keamanan Informasi

Pasal 25

(1) Evaluasi kinerja Keamanan Informasi dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun dalam bentuk tinjauan manajemen untuk memastikan pencapaian target Keamanan Informasi yang telah direncanakan.

(2) Sekretaris Daerah dengan dibantu Tim SMKI melakukan evaluasi kinerja Keamanan Informasi berdasarkan peta rencana, sasaran Keamanan Informasi, dan hasil audit Keamanan Informasi dengan cara sebagai berikut:

a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan Informasi;

b. menetapkan indikator kinerja pada setiap area proses;

c. memformulasi pelaksanaan Keamanan Informasi dengan mengukur secara kuantitatif kinerja yang diharapkan;

d. melakukan evaluasi terhadap penyelenggaraan atau pelaksanaan SMKI;

e. menganalisis efektifitas pelaksanaan Keamanan Informasi; dan

f. mendukung dan merealisasikan program Audit Keamanan Informasi.

(3) Hasil evaluasi kinerja keamanan informasi didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja Keamanan Informasi berikutnya.

Pasal 26

(1) Perbaikan berkelanjutan merupakan tindak lanjut dari hasil evaluasi kinerja Keamanan Informasi.

(2) Tim SMKI melakukan perbaikan berkelanjutan dengan cara sekurang-kurangnya sebagai berikut:

a. mengatasi permasalahan dalam pelaksanaan Keamanan Informasi; dan

b. memperbaiki pelaksanaan Keamanan Informasi secara berkala.

(3) Tindakan perbaikan yang telah dilakukan didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja Keamanan Informasi.

BAB III

PEMBIAYAAN

Pasal 27

Pembiayaan pelaksanaan SMKI yang diatur dalam Peraturan Bupati ini dapat bersumber dari:

a. anggaran pendapatan dan belanja daerah; dan

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

BAB IV

KETENTUAN PENUTUP

Pasal 28

Pada saat Peraturan Bupati ini mulai berlaku Peraturan Bupati Nomor 147 Tahun 2023 tentang Manajemen Kemanan Informasi Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Garut Tahun 2023 Nomor 147) dicabut dan dinyatakan tidak berlaku.

Pasal 29

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 17 Oktober 2025

BUPATI GARUT,

t t d

ABDUSY SYAKUR AMIN

Diundangkan di Garut
pada tanggal 17 Oktober 2025

SEKRETARIS DAERAH KABUPATEN GARUT,

t t d

NURDIN YANA

BERITA DAERAH KABUPATEN GARUT
TAHUN 2025 NOMOR 52

Mengetahui
Sesuai Dengan Aslinya
a.n. SEKRETARIS DAERAH,
ASISTEN PEMERINTAHAN DAN KESRA
u.b
KEPALA BAGIAN HUKUM

IDA NURFARIDA, SH.
NIP. 19780915 200212 2 004