SALINAN

BUPATI BANTUL

DAERAH ISTIMEWA YOGYAKARTA

PERATURAN BUPATI BANTUL

NOMOR 35 TAHUN 2023

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI BANTUL,

Menimbang :

a. bahwa dalam rangka melindungi kerahasiaan, keutuhan dan ketersediaan aset informasi di lingkungan Pemerintah Daerah dari berbagai ancaman keamanan informasi baik dari dalam maupun luar, perlu melakukan pengelolaan keamanan informasi;

b. bahwa dalam rangka mengoptimalkan penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Bantul sehingga dapat mendukung terwujudnya tata kelola pemerintahan yang baik dan bersih, perlu adanya pelaksanaan dan pengelolaan Sistem Manajemen Keamanan Informasi Pemerintah Daerah;

c. bahwa untuk menjamin kepastian hukum dalam pelaksanaan dan pengelolaan Sistem Manajemen Keamanan Informasi Pemerintah Daerah, perlu adanya pedoman yang diatur dalam Peraturan Bupati;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Bupati tentang Sistem Manajemen Keamanan Informasi;

Mengingat :

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

2. Undang-Undang Nomor 15 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten Dalam Lingkungan Daerah Istimewa Yogyakarta (Berita Negara Republik Indonesia tanggal 8 Agustus 1950 Nomor 44);

3. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
4. Peraturan Pemerintah Nomor 32 Tahun 1950 tentang Penetapan Mulai Berlakunja Undang-Undang Tahun 1950 Nomor 12, 13, 14 dan 15 dari Hal Pembentukan Daerah-Daerah Kabupaten di Djawa Timoer/Tengah/Barat dan Daerah Istimewa Jogjakarta (Berita Negara Republik Indonesia Tahun 1950 Nomor 59);

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. 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.
2. 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.

3. Sistem Informasi adalah rangkaian kegiatan yang meliputi penyimpanan dan pengelolaan informasi serta mekanisme penyampaian informasi dari penyelenggara kepada masyarakat dan sebaliknya dalam bentuk lisan, tulisan latin, tulisan dalam huruf braille, bahasa gambar, dan/atau bahasa lokal, serta disajikan secara manual ataupun elektronik.
4. Aplikasi Sistem Informasi adalah sebuah program komputer atau perangkat lunak yang didesain untuk mengerjakan tugas tertentu terkait dengan proses penyimpanan, pengelolaan dan penyampaian data atau informasi tertentu.
5. Pengguna adalah orang atau masyarakat yang menggunakan Sistem Informasi dalam layanan penyelenggaraan pemerintahan.
6. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis dan/ atau menyebarkan informasi.
7. Aset Informasi adalah unit informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.
8. Aset Pengolahan Informasi adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting informasi.
9. Informasi rahasia adalah informasi yang sangat peka dan beresiko tinggi, yang pembocoran atau penyalahgunaan akses terhadapnya dapat mengganggu kelancaran operasional secara temporer atau mengganggu citra dan reputasi instansi.
10. *Disaster Recovery Center* adalah perencanaan kontingensi dalam menghadapi situasi bencana dan kejadian luar biasa lainnya, dengan penempatan perangkat teknologi informasi, sistem, aplikasi dan data-data cadangan pada suatu tempat atau lokasi yang terpisah dari data center utama.
11. Insiden Keamanan Informasi adalah suatu kejadian tunggal atau serangkaian kejadian keamanan informasi yang tidak diduga atau tidak dikehendaki yang mempunyai kemungkinan besar mengganggu keberlangsungan bisnis dan mengancam keamanan informasi.
12. Risiko adalah kejadian atau kondisi yang tidak diinginkan yang dapat menimbulkan dampak negatif terhadap pencapaian sasaran kinerja dari layanan sistem elektronik.
13. Daerah adalah Kabupaten Bantul

14. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan Daerah otonom.
15. Bupati adalah Bupati Bantul.
16. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah Kabupaten Bantul dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah
17. Dinas Komunikasi dan Informatika yang selanjutnya disebut Dinas adalah Dinas Komunikasi dan lnformatika Kabupaten Bantul.

Pasal 2

(1) Peraturan Bupati ini dimaksudkan sebagai pedoman pengelolaan SMKI.
(2) Pengaturan SMKI bertujuan untuk pengamanan Aset Informasi guna memastikan terjaganya aspek kerahasiaan, keutuhan, dan ketersediaan.

Pasal 3

(1) SMKI dilaksanakan berdasarkan prinsip:
    a. kerahasiaan *(confidentiality);*
    b. integritas *(integrity);*
    c. keaslian *(authenticity);*
    d. ketersediaan *(availability);* dan
    e. nirpenyangkalan *(non-repudiation);*
(2) Prinsip kerahasiaan sebagaimana dimaksud pada ayat (1) huruf a yaitu pemberian jaminan bahwa informasi yang telah ada diketahui/bocor kepada pihak yang tidak berhak mengetahui dan hanya bisa diakses oleh pihak yang berhak.
(3) Prinsip integritas sebagaimana dimaksud pada ayat (1) huruf b yaitu jaminan bahwa data tidak dapat diubah tanpa ada izin dari pihak yang berwenang, menjaga kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang bisa menyebabkan perubahan pada informasi atau data asli.
(4) Prinsip keaslian sebagaimana dimaksud pada ayat (1) huruf c yaitu jaminan kepastian terhadap informasi yang ditransaksikan dalam Sistem Informasi yang bersumber dari pihak yang sah.
(5) Prinsip ketersediaan sebagaimana dimaksud pada ayat (1) huruf d yaitu pemberian jaminan atas ketersediaan data atau informasi yang sedang ditransaksikan.

(6) Prinsip nirpenyangkalan sebagaimana dimaksud pada ayat (1) huruf e yaitu tidak bisa disangkalnya oleh seseorang atau pihak tertentu atas tindakannya yang telah dilakukan dalam sebuah Sistem Informasi.

Pasal 4

(1) SMKI dilaksanakan berdasarkan asas:
   a. manfaat;
   b. keamanan dan keandalan;
   c. efektif dan efisien;
   d. keterpaduan;
   e. integrasi;
   f. otorisasi; dan
   g. kepatuhan.

(2) Asas manfaat sebagaimana dimaksud pada ayat (1) huruf a merupakan pemanfaatan seoptimal mungkin dalam pelaksanaan dan pengelolaan sistem keamanan informasi Pemerintah Daerah sehingga dapat menyajikan informasi yang bermanfaat untuk kelancaran pelaksanaan ketugasan pegawai.

(3) Asas keamanan dan keandalan integritas sebagaimana dimaksud pada ayat (1) huruf b merupakan jaminan keamanan atas keadaan informasi yang diolah, disimpan dan disajikan dalam pelaksanaan dan pengelolaan sistem keamanan informasi Pemerintahan Daerah.

(4) Asas efektif dan efisien sebagaimana dimaksud pada ayat (1) huruf c merupakan pelaksanaan dan pengelolaan sistem keamanan informasi Pemerintah Daerah sebagai penunjang keberhasilan pelaksanaan tugas pegawai agar menjadi efektif dan efisien.

(5) Asas keterpaduan sebagaimana dimaksud pada ayat (1) huruf d merupakan kesatuan/keterpaduan dari berbagai kepentingan secara serasi dan proporsional dalam pelaksanaan dan pengelolaan sistem keamanan informasi Pemerintah Daerah.

(6) Asas integrasi sebagaimana dimaksud pada ayat (l) huruf e merupakan kemampuan pelaksanaan dan pengelolaan sistem keamanan informasi Pemerintah Daerah untuk memadukan/mempersatukan semua informasi strategis sebagai bahan pertimbangan dalam pengambilan keputusan bagi kepala Perangkat Daerah.

(7) Asas otorisasi sebagaimana dimaksud pada ayat (1) huruf f merupakan kemampuan menjaga keabsahan hak milik atas penyajian informasi sesuai dengan kewenangan masing-masing dalam pelaksanaan dan pengelolaan sistem keamanan informasi Pemerintah Daerah.

(8) Asas Kepatuhan sebagaimana dimaksud pada ayat (1) huruf g merupakan kemampuan pemenuhan terkait peraturan perundangan-undangan yang berlaku.

BAB II
PELAKSANAAN DAN PENGELOLAAN SISTEM MANAJEMEN KEAMANAN INFORMASI

Pasal 5

Kepala Perangkat Daerah menyediakan sumber daya yang dibutuhkan untuk membentuk, mengimplementasikan, memelihara, dan meningkatkan pelaksanaan dan pengelolaan SMKI secara berkesinambungan.

Pasal 6

(1) Pelaksanaan dan Pengelolaan SMKI terdiri atas:
   a. perencanaan pelaksanaan SMKI;
   b. organisasi SMKI;
   c. manajemen risiko keamanan informasi;
   d. keamanan sumber daya manusia;
   e. pengelolaan aset dan klasifikasi informasi;
   f. pengelolaan akses;
   g. manajemen kriptografi;
   h. manajemen keamanan fisik dan lingkungan;
   i. manajemen keamanan operasional Sistem Informasi;
   j. keamanan komunikasi;
   k. akuisisi, pengembangan, dan pemeliharaan sistem;
   l. penanganan Insiden Keamanan Informasi;
   m. manajemen keberlangsungan bisnis; dan
   n. kepatuhan;

(2) Pelaksanaan dan pengelolaan SMKI sebagaimana dimaksud pada ayat (1) diuraikan dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

BAB III

PENGAMANAN INFORMASI

Pasal 7

Pengamanan informasi yang diatur dalam Peraturan Bupati ini meliputi:

a. Aset Informasi;
b. aset pengolahan informasi; dan
c. penyimpanan informasi

Pasal 8

Aset Informasi sebagaimana dimaksud dalam Pasal 7 huruf a merupakan aset dalam bentuk:

a. fisik, 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.

Pasal 9

Aset Pengolahan Informasi sebagaimana dimaksud dalam Pasal 7 huruf b berupa:

a. peralatan mekanik yang digerakkan dengan tangan secara manual; dan
b. peralatan elektronik yang bekerja secara elektronik penuh.

Pasal 10

Penyimpanan Informasi sebagaimana dimaksud dalam Pasal 7 huruf c menggunakan media:

a. elektronik, terdiri atas *server, hard disk, flash disk*, kartu memori, dan perangkat elektronik sejenis lainnya; atau
b. non-elektronik, terdiri atas lemari, rak, laci, *filing cabinet*, dan perangkat non-elektronik sejenis lainnya.

Pasal 11

(1) Dinas menyusun standar operasional prosedur untuk melaksanakan Perlindungan keamanan, kerahasiaan, kekinian, akurasi, keutuhan data dan informasi sesuai prasyarat keamanan informasi.

(2) Prasyarat keamanan informasi sebagaimana dimaksud pada ayat (1) meliputi aspek sebagai berikut:
   a. organisasi keamanan informasi;
   b. keamanan sumber daya manusia;
   c. pengelolaan aset;
   d. pengendalian akses;
   e. kriptografi;
   f. keamanan fisik dan lingkungan;
   g. keamanan operasional;
   h. keamanan komunikasi;
   i. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan Sistem Informasi;
   j. hubungan kerja dengan pemasok;
   k. penanganan Insiden Keamanan Informasi;
   l. kelangsungan usaha; dan
   m. kepatuhan.
(3) Standar operasional prosedur keamanan informasi yang disusun oleh Dinas sebagaimana dimaksud pada ayat (1) berlaku untuk Pengguna layanan teknologi informasi dan komunikasi.

Pasal 12

(1) Setiap Perangkat Daerah harus melakukan uji keamanan Aplikasi Sistem Informasi guna menjamin keamanan data dan informasi serta meminimalisir kerentanan.
(2) Pengujian Aplikasi Sistem Informasi dilakukan oleh Dinas sebelum diimplementasikan ke infrastruktur layanan.

Pasal 13

(1) Dinas melaksanakan monitoring dan evaluasi dalam rangka pengamanan informasi sebagaimana dimaksud dalam Pasal 7.
(2) Monitoring dan evaluasi sebagaimana dimaksud pada ayat (1) dapat melibatkan Perangkat Daerah terkait.
(3) Hasil kegiatan monitoring dan evaluasi sebagaimana dimaksud pada ayat (1) dijadikan sebagai bahan rekomendasi dalam pengelolaan Aplikasi Sistem Informasi Perangkat Daerah dan dilaporkan kepada Bupati melalui Sekretaris Daerah.

BAB V

MANAJEMEN RISIKO

Pasal 14

(1) Perangkat Daerah penyelenggara Teknologi Informasi harus melakukan manajemen risiko dalam menerapkan SMKI.
(2) Manajemen risiko sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. pengembangan sistem;
    b. operasional Teknologi Informasi;
    c. jaringan komunikasi;
    d. penggunaan perangkat komputer;
    e. pengendalian terhadap informasi; dan/atau
    f. penggunaan pihak ketiga sebagai penyedia jasa Teknologi Informasi.
(3) Manajemen risiko sebagaimana dimaksud pada ayat (2) dilaksanakan melalui tahapan:
    a. identifikasi;
    b. pengukuran;
    c. pemantauan; dan
    d. pengendalian atas risiko terkait penggunaan Teknologi Informasi.
(4) Penerapan manajemen risiko harus dilakukan secara terintegrasi pada setiap penggunaan operasional Teknologi Informasi terkait sistem yang digunakan.

Pasal 15

(1) Dinas mengelola atas Insiden Keamanan Informasi.
(2) Pengelolaan Insiden Keamanan Informasi sebagaimana dimaksud pada ayat (1) dapat melibatkan Perangkat Daerah dan pihak lain yang terkait.
(3) Pihak lain sebagaimana dimaksud pada ayat (2) meliputi Pemerintah Daerah Daerah Istimewa Yogyakarta dan Pemerintah.
(4) Pengelolaan Insiden Keamanan Informasi sebagaimana dimaksud pada ayat (2) meliputi tahapan:
    a. identifikasi;
    b. lokalisasi insiden;
    c. mitigasi insiden;
    d. analisis insiden;
    e. penyusunan rekomendasi; dan
    f. pemulihan.

(5) Tahapan pengelolaan Insiden Keamanan Informasi sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan standar operasional prosedur.

Pasal 16

(1) Perangkat Daerah harus menerapkan prinsip pengendalian terhadap aktivitas Teknologi Informasi melalui proses evaluasi dan monitoring secara berkala.
(2) Setiap Perangkat Daerah harus melakukan kegiatan pemantauan dan tindakan koreksi penyimpangan terhadap kendali keamanan informasi yang meliputi:
    a. kegiatan pemantauan secara berkelanjutan; dan
    b. pelaksanaan fungsi pemeriksaan internal yang efektif dan menyeluruh.
(3) Perangkat Daerah Penyelenggara Teknologi Informasi berdasarkan hasil audit, umpan balik, maupun evaluasi terhadap pengendalian keamanan Informasi yang dilakukan, meningkatkan efektivitas sistem manajemen keamanan informasi secara berkesinambungan melalui perbaikan terhadap akibat penyimpangan kegiatan Teknologi Informasi.
(4) Kegiatan Audit sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Perangkat Daerah yang menyelenggarakan fungsi pengawasan dan pemantauan sesuai dengan perundang-undangan.
(5) Hasil dari tindakan perbaikan dan peningkatan sebagaimana dimaksud pada ayat (3) harus dilaporkan kepada Kepala Perangkat Daerah.

Pasal 17

(1) Bupati dapat menunjuk auditor independen untuk melakukan investigasi dalam hal terjadi kebocoran informasi pada instansi terkait.
(2) Dalam rangka melakukan investigasi sebagaimana dimaksud pada ayat (1) auditor independen mendapatkan hak akses.
(3) Hak akses sebagaimana dimaksud pada ayat (2) diperoleh dari Kepala Dinas atas persetujuan Kepala Perangkat Daerah.

BAB IV

KETENTUAN PENUTUP

Pasal 18

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Bantul
pada tanggal 14 Juli 2023

BUPATI BANTUL,

ttd

ABDUL HALIM MUSLIH

Diundangkan di Bantul
pada tanggal 14 Juli 2023

SEKRETARIS DAERAH KABUPATEN BANTUL,

ttd

AGUS BUDIRAHARJA

BERITA DAERAH KABUPATEN BANTUL TAHUN 2023 NOMOR 35

SALINAN SESUAI DENGAN ASLINYA
a.n SEKRETARIS DAERAH KABUPATEN BANTUL
ASISTEN PEMERINTAHAN DAN KESEJAHTERAAN RAKYAT
u.b. Kepala Bagian Hukum

PEMERINTAH KABUPATEN BANTUL
SETDA

SUPARMAN, S.IP., M.Hum
NIP 19680208199203 1007

LAMPIRAN
PERATURAN BUPATI BANTUL
NOMOR 35 TAHUN 2023
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI

SISTEM MANAJEMEN KEAMANAN INFORMASI

BAB I
PENDAHULUAN

1. **Tujuan**

   Sistem Manajemen Keamanan Informasi (SMKI) ini disusun sebagai arahan dan pedoman dalam pengelolaan sistem manajemen keamanan informasi secara terpadu serta untuk pengamanan Aset Informasi guna memastikan terjaganya aspek kerahasiaan (*confidentiality*), keutuhan (*integrity),* dan ketersediaan *(availability).*

2. **Ruang Lingkup**

   Ruang lingkup keamanan informasi meliputi:

   a. Keamanan informasi seperti keamanan database, kontrak, dokumentasi sistem, manual Pengguna, prosedur pendukung, *business continuity plan.*
   b. Keamanan aset perangkat lunak seperti keamanan perangkat lunak aplikasi, perangkat lunak sistem, perkakas pengembangan, dan *utilitas.*
   c. Keamanan aset fisik meliputi keamanan perangkat komputer, perangkat jaringan.
   d. Keamanan layanan meliputi keamanan layanan komputasi dan komunikasi, utilitas umum (listrik, pemanas, *air-conditioning*).
   e. Keamanan sumber daya manusia beserta kualifikasi, keterampilan dan pengalaman.
   f. Keamanan aset yang tidak berwujud seperti reputasi, image organisasi.

   Keamanan informasi merupakan tanggung jawab dari semua pihak yang terkait pada Pemerintah Kabupaten meliputi:

   a) Bupati Bantul
   b) Wakil Bupati Bantul

c) Sekretaris Daerah;
d) Asisten Pemerintah & Kesra;
e) Asisten Perekonomian
f) Asisten Umum;
g) Staf Ahli Bupati
h) Inspektorat;
i) Sekretariat DPRD;
j) Sekretariat Daerah;
k) Dinas Daerah (Dinas, Badan, Kantor, Satpol Pamong Praja);
l) Badan dan Lembaga Daerah lainnya yang meliputi Badan Perencanaan Pembangunan Daerah, Badan Pengelolaan Keuangan dan Aset Daerah, Badan Kepegawaian Pendidikan dan Pelatihan, Lembaga Teknis Daerah, Kecamatan/Kelurahan dan Lembaga Lain;
m) Serta pihak luar yang berhubungan dengan Pemerintah Kabupaten Bantul melalui akses fisik maupun *logic* antara lain tamu, pihak ketiga maupun pegawai di lingkungan perusahaan yang menggunakan fasilitas Pemerintah Kabupaten Bantul.

Pengecualian terhadap kepatuhan tersebut disetujui oleh pemilik asset informasi terkait dan Bupati Bantul

3. **Klasifikasi Kebijakan**

Kebijakan umum keamanan informasi memuat kebijakan keamanan informasi yang akan menjadi acuan dalam kebijakan spesifik, pedoman, prosedur, risk assessment maupun proses operasional keamanan informasi lainnya. Kebijakan spesifik akan digunakan oleh bagian teknis dalam menyelesaikan tanggung jawab keamanan informasi. Pedoman dan prosedur digunakan untuk mengimplementasikan kebijakan yang telah ditetapkan dan sifatnya anjuran. Hal tersebut berbeda dengan kebijakan yang sifatnya keharusan.

Kebijakan umum keamanan informasi memiliki kesamaan tingkat dengan kebijakan di Pemerintah Kabupaten Bantul yang lainnya dan dipatuhi oleh semua Pengguna. Berbeda dengan kebijakan spesifik yang hanya berlaku untuk OPD tertentu sesuai dengan bidangnya. Begitu pula dengan pedoman dan prosedur, pedoman dan prosedur dilaksanakan oleh OPD tertentu

BAB II
PERENCANAAN PELAKSANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI

1. **Tujuan Perencanaan Keamanan Informasi Kabupaten Bantul**

   Tujuan keamanan informasi Pemerintah Kabupaten Bantul sebagai berikut.

   a. Memastikan kerahasiaan terhadap Aset Informasi Pemerintah Kabupaten Bantul;
   b. Memastikan ketersediaan dan integritas informasi bagi *stakeholder*;
   c. Memastikan kepatuhan terhadap hukum, undang-undang dan peraturan yang berlaku; dan
   d. Memastikan kapabilitas organisasi untuk melanjutkan operasi atau layanannya ketika terjadi insiden keamanan.

2. **Prinsip Sistem Manajemen Keamanan Informasi**

   Prinsip keamanan informasi Pemerintah Kabupaten Bantul sebagai berikut:

   a. **Prinsip Kerahasiaan**

      Kemampuan akses atau modifikasi informasi diberikan hanya kepada pihak yang berwenang untuk tujuan yang jelas.

   b. **Prinsip Ketersediaan**

      Informasi dan aset TI yang dimiliki oleh Pemerintah Kabupaten Bantul tersedia untuk mendukung organisasi dalam rentang waktu yang disepakati bersama sesuai tujuan organisasi.

   c. **Prinsip Integritas**

      Informasi yang digunakan Pengguna bisa dipercaya kebenarannya merefleksikan realitas sebenarnya, terutama informasi strategis.

   d. **Prinsip Akuntabilitas**

      Tanggung jawab dan akuntabilitas pemilik, penyedia dan Pengguna Sistem Informasi dan pihak lain yang terkait dengan keamanan informasi harus dideskripsikan dengan jelas.

   e. **Prinsip Kesadaran**

      Pemilik, penyedia, Pengguna Sistem Informasi dan pihak lain yang terkait memiliki pemahaman dan informasi yang cukup mengenai kebijakan, pedoman, prosedur, ukuran, praktek keamanan informasi.

   f. **Prinsip Integrasi**

      Kebijakan, pedoman, prosedur, ukuran dan praktek untuk keamanan informasi harus dikoordinasikan dan diintegrasikan antara satu dengan yang lainnya.

g. **Prinsip Perbaikan Berkelanjutan**

Keamanan informasi harus diperbaiki terus menerus mengikuti perkembangan risiko dan kebutuhan organisasi.

3. **Acuan Perencanaan Sistem Manajemen**

1. Perangkat Daerah harus merencanakan suatu Sistem Manajemen Keamanan Informasi dengan mengadopsi siklus proses pada standar ISO/IEC 27001:2022. Deskripsi umum tentang siklus proses berdasarkan arahan standar ISO/IEC 27001:2022 dan Indeks KAMI (Keamanan Informasi).
2. Proses perencanaan dalam pengembangan Sistem Manajemen Keamanan Informasi menurut ISO/IEC 27001:2022 meliputi:

2.1 Klausul ISO/IEC 27001

a) Konteks Organisasi
b) Kepemimpinan
c) Perencanaan
d) Pendukung
e) Operasi
f) Evaluasi
g) Dan Tindakan Perbaikan

2.2 *Annex* Kontrol ISO/IEC 27001

a) organisasi keamanan informasi;
b) keamanan sumber daya manusia;
c) pengelolaan aset;
d) pengendalian akses;
e) kriptografi*;*
f) keamanan fisik dan lingkungan;
g) keamanan operasional;
h) keamanan komunikasi;
i) keamanan dalam proses akuisisi, pengembangan dan pemeliharaan Sistem Informasi;
j) hubungan kerja dengan pemasok;
k) penanganan insiden keamanan informasi;
l) kelangsungan usaha; dan
m) kepatuhan.

3. Proses perencanaan dalam pengembangan Sistem Manajemen Keamanan Informasi menurut Indeks KAMI (Keamanan Informasi) meliputi:

a. Tata kelola keamanan informasi;
b. Pengelolaan risiko keamanan informasi;
c. Kerangka kerja keamanan informasi;
d. Pengelolaan Aset Informasi;
e. Teknologi dan keamanan informasi.

BAB III
ORGANISASI SISTEM MANAJEMEN KEAMANAN INFORMASI

1. **Tujuan**

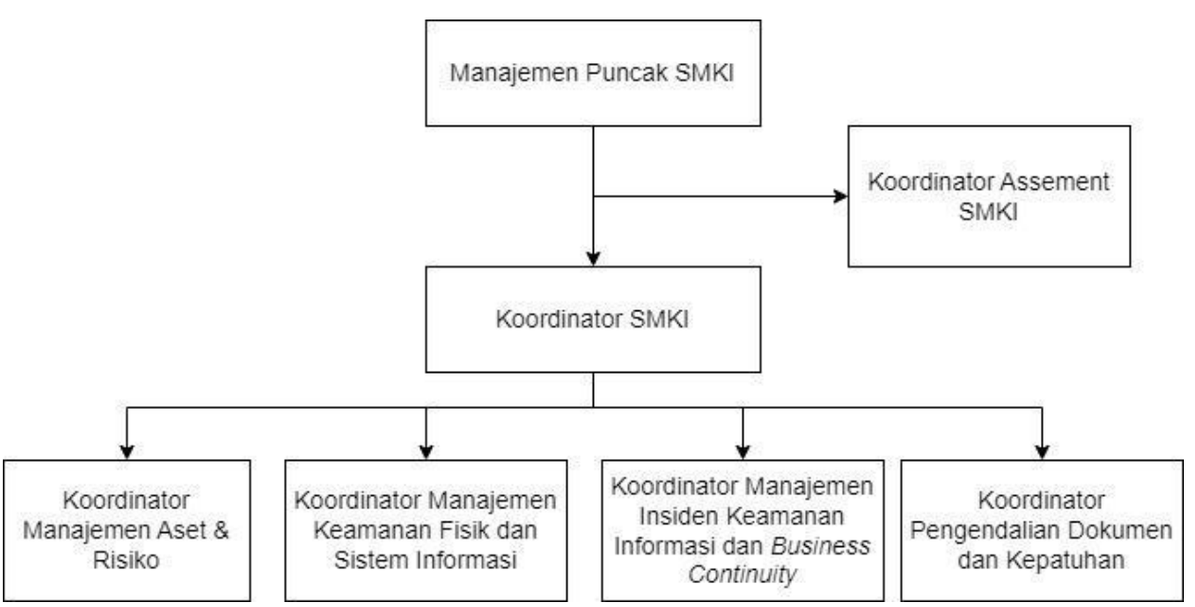
   Organisasi Tim Keamanan Informasi Pemerintah Daerah Kabupaten Bantul dibentuk dengan tujuan sebagai berikut:

   a) Sebagai pedoman dalam pembentukan organisasi fungsional keamanan informasi yang bertanggung jawab dalam pengelolaan keamanan informasi serta hubungan kerja dengan pihak eksternal;
   b) Menumbuhkan kesadaran pada sumber daya manusia Pemerintah Daerah Kabupaten Bantul tentang arti penting keamanan informasi;
   c) Menindaklanjuti terkait keamanan informasi insiden yang terjadi dalam implementasi Sistem manajemen keamanan Informasi.

2. **Struktur Organisasi Sistem Manajemen Keamanan Informasi Perangkat Daerah**

   2.1 Perangkat Daerah wajib membentuk struktur organisasi berbasiskan sistem manajemen keamanan informasi untuk memastikan pelaksanaan keamanan informasi sesuai dengan standar ISO/IEC 27001:2022

   2.2 Organisasi Sistem Manajemen Keamanan Informasi merupakan organisasi fungsional yang memiliki struktur seperti yang diberikan pada Gambar 1 berikut:



Gambar 1. Struktur Organisasi SMKI Perangkat Daerah

2.3 Manajemen puncak SMKI memiliki tugas dan tanggung jawab sebagai berikut:

a. memberikan arahan dan tujuan umum dari SMKI organisasi, dalam bentuk kebijakan Sistem Manajemen Keamanan Informasi (SMKI);
b. memastikan bahwa tujuan dan rencana dari SMKI organisasi telah ditetapkan;
c. menetapkan struktur organisasi beserta alokasi tugas dan tanggung jawab dalam SMKI organisasi;
d. mengkomunikasikan kepada personil dalam organisasi terkait pentingnya pemenuhan aturan terkait keamanan informasi organisasi sesuai ketentuan peraturan perundang-undangan serta perlunya peningkatan SMKI organisasi secara berkesinambungan;
e. menyediakan sumber daya yang memadai untuk menetapkan, mengimplementasi, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan SMKI organisasi;
f. menetapkan kriteria penerimaan risiko dan tingkat risiko yang dapat diterima;
g. menyetujui tingkat risiko residual keamanan informasi;
h. memastikan pelaksanaan audit internal SMKI; dan
i. menghadiri dan memimpin rapat tinjauan manajemen SMKI.

2.4 Koordinator SMKI memiliki tugas dan tanggung jawab sebagai berikut:

a. menyusun, mengoordinasikan, serta memantau pelaksanaan program kerja SMKI;
b. mengoordinasikan pelaksanaan proses manajemen risiko SMKI organisasi;
c. mengoordinasikan pelaksanaan aktivitas SMKI serta pengamanan informasi di organisasi;
d. mengoordinasikan proses peninjauan secara berkala terhadap implementasi SMKI di organisasi;
e. mengoordinasikan proses pengukuran efektivitas SMKI dan kontrol keamanan informasi di organisasi;
f. mengoordinasikan aktivitas dan tindakan untuk meningkatkan efektivitas SMKI, yang mencakup antara lain koreksi dan tindakan korektif untuk ketidaksesuaian yang ditemukan serta pelaksanaan rencana penanganan risiko; dan
g. memberikan laporan secara berkala terkait kondisi SMKI dan keamanan informasi organisasi kepada manajemen puncak SMKI.

2.5 Koordinator Asesmen SMKI memiliki tugas dan tanggung jawab sebagai berikut:

a. menyusun dan memantau program dan jadwal *Assement* SMKI;
b. mengoordinasikan pelaksanaan proses Asesmen SMKI;
c. merangkum dan melaporkan hasil Asesmen SMKI kepada manajemen puncak SMKI;
d. memberikan rekomendasi terkait kontrol keamanan informasi yang diperlukan untuk meningkatkan efektivitas SMKI; dan
e. mengoordinasikan proses verifikasi koreksi dan Tindakan korektif yang diambil terhadap ketidaksesuaian yang ditemukan dalam proses audit internal SMKI.

2.6 Koordinator manajemen aset dan risiko SMKI memiliki tugas dan tanggung jawab sebagai berikut:

a. mengoordinasikan dan memantau pengelolaan Aset Informasi dan aset pengolahan dan penyimpanan informasi organisasi, hal ini mencakup proses registrasi, inventarisasi, serta pemeliharaan inventarisasi aset tersebut;
b. menyusun dan memelihara dokumen registrasi Aset Informasi dan aset pengolahan dan penyimpanan informasi organisasi;
c. melakukan peninjauan terkait proses penanganan asset informasi dan aset pengolahan dan penyimpanan informasi organisasi berdasarkan kebijakan dan prosedur terkait pengelolaan aset SMKI organisasi;
d. menyusun dan mengoordinasikan aktivitas proses pengelolaan manajemen risiko SMKI di organisasi, bekerja sama dengan pemilik risiko, berdasarkan kebijakan dan prosedur terkait pengelolaan risiko SMKI organisasi;
e. mengoordinasikan proses registrasi terhadap risiko SMKI di organisasi, bekerja sama dengan pemilik risiko;
f. mengoordinasikan pengkinian secara rutin terhadap registrasi risiko organisasi, bekerja sama dengan pemilik risiko; dan
g. menyusun dan memelihara dokumen risk profile dan risk treatment plan SMKI organisasi.

2.7 Koordinator manajemen keamanan fisik dan Sistem Informasi SMKI memiliki tugas dan tanggung jawab sebagai berikut:

a. mengoordinasikan dan memantau proses dan aktivitas pengamanan fisik dan lingkungan dalam organisasi;

b. melaksanakan proses pengelolaan dan pemeliharaan fasilitas pengamanan fisik organisasi berdasarkan kebijakan dan prosedur terkait keamanan fisik dan lingkungan SMKI organisasi;
c. melaksanakan proses pengelolaan dan pemeliharaan hak akses fisik ke fasilitas organisasi berdasarkan kebijakan dan prosedur terkait keamanan fisik dan lingkungan SMKI organisasi;
d. mengoordinasikan dan memantau proses dan aktivitas pengelolaan akses *logical*;
e. Melaksanakan proses pengelolaan dan pemeliharaan akses *logical* dari Pengguna ke Sistem Informasi organisasi berdasarkan kebijakan dan prosedur terkait keamanan akses logical ke Sistem Informasi organisasi, hal ini mencakup proses pendaftaran, pemeliharaan dan pencabutan hak akses *logical* Pengguna ke Sistem Informasi;
f. mengakomodasi penyusunan dan pemeliharaan *access control matrix* bersama-sama dengan Perangkat Daerah pemilik aplikasi dan/atau informasi;
g. mengoordinasikan dan memantau pengelolaan keamanan operasional Sistem Informasi organisasi berdasarkan kebijakan dan prosedur terkait pengelolaan keamanan operasional Sistem Informasi organisasi; dan
h. merancang, memantau dan memelihara sistem keamanan dari Sistem Informasi organisasi yang ini mencakup perangkat keras, lunak maupun aktif jaringan dan keamanan jaringan dalam Sistem Informasi organisasi.

2.8 Koordinator manajemen insiden keamanan informasi dan keberlangsungan bisnis SMKI memiliki tugas dan tanggung jawab sebagai berikut:
a. mengoordinasikan proses pendokumentasian laporan terkait kejadian, kelemahan dan insiden keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi organisasi;
b. mengoordinasikan dan memantau pengelolaan insiden keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi organisasi;
c. mendokumentasikan proses pengelolaan insiden keamanan
d. informasi di organisasi;

e. mengoordinasikan dan memantau pengelolaan *business continuity management* di organisasi berdasarkan kebijakan dan prosedur terkait business continuity management organisasi;
f. mengoordinasikan penyusunan, pengujian, dan pemeliharaan *business continuity plan* dan *disaster recovery plan* organisasi;
g. memastikan terjaganya aspek keamanan informasi dalam proses *business continuity management*.

2.9 Koordinator pengendalian dokumen dan kepatuhan SMKI memiliki tugas dan tanggung jawab sebagai berikut:
a. mengoordinasikan dan memantau proses pengelolaan dokumentasi terkait SMKI organisasi hal ini mencakup kebijakan dan prosedur terkait SMKI organisasi;
b. mengidentifikasi dan mendokumentasikan peraturan perundang-undangan dan kewajiban kontrak yang relevan dengan SMKI dan keamanan informasi organisasi;
c. melakukan pemantauan berkala terhadap kepatuhan SMKI organisasi dengan prasyarat dari kebijakan dan prosedur SMKI organisasi serta peraturan perundang-undangan dan kewajiban kontrak yang relevan dengan SMKI dan keamanan informasi organisasi;
d. menyusun dan mengoordinasikan pelaksanaan program security awareness bagi personil organisasi; dan
e. menyusun metrik pengukuran efektivitas SMKI dan control keamanan informasi organisasi.

3. **Struktur Organisasi Sistem Manajemen Keamanan Informasi Tingkat Kabupaten Bantul**

Organisasi keamanan informasi Pemerintah Kabupaten Bantul terdiri dari:

3.1 Penanggung Jawab Eksekutif *(Government Chief Information Officer/ GCIO)*

Dipimpin oleh Sekretaris Daerah untuk menentukan prinsip berdasarkan fakta dan kebijakan keamanan informasi, menjamin ketersediaan, keakuratan, ketepatan, dan keamanan informasi yang dibutuhkan oleh organisasi untuk mencapai tujuan organisasi, serta mendapatkan laporan dari GCISO, Komite Risiko, dan Komite Audit untuk memastikan prinsip, aksioma, kebijakan dan pelaksanaan keamanan informasi diterapkan.

3.2 Penanggung Jawab Utama Keamanan Informasi *(Government Chief Information Security Officer/ GCISO)*

Dijabat oleh Kepala Dinas Komunikasi dan Informatika bertanggung jawab atas aspek keamanan informasi di lingkungan Pemerintah Kabupaten Bantul.

3.3 Komite Keamanan Informasi (KKI)

Komite yang dipimpin oleh GCISO dan anggotanya meliputi semua Kepala OPD. KKI merupakan Komite yang dibentuk untuk membahas dan memutuskan sejumlah aspek yang terkait dengan keamanan dalam pengembangan, implementasi, pengoperasian, monitoring, pemeliharaan dan peningkatan Tata Kelola Keamanan Informasi Pemerintah Kabupaten Bantul.

3.4 Tim Teknis SMKI

Tim teknis SMKI dipimpin KKI (Komite Keamanan Informasi) disetiap OPD. KKI membentuk tim teknis dengan rincian sebagai berikut:

1. Koordinator SMKI
2. Koordinator Manajemen Keamanan Fisik dan Sistem Informasi
3. Koordinator Manajemen Aset dan Manajemen Risiko
4 Koordinator Manajemen Insiden Keamanan Informasi dan Kelangsungan Bisnis
5 Koordinator Pengendalian Dokumen dan Kepatuhan
6 Koordinator Asesmen SMKI

Dalam pemilihan tim Teknis di setiap OPD wajib dilakukan pengesahan oleh KKI.

3.5 Audit Internal

Ditugaskan kepada Inspektorat untuk bertanggung jawab dalam melakukan peninjauan independen atas tata kelola keamanan informasi. Mencakup peninjauan implementasi kebijakan, pedoman dan prosedur keamanan informasi untuk menjamin efektivitasnya.

3.6 Tugas dan Wewenang (*Government Chief Information Officer*/GCIO) Penanggung Jawab Utama Keamanan Informasi *(Government Chief Information Security Officer*/GCISO) harus menunjukkan kepemimpinan dan komitmen terkait Keamanan Informasi dengan cara:

a. Memastikan kebijakan keamanan informasi dan sasaran keamanan informasi ditetapkan dan selaras dengan arah strategis Pemerintah Kabupaten Bantul
b. Memastikan persyaratan Keamanan Informasi terintegrasi ke dalam proses organisasi;

c. Memastikan tersedianya sumber daya yang dibutuhkan untuk pelaksanaan Keamanan Informasi;
d. Mengomunikasikan pentingnya manajemen keamanan informasi yang efektif dan kesesuaian dengan persyaratan Keamanan Informasi;
e. Memastikan bahwa pelaksanaan Keamanan Informasi mencapai manfaat yang diharapkan;
f. Memberikan arahan dan dukungan pada personel untuk berkontribusi dalam efektivitas pelaksanaan Keamanan Informasi;
g. Mempromosikan perbaikan berkelanjutan; dan
h. Mendukung peran manajemen yang relevan lainnya untuk menunjukkan kepemimpinannya ketika diterapkan pada wilayah tanggung jawabnya.

3.7 Tanggung Jawab Penanggung Jawab Eksekutif (*Government Chief Information Officer*/ GCIO)

Penanggung Jawab Eksekutif bertanggung jawab memberikan arahan strategis keamanan informasi.

Penanggung Jawab Eksekutif mempunyai peran sebagai berikut:

a. Memberikan dukungan terhadap keamanan informasi;
b. Mereview dan menyetujui prinsip dan aksioma keamanan informasi;
c. Menyetujui anggaran keamanan informasi;
d. Menerima dan menindaklanjuti laporan manajemen terkait keamanan informasi.

3.8 Tanggung Jawab Komite Keamanan Informasi (KKI)

KKI merupakan Komite yang dibentuk untuk membahas dan memutuskan sejumlah aspek yang terkait dengan pengembangan, implementasi, pengoperasian, monitoring, pemeliharaan dan peningkatan tata Kelola keamanan informasi. Mekanisme koordinasi dalam KKI dilakukan melalui pertemuan tatap muka secara berkala atau melalui media komunikasi lain seperti email atau social media internal Pemerintah Kabupaten Bantul.

Komite Keamanan Informasi mempunyai peran sebagai berikut.

a. Melakukan revisi kebijakan keamanan informasi yang disampaikan oleh GCISO dan disahkan oleh Bupati Bantul;
b. Membahas dan memutuskan pelaksanaan reviu independen atas kebijakan keamanan informasi;

c. Menyepakati klasifikasi Aset Informasi Pemerintah Kabupaten Bantul. Klasifikasi Aset Informasi tersebut disahkan Kabupaten Bantul;
d. Menyepakati sanksi yang akan dikenakan apabila terjadi pelanggaran.

3.9 Tanggung Jawab Auditor Internal

Auditor internal dibentuk oleh pihak Inspektorat Daerah dan diperbolehkan mengambil auditor eksternal dengan keahlian keamanan informasi sesuai persyaratan yang ditentukan/

Auditor internal keamanan informasi mempunyai peran sebagai berikut:

a. mengoordinasikan pelaksanaan proses Audit SMKI;
b. merangkum dan melaporkan hasil Audit SMKI kepada manajemen puncak SMKI;
c. memberikan rekomendasi terkait kontrol keamanan informasi yang diperlukan untuk meningkatkan efektivitas SMKI; dan
d. mengoordinasikan proses verifikasi koreksi dan Tindakan korektif yang diambil terhadap ketidaksesuaian yang ditemukan dalam proses audit internal SMKI.

BAB IV
MANAJEMEN RISIKO KEAMANAN INFORMASI

1. **Tujuan**

   Tujuan manajemen risiko dalam penerapan Sistem Manajemen Keamanan Informasi Pemerintah Kabupaten Bantul yaitu:

   a. Mendukung tata kelola keamanan informasi;
   b. Mengetahui risiko yang bersumber dari Aset Informasi dan proses bisnis;
   c. Kepatuhan terhadap ISO 27001;
   d. Persiapan business continuity plan;
   e. Persiapan incident response plan;
   f. Penyusunan persyaratan keamanan informasi.

2. **Ruang Lingkup**

   Ruang lingkup manajemen risiko meliputi identifikasi risiko, analisa dan evaluasi risiko, identifikasi dan evaluasi alternatif penanganan risiko, persetujuan pimpinan atas manajemen risiko serta pernyataan pelaksanaan manajemen risiko.

3. **Kebijakan Manajemen Risiko**

   Manajemen risiko terdiri dari beberapa tahapan yaitu pembentukan konteks, identifikasi risiko, analisa & evaluasi risiko, identifikasi & evaluasi alternatif penanganan risiko, persetujuan pimpinan dan pernyataan penerapan manajemen keamanan informasi.

   Berikut kebijakan pada masing-masing tahapan tersebut.

   a. Pembentukan Konteks Risiko;
      1) Menentukan lingkup dan batasan manajemen risiko sesuai dengan operasi, struktur, lokasi, aset, dan teknologi yang ada di Pemerintah Kabupaten Bantul.
      2) Merupakan kriteria yang akan digunakan untuk mengevaluasi risiko keamanan informasi di Pemerintah Kabupaten Bantul.
   b. Identifikasi Risiko;
      1) Identifikasi Aset Informasi sesuai dengan lingkup manajemen risiko dan pemilik dari aset tersebut;
      2) Identifikasi ancaman atas Aset Informasi tersebut;
      3) Identifikasi kerentanan sebagai hasil ancaman tersebut;

4) Identifikasi dampak dari hilangnya kerahasiaan, integritas dan ketersediaan serta independensi yang mungkin terjadi atas Aset Informasi tersebut.

c. Analisis dan Evaluasi Risiko;
   1) Perkiraan dampak yang diterima oleh Pemerintah Kabupaten Bantul jika terjadi suatu kegagalan keamanan informasi, termasuk juga konsekuensi atas hilangnya kerahasiaan, integritas dan ketersediaan informasi;
   2) Perkiraan kemungkinan munculnya kegagalan keamanan akibat adanya ancaman, kerentanan, dan dampak yang berkaitan dengan Aset Informasi tersebut dan pengendalian yang dilakukan saat ini;
   3) Perkirakan tingkatan untuk setiap risiko;
   4) Tentukan apakah risiko dapat diterima atau memerlukan Tindakan lebih lanjut menggunakan kriteria risiko yang wajar yang telah ditetapkan;

d. Identifikasi dan Evaluasi Alternatif Penanganan Risiko;
   1) Melakukan pengendalian yang memadai atas risiko tersebut;
   2) Menerima risiko tersebut sesuai dengan kebijakan Pemerintah Kabupaten Bantul;
   3) Menghindari risiko tersebut;
   4) Memilih tujuan dan rancangan pengendalian sebagai bentuk penanganan risiko, yang didasarkan kepada standar SNI ISO/IEC 27001:2022, ISO 27001:2022, ISO/IEC 27005:2018, PP60/2008 SPIP dan standar lain.

BAB V
KEAMANAN SUMBER DAYA MANUSIA

1. **Tujuan**

   Kebijakan keamanan sumber daya manusia ditetapkan memiliki tujuan:

   a. untuk memberikan pedoman dalam mengelola keamanan sumber daya manusia dalam ruang lingkup SMKI di Pemerintah Daerah Kabupaten Bantul
   b. Memastikan bahwa seluruh pegawai Pemerintah Kabupaten Bantul memahami peran dan tanggung jawab mereka terhadap keamanan informasi untuk mengurangi risiko terjadinya pencurian, kecurangan, dan penyalahgunaan Aset Informasi dan fasilitas pengolahnya;
   c. Memastikan bahwa seluruh pegawai Pemerintah Kabupaten Bantul waspada terhadap ancaman keamanan informasi sehingga mereka sadar akan peran dan tanggungjawab mereka untuk mengurangi risiko terjadinya insiden karena faktor kelalaian manusia.

2. **Ruang Lingkup**

   Ruang lingkup pengendalian aspek SDM yaitu:

   a. Proses pemeriksaan dan verifikasi pegawai internal Pemerintah Daerah Kabupaten Bantul mulai dari latar belakang (screening) calon pegawai, sosialisasi peran dan tanggung jawab dalam keamanan informasi termasuk perjanjian kerahasiaan, pendidikan dan pelatihan peningkatan keamanan informasi, dan perubahan dan/atau penghapusan hak akses informasi dan pengembalian Aset Informasi jika ada pemberhentian, perubahan, atau berakhirnya perjanjian kerja
   b. Pegawai dari pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke Aset Informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Daerah Kabupaten Bantul.

3. **Kebijakan**

   a. Calon pegawai di lingkungan Pemerintah Daerah Kabupaten Bantul dan pegawai dari pihak eksternal, harus melalui proses screening untuk memastikan bahwa mereka sesuai dengan tugas dan tanggung jawab yang akan mereka dapatkan.
   b. Proses screening perlu mencakup verifikasi terhadap latar belakang kandidat sesuai dengan peraturan perundang-undangan serta etika yang ada.

c. Pegawai dalam lingkungan Pemerintah Daerah Kabupaten Bantul dan pegawai dari pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke Aset Informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Daerah Kabupaten Bantul harus menandatangani perjanjian kerahasiaan (*non-disclosure agreement)* dengan memperhatikan tingkat sensitivitas dari aset yang diakses.
d. Setiap pegawai internal maupun eksternal harus mematuhi seluruh kebijakan dan prosedur Perangkat Daerah terkait keamanan informasi.
e. Setiap pegawai internal maupun eksternal harus diberikan informasi yang memadai terkait tugas dan tanggung jawab terkait keamanan informasi yang mereka miliki.
f. Program peningkatan kesadaran keamanan informasi *(awareness)* secara berkelanjutan untuk menjaga dan meningkatkan kesadaran keamanan informasi dari pegawai harus dilaksanakan.
g. Setiap pelanggaran terhadap kebijakan dan prosedur terkait keamanan informasi harus ditindaklanjuti dan apabila diperlukan, tindakan pendisiplinan harus diambil sesuai dengan peraturan yang berlaku.
h. Tanggung jawab dan kewajiban terkait keamanan informasi yang tetap berlaku setelah pemberhentian atau perubahan status kepegawaian harus didefinisikan, dikomunikasikan, dan ditegakkan kepada pegawai internal maupun eksternal.
i. Hal ini mencakup tanggung jawab keamanan informasi yang tercakup dalam perjanjian kerja seperti:
    1. Seluruh aset organisasi harus dikembalikan setelah pemberhentian kepegawaian;
    2. Seluruh hak akses organisasi harus dinonaktifkan atau dihapus setelah pemberhentian kepegawaian;
    3. Seluruh hak akses organisasi harus disesuaikan setelah perubahan status kepegawaian; dan
    4. Untuk pihak ketiga penonaktifan hak akses setelah pekerjaan selesai.

BAB VI
PENGELOLAAN ASET DAN KLASIFIKASI INFORMASI

1. **Tujuan**

   Pengelolaan Aset Informasi dalam implementasi Sistem Manajemen Keamanan Informasi bertujuan sebagai berikut:

   a. Untuk memberikan pedoman dalam mengelola aset yang terkait informasi serta fasilitas fisik pengolahan informasi,
   b. Melakukan klasifikasi informasi sehingga Aset Informasi mendapatkan perlindungan yang sesuai dengan tingkat kepentingannya dalam proses distribusi informasi

2. **Ruang Lingkup**

   Ruang lingkup kebijakan terkait pengelolaan Aset Informasi terdiri dari:

   a. Klasifikasi, pelabelan dan penanganan informasi dalam ruang lingkup Peraturan Bupati terkait SMKI; dan
   b. penanganan aset pengolahan dan penyimpanan informasi dalam ruang lingkup Peraturan Bupati.

3. **Kebijakan**

   3.1 *GCISO (Government Chief Information Security Officer)* menetapkan pemilik Aset Informasi di setiap unit Perangkat Daerah, beserta perangkat fisik pengolah informasi yang terkait.

   3.2 Klasifikasi Aset

   Klasifikasi Aset dibagi menjadi 6 yaitu:

   a. perangkat keras, meliputi perangkat keras yang digunakan untuk mengolah dan menyimpan informasi dalam bentuk fisik maupun elektronik, yang mencakup namun tidak terbatas pada komputer, *notebook*, server, *hard disk drive*, *USB disk*;
   b. perangkat lunak, meliputi perangkat lunak yang digunakan untuk mengolah informasi dalam bentuk elektronik, yang mencakup namun tidak terbatas pada sistem operasi, aplikasi, dan *database;*
   c. perangkat jaringan, meliputi perangkat keras dan lunak yang digunakan untuk membentuk dan infrastruktur jaringan telekomunikasi, yang mencakup namun tidak terbatas pada *hub, switch, router, firewall, IDS, IPS, dan network monitoring tools*;

d. perangkat pendukung meliputi perangkat digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan informasi yang mencakup namun tidak terbatas pada genset, *UPS, AC*, rak server, lemari penyimpanan informasi, dan *CCTV*;
e. layanan, meliputi layanan yang digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan informasi yang mencakup namun tidak terbatas pada layanan jaringan komunikasi, layanan *hosting* dan *co-location*, layanan pemeliharaan perangkat dan sistem, dan layanan pemasangan infrastruktur; dan
f. sumber daya manusia meliputi personil baik internal maupun eksternal yang terlibat dalam pengolahan dan penyimpanan informasi

3.3 Klasifikasi Informasi

Klasifikasikan berdasarkan tiga kriteria. Berikut klasifikasi pada masing masing kriteria:

1. Informasi Publik
2. Informasi Terbatas
3. Informasi Rahasia
4. Informasi Sangat Rahasia

3.4 Pemilik aset dapat mendelegasikan tugas pengamanan dan pemeliharaan aset kepada kustodian aset, namun tanggung jawab akhir terhadap aset tetap berada pada pemilik aset.

3.5 Aset pengolahan dan penyimpanan informasi harus secara berkala dipelihara dengan memadai.

3.6 Apabila dalam pemeliharaan aset pengolahan dan penyimpanan informasi tersebut harus menggunakan jasa pihak ketiga penyedia, maka:

a. kontrak pemeliharaan perlu dibuat dengan pihak ketiga penyedia jasa yang kompeten dan relevan; dan
b. peralatan yang dibawa keluar untuk pemeliharaan harus diperiksa untuk mencegah kebocoran informasi.

3.7 Dalam proses penghapusan aset harus dilakukan secara aman dengan metode yang dapat mencegah kebocoran informasi seperti menghancurkan secara fisik *harddisk drive*.

3.8 Semua Aset Informasi dan pengolahan dan penyimpanan informasi milik Pemerintah Daerah Kabupaten Bantul harus dikembalikan setelah personil Pengguna tidak memiliki hubungan kepegawaian lagi dengan Pemerintah Daerah Kabupaten Bantul, misalnya karena pengunduran diri, pensiun.

3.9 Ketentuan dalam proses pengembalian aset tersebut mencakup:

a. pengembalian aset harus terdokumentasi secara formal;
b. untuk pengembalian aset yang disebabkan oleh terhentinya status kepegawaian, informasi yang tersimpan dalam aset harus di-*backup* dan informasi yang tersimpan dalam aset harus dihapus secara aman, antara lain dengan *secure format* atau melakukan instalasi ulang sistem operasi secara menyeluruh; dan
c. media penyimpanan backup informasi harus diamankan secara fisik, antara lain dengan menyimpan dalam lemari terkunci dengan akses yang terbatas.

3.10 Aset pengolahan informasi, seperti komputer dan laptop yang akan digunakan kembali baik oleh pihak internal maupun eksternal harus diperiksa untuk menjamin tidak ada informasi sensitive yang tersimpan dalam aset tersebut.

3.11 Setiap pemilik informasi harus memperhatikan keamanan informasi yang tersimpan dalam media penyimpanan informasi antara lain:

a. Dalam hal data yang tersimpan di dalam media bersifat rahasia, perlu diberikan proteksi kata sandi untuk melindungi data;
b. Dalam hal tidak lagi dibutuhkan atau digunakan, seluruh data yang tersimpan di dalam media harus sepenuhnya dihapus sehingga tidak lagi dapat dipulihkan;
c. Data yang tersimpan di dalam media yang akan dibuang harus mendapatkan perlakuan khusus guna meminimalkan terjadinya kebocoran informasi kepada pihak yang tidak sah yaitu:
    1) data yang tersimpan di dalam media yang memuat informasi rahasia harus dibuang dengan cara dihancurkan atau dibakar; dan
    2) data yang tersimpan di dalam media yang memuat informasi lainnya harus dilakukan penghapusan total dengan cara-cara tertentu yang tidak lagi dapat dipulihkan.

3.12 Informasi yang dianggap kritikal oleh Perangkat Daerah harus di-*backup* secara memadai untuk menjamin ketersediaannya.

3.13 Hal yang perlu dipertimbangkan dalam proses backup informasi meliputi:

a. pemilik informasi bertanggung jawab untuk menentukan informasi yang membutuhkan backup, frekuensi dan metode backup serta waktu retensi untuk setiap backup informasi yang ada;
b. pernyataan formal terkait informasi yang dibutuhkan untuk di-backup beserta metode dan frekuensi dari backup harus ditentukan bersama dengan personil yang bertugas melaksanakan proses backup serta harus dinyatakan secara jelas dalam sebuah rencana backup resmi;
c. backup informasi harus disimpan sesuai dengan masa retensi dari informasi utama;
d. masa retensi harus dinyatakan secara jelas dalam rencana backup; dan
e. perlindungan terhadap backup informasi harus dilakukan berdasarkan klasifikasi dari informasi utama.

3.14 Perangkat Daerah menyediakan akses internet dan *email* kepada pegawainya hanya untuk kebutuhan pekerjaan dan operasional Pemerintah.

3.15 Ketentuan dalam penggunaan internet dan *email* adalah sebagai berikut:

a. Pengguna dilarang menggunakan akses internet dan *email* Perangkat Daerah untuk kegiatan melanggar hukum dan aktivitas yang dapat membahayakan keamanan jaringan Pemerintah;
b. Pengguna dilarang untuk menggunakan akses internet dan *email* Perangkat Daerah untuk mengakses, mendistribusikan, mengunggah, dan/atau mengunduh:
    1) materi pornografi;
    2) materi bajakan seperti, perangkat lunak, *file* music, dan video/film;
    3) materi yang melecehkan, mendiskriminasikan, yang membakar emosi atau menimbulkan kebencian atau membuat pernyataan palsu atau yang bersifat merusak mengenai orang lain;
    4) situs yang dapat menimbulkan risiko serangan *malware,* penyusupan, atau *hacking* ke jaringan Pemerintah.

3.16 Pengguna disarankan untuk tidak membagi informasi pribadi melalui situs internet atau media sosial.

3.17 Pengguna dilarang untuk mendistribusikan informasi pemerintah yang bersifat rahasia tanpa izin dari pemilik informasi.

3.18 Pesan penyangkalan ini harus dituliskan pada akhir setiap *email.* "Pesan ini mungkin berisi informasi rahasia dan hanya ditujukan kepada pihak yang dituju. Apabila anda bukanlah pihak yang dituju, anda dilarang untuk mengungkapkan, menyebarkan atau menyalin isi *email* ini. Apabila anda mendapatkan email ini tanpa sengaja mohon segera hubungi pengirim *email* dan hapus *email* ini segera. Pemerintah Daerah tidak bertanggung jawab untuk pengiriman informasi ini secara lengkap dan tepat dan juga tidak bertanggung jawab untuk keterlambatan dalam pengiriman email ini."

3.19 Perangkat Daerah yang mengelola akun *email* Perangkat Daerah berhak untuk mem-*block* akun *email* pemerintah pada saat terdapat bukti memadai terkait penyalahgunaan dan/atau pelanggaran keamanan.

3.20 Manajemen Kapasitas wajib diatur dalam proses penentuan kapasitas berupa CPU, Server, dan RAM minimal 70%.

BAB VII
PENGELOLAAN AKSES

1. **Tujuan**

   Tujuan pengelolaan hak akses yaitu :

   a. Untuk mengendalikan akses terhadap informasi yang dimiliki Pemerintah Kabupaten Bantul sehingga informasi hanya bisa diakses oleh pihak yang berwenang saja.
   b. Pengelolaan hak akses meliputi pemberian hak akses, pemberian hak akses kepada pihak eksternal, pengendalian akses jaringan dan sistem operasi.

2. **Ruang Lingkup**

   Ruang Lingkup dari pengendalian akses adalah akses ke Aset Informasi dan aset pengolahan dan penyimpanan informasi berupa fisik dan Logika maupun elektronik dan non elektronik dalam lingkungan Pemerintah Daerah Kabupaten Bantul yang mencakup:

   a. persyaratan pengendalian akses;
   b. pengendalian akses jaringan;
   c. pengelolaan akses Pengguna;
   d. tanggung jawab Pengguna; dan
   e. pengendalian akses atas sistem dan aplikasi.

3. Kebijakan

3.1 Persyaratan pengendalian akses pada suatu sistem meliputi:

   a. akses ke Aset Informasi serta aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Daerah Kabupaten Bantul harus dikendalikan menggunakan metode pengendalian akses yang memadai;
   b. pemberian hak akses dikelola secara formal pada seluruh siklusnya, mulai dari proses pengajuan, persetujuan, serta pencabutan, serta dilaksanakan oleh para pihak terkait sesuai jenjang kewenangannya;
   c. Pengguna yang mengakses Sistem Informasi dalam lingkungan Pemerintah Daerah Kabupaten Bantul diharuskan untuk mengotentikasi dirinya dengan menggunakan kombinasi user ID dan informasi otentikasi pribadi seperti *password* atau PIN;
   d. pengembangan aturan pemberian akses perlu mempertimbangkan:
      1) klasifikasi dari informasi;

2) kritikalitas dari aset yang digunakan untuk mendukung operasional bisnis;
3) prasyarat perundang-undangan, kontraktual, serta keamanan yang relevan; dan
4) didasarkan atas prinsip need to know dan need to use, yaitu disesuaikan dengan kebutuhan pekerjaan dan operasional dalam lingkungan Pemerintah Daerah Kabupaten Bantul;

e. Aturan pemberian akses harus dikembangkan dan didokumentasikan oleh setiap pemilik sistem dalam bentuk daftar atau *matriks akses*;
f. peninjauan terhadap aturan pemberian akses harus dilakukan oleh pemilik aset/sistem secara berkala tergantung tingkat kritikalitas sistem tersebut;
g. peninjauan terhadap hak akses Pengguna harus didokumentasikan secara formal; dan
h. setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan cara menyesuaikan atau mencabut hak akses yang menyimpang.

3.2 Pengendalian akses jaringan di lingkungan Perangkat Daerah meliputi:

a. penggunaan layanan jaringan *(network services)* hanya diperbolehkan secara terbatas, sesuai kebutuhan ketugasan dan kepentingan Perangkat Daerah, layanan lainnya yang tidak diperlukan harus dinonaktifkan;
b. jaringan komunikasi dalam lingkungan Perangkat Daerah harus dipisahkan kedalam *domain* jaringan yang terpisah sesuai dengan kebutuhan bisnis dan operasional, dalam rangka untuk mengamankan jaringan internal Perangkat Daerah dan aset di jaringan tersebut;
c. akses secara *remote* ke jaringan internal Perangkat Daerah dari jaringan publik harus sangat dibatasi baik dari perangkat yang digunakan maupun waktu untuk kebutuhan *troubleshooting* dan harus dilakukan melalui secure channel, antara lain dengan menggunakan teknologi *VPN*; dan
d. pemberian akses Pengguna terhadap jaringan, baik *LAN* maupun W*AN*, dilakukan melalui mekanisme formal.

3.3 Pengelolaan akses terhadap Pengguna di Perangkat Daerah harus memenuhi ketentuan sebagai berikut:

a. pemilik Aset Informasi harus memiliki manajemen identitas Pengguna yang mencakup proses pendaftaran dan terminasi Pengguna yang didalamnya termasuk:
   1) identitas Pengguna *(user account)* harus unik, melekat ke setiap individu tunggal, sehingga setiap tindakan Pengguna dapat dipertanggung jawabkan;
   2) tidak diijinkan menggunakan satu identitas Pengguna yang digunakan secara bersama-sama oleh lebih dari 1 (satu) individu, kecuali untuk tujuan tertentu yang sebelumnya harus mendapatkan persetujuan dari pihak berwenang; dan
   3) memastikan secara berkala bahwa tidak ada identitas Pengguna yang terduplikasi atau redundan sehingga seluruh identitas Pengguna aktif adalah sesuai dengan pegawai Perangkat Daerah aktif.
b. pendaftaran, modifikasi, dan pencabutan hak akses Pengguna mencakup proses pembuatan user ID, memberikan hak akses kepada user ID serta mencabut hak akses dan user ID.
c. pendaftaran, modifikasi dan pencabutan hak akses Pengguna harus disetujui oleh atasan dari Pengguna yang memohon hak akses tersebut dan pemilik informasi dan/atau sistem. Persetujuan tersebut harus diberikan sesuai dengan aturan pemberian akses.
d. identitas Pengguna harus diotorisasi secara formal oleh pejabat berwenang pada pemilik Aset Informasi. Akses atas sistem dan aplikasi hanya dapat diaktifkan jika proses otorisasi telah selesai.
e. identitas Pengguna pada sistem, seperti *user ID*, harus bersifat unik untuk memungkinkan mengidentifikasi dan meminta pertanggungjawaban Pengguna.
f. pemberian informasi otentikasi suatu Pengguna yang bersifat rahasia harus dilakukan melalui proses formal yang mencakup:
   1) informasi otentikasi perdana yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana Pengguna wajib menggantinya pada kesempatan pertama mengakses sistem atau aplikasi; dan
   2) informasi otentikasi bawaan *(default)* dari penyedia barang/jasa harus segera diganti pada saat instalasi sistem atau aplikasi.

g. pemilik aset harus melakukan tinjauan secara berkala atas seluruh hak akses Pengguna secara berkala, dengan tambahan tinjauan insidental yang dilakukan pada saat:
   1) terjadinya proses kepegawaian, seperti promosi, mutasi, terminasi; dan
   2) terjadinya perubahan struktur organisasi.
h. hak akses khusus (*privileged access rights*) dari Sistem Informasi dalam lingkungan Perangkat Daerah, seperti administrator, *root*, hak akses untuk memodifikasi database atau hak akses untuk membuat, memodifikasi, atau mencabut Pengguna dalam sistem aplikasi, harus sangat dibatasi kepada personil yang terotorisasi.
i. Hak akses khusus harus disetujui dan didokumentasikan secara formal.
j. Alokasi dari hak akses khusus harus ditinjau secara berkala dan setiap terdapat perubahan dalam status penggunaan akses tersebut.
k. Setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan menyesuaikan atau menghapus hak akses khusus yang menyimpang.
l. Apabila memungkinkan, hak akses khusus harus dialokasikan secara individual dan tidak dibagikan (*share*). Hal ini dilakukan untuk menjamin akuntabilitas dari Pengguna khusus.
m. apabila hak akses khusus tidak bisa dialokasikan secara individual, kontrol tambahan seperti *dual custody*, harus diimplementasikan untuk menghindari penyalahgunaan.
n. jejak audit (log) untuk hak akses khusus pada Sistem Informasi dalam lingkungan Pemerintah Daerah Kabupaten Bantul harus diaktifkan.

3.4 Setiap Pengguna harus mempunyai tanggung jawab dalam penggunaan User ID dan password yaitu:
a. Pengguna harus menjaga kerahasiaan dan keamanan *password* pribadi atau kelompok serta informasi otentikasi rahasia lainnya;
b. Pengguna harus segera mengganti informasi otentikasi rahasia jika terindikasi bahwa informasi tersebut telah diketahui oleh orang lain;
c. *password* yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana Pengguna wajib menggantinya pada kesempatan pertama pada saat mengakses sistem atau aplikasi;
d. *Password* untuk mengakses Sistem Informasi dalam lingkungan Perangkat Daerah harus memiliki karakteristik sebagai berikut:

1) memiliki panjang minimum 8 karakter;
2) mengandung kombinasi huruf besar, huruf kecil, nomor, dan tanda baca;
3) tidak terdiri dari kata atau nomor yang mudah ditebak seperti password, admin, 12345678 atau abc123; dan
4) tidak terdiri dari informasi pribadi seperti ulang tahun Pengguna, nama perusahaan, atau nama Pengguna;

e. *password* untuk mengakses Sistem Informasi dalam lingkungan Pemerintah Daerah Kabupaten Bantul harus diganti paling sedikit setiap 6 (Enam) bulan sekali;

f. prosedur login dari sistem harus menjamin keamanan dari password dengan cara:
1) tidak menampilkan password yang dimasukkan; dan
2) tidak menyediakan pesan bantuan pada saat proses login yang dapat membantu Pengguna yang tidak berwenang;

g. Pengguna wajib menggunakan kata sandi yang berbeda untuk keperluan ketugasan dan pribadi.

3.5 pengendalian akses sistem dan aplikasi yang dikelola oleh Perangkat Daerah meliputi:

a. pemilik Aset Informasi harus memastikan bahwa sistem dan aplikasi dibawah pengelolaannya memiliki fasilitas manajemen hak akses Pengguna, manajemen kata sandi yang baik, serta mekanisme otentikasi Pengguna yang aman;

b. fasilitas manajemen hak akses Pengguna harus mampu membatasi akses informasi sesuai ketugasannya *(role based access control)*;

c. fasilitas manajemen kata sandi harus memastikan dihasilkannya kata sandi yang berkualitas yaitu:
1) menegakkan akuntabilitas Pengguna melalui penggunaan identitas Pengguna tunggal untuk setiap individu;
2) memberikan fasilitas penggantian kata sandi mandiri; membantu memberikan rekomendasi kata sandi yang berkualitas;
3) mewajibkan Pengguna untuk mengganti kata sandi pada saat pertama kali login;
4) mewajibkan Pengguna untuk mengganti kata sandi secara berkala;

5) menyimpan riwayat kata sandi Pengguna dan mencegah agar Pengguna tidak menggunakan kata sandi yang sebelumnya telah digunakan;
6) tidak menampilkan kata sandi saat sedang dientrikan; dan
7) kata sandi disimpan dalam bentuk terlindungi (dienkripsi), demikian juga pada saat kata sandi ditransmisikan.

d. mekanisme otentikasi Pengguna perlu dirancang agar meminimalkan peluang terjadinya akses yang tidak sah, yaitu:
1) kata sandi tidak ditransmisikan melalui jaringan secara *plaintext*;
2) memiliki mekanisme penguncian sistem sementara sebagai perlindungan terhadap *brute force attacks*;
3) adanya pencatatan terhadap seluruh upaya otentikasi yang sukses dan gagal; dan
4) adanya pembatasan jumlah akses Pengguna yang sama secara simultan.

e. penggunaan program *utility* khusus dalam operasional sistem di lingkungan Perangkat Daerah harus mempertimbangkan keamanan sebagai berikut yaitu penggunaan program *utility* khusus seperti *registry cleaner* atau system monitoring yang dapat mengambil alih kendali sistem/aplikasi atau mendapatkan hak akses khusus pada sistem/aplikasi harus sangat dibatasi berdasarkan kebutuhan operasional Pengguna.

f. Perangkat Daerah yang mengelola aplikasi harus memastikan bahwa *source code* dikelola dan disimpan secara memadai baik yang dikembangkan oleh internal Perangkat Daerah maupun yang dikembangkan oleh penyedia jasa aplikasi.

g. Apabila *source code* dari penyedia jasa aplikasi tidak dapat diserahkan kepada pengelola aplikasi, Perangkat Daerah Bersama penyedia jasa aplikasi tersebut harus mempertimbangkan *escrow agreement* untuk memastikan kelangsungan operasional sistem aplikasi jika ada pengembangan selanjutnya.

h. Pengendalian terhadap akses ke *source code* aplikasi sebagai berikut:
1. untuk sistem aplikasi yang dikembangkan secara internal dan/atau dibeli dengan source code, pengendalian akses harus diimplementasikan untuk mencegah akses tanpa izin ke *source code* tersebut.

2. pengendalian tersebut mencakup:
    - tidak melakukan perubahan source code pada sistem operasional;
    - menyimpan *source code* pada lokasi fisik yang aman dari ancaman akses tanpa izin maupun ancaman kerusakan karena kondisi lingkungan;
    - membatasi akses secara fisik maupun logical ke *source code* program hanya kepada pengembang dan personil yang berwenang; dan
    - mengimplementasikan metode *versioning* dan proses manajemen perubahan untuk menjamin integritas dari source code aplikasi.

BAB VIII
MANAJEMEN KRIPTOGRAFI

1. **Tujuan**

   Tujuan dari kebijakan terkait teknologi kriptografi adalah untuk memastikan penggunaan teknologi kriptografi yang sesuai dan efektif untuk melindungi kerahasiaan, keaslian, dan/atau integritas dari informasi dalam lingkungan Pemerintah Daerah Kabupaten Bantul.

2. **Ruang Lingkup**

   Ruang Lingkup kebijakan terkait teknologi kriptografi adalah penggunaan teknologi kriptografi dalam pengolahan dan penyimpanan informasi di lingkungan Pemerintah Daerah Kabupaten Bantul.

3. **Kebijakan**

   1) kontrol kriptografi dapat digunakan untuk menjamin kerahasiaan dan integritas dari informasi sensitif di lingkungan Perangkat Daerah.
   2) kontrol kriptografi dapat mencakup namun tidak terbatas pada:
      a. enkripsi informasi dan jaringan komunikasi;
      b. pemeriksaan integritas informasi, seperti *hashing*;
      c. otentikasi identitas; dan
      d. digital *signatures*;
   3) implementasi dari kontrol kriptografi harus mempertimbangkan klasifikasi dari informasi yang akan diamankan.
   4) pemilihan kontrol kriptografi harus mempertimbangkan:
      a. jenis dari kontrol kriptografi;
      b. kekuatan dari algoritma kriptografi; dan
      c. panjang dari kunci kriptografi.
   5) implementasi dari kontrol kriptografi harus secara berkala ditinjau untuk memastikan kecukupan dan kesesuaian dari control tersebut dalam mengamankan kerahasiaan dan integritas dari informasi.
   6) pengelolaan dari kunci kriptografi harus dikendalikan secara ketat dan dibatasi hanya pada personil yang terotorisasi.
   7) pengelolaan dari kunci kriptografi didasarkan pada prinsip dua pemilik *(dual custody)* untuk mengurangi risiko penyalahgunaan

BAB IX
MANAJEMEN KEAMANAN FISIK DAN LINGKUNGAN

1. **Tujuan**

   Tujuan dari kebijakan keamanan fisik dan lingkungan adalah untuk:

   a. Menghindari terjadinya akses fisik secara ilegal, penghancuran, atau campur tangan dari pihak lain terhadap Aset Informasi di lingkungan Pemerintah Kabupaten Bantul;
   b. Menghindari terjadinya kehilangan, kerusakan, pencurian, persekongkolan terhadap aset dan informasi, serta gangguan lainnya akibat aktivitas yang dilakukan oleh Pemerintah Kabupaten Bantul.

2. **Ruang Lingkup**

   Ruang lingkup fisik dan lingkungan meliputi wilayah kerja dan peralatan kerja.

   a. Pengamanan wilayah kerja termasuk batasan keamanan fisik, pengendalian akses fisik, keamanan kantor, ruangan, dan fasilitas, perlindungan terhadap ancaman dari lingkungan eksternal, area akses publik, pengantaran, dan penerimaan, aktivitas pekerjaan di area rahasia;
   b. Pengamanan peralatan kerja termasuk penempatan peralatan dan perlindungannya, fasilitas pendukung, keamanan instalasi kabel, pemeliharaan peralatan, keamanan peralatan yang berada di luar lingkungan Pemerintah Kabupaten Bantul, keamanan penghapusan dan penggunaan ulang peralatan atau media informasi, pemindahan Aset Informasi, seperti Data Center, *disaster recovery center* atau ruang arsip.

3. **Kebijakan**

   1) Setiap area yang didalamnya terdapat informasi dan fasilitas pengolahan informasi Perangkat Daerah harus dilindungi dengan menerapkan pengamanan fisik pada perimeter area tersebut.
   2) Setiap area harus merupakan akses terbatas, dimana akses masuk hanya diberikan bagi personil yang telah mendapatkan otorisasi. Mekanisme pembatasan ini dapat dilakukan aturan penerimaan tamu yang diterapkan berdasarkan kritikalitas area tersebut.

3) Untuk area Data Center, *disaster recovery center* dan ruang arsip Perangkat Daerah harus dilindungi dengan menerapkan pengamanan fisik pada perimeter area tersebut dengan kriteria:
   a. konstruksi dinding, atap, dan lantai yang kuat;
   b. pintu akses menuju area harus dilengkapi dengan mekanisme kontrol akses seperti: *access door lock*;
   c. pintu dan jendela harus senantiasa dalam kondisi terkunci, khususnya pada saat tanpa penjagaan;
   d. perangkat CCTV perlu terpasang pada sisi eksterior dan interior area;
   e. tidak diperbolehkan menyimpan bahan-bahan berbahaya yang mudah terbakar;
   f. area bongkar muat atau penerimaan barang harus diamankan dan dipantau untuk mencegah akses tanpa izin ke Data Center, disaster recovery center dan ruang arsip Pemerintah Daerah Kabupaten Bantul; dan
   g. pengiriman barang harus dilaporkan dan diperiksa sebelum barang tersebut dapat dipindahkan dari area bongkar muat atau penerimaan barang ke Data Center, *disaster recovery center* dan ruang arsip Pemerintah Daerah Kabupaten Bantul.
4) Pengendalian akses pengunjung ke dalam area di lingkungan Perangkat Daerah harus memperhatikan keamanan fisik yang meliputi:
   a. kunjungan ke dalam area tersebut harus disetujui secara formal oleh pengelolaan area tersebut;
   b. selama kunjungan di dalam area tersebut, pengunjung harus senantiasa didampingi oleh petugas yang telah mendapatkan otorisasi;
   c. kartu identitas pengunjung perlu diverifikasi, disimpan oleh petugas selama kunjungan, dan dikembalikan sesudah selesai kunjungan; dan
   d. setiap pengunjung ke dalam area harus tercatat, mencakup jam masuk dan keluar, serta selalu dimonitor kesesuaiannya dengan rekaman *CCTV*.

5) Perangkat Daerah harus memperhatikan aspek pengamanan terhadap perangkat yang digunakan melalui:
   a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya pencurian, akses oleh pihak yang tidak berwenang, kebakaran, air, debu, dan sebagainya;
   b. seluruh perangkat di dalam area harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang berwenang untuk menjamin keberlangsungan efektivitas fungsionalnya;
   c. pemeliharaan yang dilakukan oleh pihak kedua, harus dilaksanakan sesuai dengan kesepakatan tingkat layanan *(Service Level Agreement/ SLA)* yang menjabarkan tingkat pemeliharaan dan kinerja yang harus dipenuhi pihak kedua;
   d. bagi pemeliharaan yang tidak dapat dilakukan di lokasi kantor Perangkat Daerah, maka informasi rahasia dan kritikal yang tersimpan dalam peralatan tersebut harus dipindahkan terlebih dahulu;
   e. pemeliharaan perangkat yang mengharuskan dibawa dari luar area harus atas persetujuan pejabat berwenang;
   f. peralatan pengolahan dan penyimpanan informasi yang tidak digunakan lagi oleh Pemerintah Daerah Kabupaten Bantul, baik karena rusak, diganti, atau karena sebab lainnya harus dipastikan tidak lagi menyimpan informasi sensitif dan kritikal; dan
   g. media penyimpan informasi yang sudah tidak digunakan lagi harus dihancurkan, atau dihapus isinya agar tidak bisa dibaca dan digunakan lagi oleh pihak yang tidak berwenang.
6) Khusus pengamanan area fisik di Data Center harus mempertimbangkan hal-hal sebagai berikut:
   a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya kebakaran, kebocoran, debu, dan sebagainya;
   b. seluruh perangkat di dalam Data Center harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang kompeten dan berwenang sesuai dengan rekomendasi dari pembuat perangkat tersebut;
   c. Data Center harus dilengkapi dengan UPS, generator listrik cadangan, perangkat pemadam kebakaran, dan diusahakan terdapat perlindungan kejut listrik (petir, tegangan tidak stabil);

d. Data Center dan *disaster recovery center* dilengkapi dengan sistem sensor deteksi asap, air, suhu dan kelembaban, yang dapat terpantau;
e. parameter temperatur dan kelembaban berikut perlu dijaga untuk data center meliputi:
    1) temperatur antara 18°-26° (delapan belas derajat sampai dengan dua puluh enam derajat) celcius;
    2) kelembaban (rh) antara 40%-60% (empat puluh persen sampai dengan enam puluh persen).
f. kabel listrik dan jaringan telekomunikasi yang membawa data atau mendukung layanan Sistem Informasi harus dilindungi dari penyambungan yang tidak sah (penyadapan) atau kerusakan.

BAB X
MANAJEMEN KEAMANAN OPERASIONAL SISTEM INFORMASI

1. **Tujuan**

   Tujuan dari kebijakan keamanan operasional Sistem Informasi adalah untuk:

   a. memastikan pengoperasian aset pengolahan dan penyimpanan informasi di Pemerintah Daerah Kabupaten Bantul secara benar dan aman;
   b. memastikan terlindunginya Aset Informasi beserta aset pengolahan dan penyimpanan informasi di Pemerintah Daerah Kabupaten Bantul dari ancaman *malware*;
   c. melindungi terjadinya kehilangan atas Aset Informasi;
   d. tersedianya catatan (log) atas aktivitas Sistem Informasi sebagai barang bukti; dan
   e. mencegah terjadinya eksploitasi atas kelemahan Sistem Informasi pada Pemerintah Daerah Kabupaten Bantul.

2. **Ruang Lingkup**

   Ruang lingkup dari kebijakan keamanan operasional Sistem Informasi adalah pengoperasian aset pengolahan dan penyimpanan informasi di lingkungan Pemerintah Daerah Kabupaten Bantul.

3. **Kebijakan**

   a. Aktivitas operasional terkait fasilitas pengolahan informasi serta fasilitas komunikasi harus memiliki prosedur yang terdokumentasi dengan baik;
   b. Prosedur operasional tersebut harus tersedia bagi Pengguna yang memerlukannya;
   c. Seluruh perubahan pada fasilitas pengolahan informasi yang dapat berimplikasi pada keamanan informasi, perlu diperlakukan secara terkendali mencakup antara lain:
      1) menyusun perencanaan mengenai perubahan yang mungkin terjadi serta melakukan pengujian terkait terpenuhinya persyaratan keamanan;
      2) melakukan kajian atas implikasi keamanan informasi yang mungkin terjadi;
      3) mengajukan persetujuan secara formal atas perubahan yang akan dilakukan; dan

4) mencatat seluruh perubahan yang telah dilakukan.

d. Kinerja dan utilisasi atas fasilitas pengolahan informasi harus senantiasa dipantau dengan alat bantu peringatan dini, dioptimalkan pemanfaatannya, serta diproyeksikan kebutuhan kapasitasnya untuk masa yang akan datang.

e. Untuk mengurangi risiko perubahan tanpa izin atau penyalahgunaan hak akses, pemisahan fasilitas pengembangan, pengujian, dan operasional harus dilakukan.

f. Setiap Sistem Informasi di lingkungan Perangkat Daerah harus terlindungi dari *malware* secara memadai melalui:
   1) instalasi dari perangkat lunak antivirus pada Sistem Informasi;
   2) memblok akses ke website yang dapat menimbulkan ancaman kepada Sistem Informasi;
   3) program peningkatan kesadaran bagi personil organisasi untuk menangani ancaman malware; dan
   4) setiap insiden terkait dengan malware harus dilaporkan kepada administrator sistem dan dikategorikan sebagai insiden keamanan informasi.

g. Seluruh Aset Informasi yang berada di dalam fasilitas pengolahan informasi wajib dilakukan backup, dengan persyaratan berikut:
   1) backup mencakup aplikasi, database, dan system image;
   2) frekuensi backup dilakukan secara harian, bulanan, dan tahunan;
   3) salinan backup harus disimpan secara aman sesuai dengan periode retensi. Periode retensi backup adalah 1 (satu) tahun dimana:
      - backup harian disimpan selama 31 (tiga puluh satu) hari; dan
      - backup bulanan disimpan selama 12 (dua belas) bulan.

h. seluruh hasil *backup* harus dilakukan uji *restore* secara berkala;

i. media backup disimpan pada perangkat *storage* yang terpisah dari perangkat pengolahan informasi utama;

j. backup merupakan tanggung jawab pengelola Data Center, sedangkan pengujian *restore* merupakan tanggung jawab pemilik Aset Informasi;

k. Sistem harus dikonfigurasi untuk melakukan pencatatan *(logging)* atas seluruh aktivitas Pengguna, jaringan, sistem, aplikasi, *error* yang terjadi *(exceptions)*. Pemilik Aset Informasi harus menganalisis log terkait pola-pola penggunaan yang tidak wajar.

l. Fasilitas pencatatan log dan informasi log yang dicatat harus dilindungi dari penghapusan dan akses oleh pihak yang tidak berwenang.

m. semua fasilitas pemrosesan informasi yang terhubung ke jaringan internal Perangkat Daerah harus disinkronisasi dengan sumber waktu yang akurat dan telah disepakati.
n. Proses dan prosedur untuk mengendalikan instalasi perangkat lunak pada sistem operasional harus ditetapkan dan diimplementasikan untuk memastikan terjaganya kerahasiaan, integritas, dan ketersediaan informasi.
o. Instalasi *software* harus dilakukan oleh administrator sistem yang relevan.
p. Pemilik Aset Informasi wajib melakukan upaya-upaya identifikasi atas kelemahan teknis *(vulnerabilities)* dari seluruh Aset Informasi dibawah pengelolaannya, serta melakukan tindakan pengendalian yang sesuai untuk meminimalkan risiko atas hilangnya Aset Informasi. Tindakan pengendalian dapat berupa penonaktifan fitur tertentu, perbaikan/*upgrade* sistem, aplikasi, atau patching.
q. Setiap Sistem Informasi di lingkungan Perangkat Daerah dapat dilakukan proses audit yang mencakup proses verifikasi terhadap Sistem Informasi dan/atau informasi Perangkat Daerah dengan mempertimbangkan sebagai berikut:
    1) harus direncanakan dan dikelola dengan baik untuk meminimalisasi gangguan terhadap proses bisnis;
    2) setiap proses audit yang membutuhkan akses kepada Sistem Informasi dan/atau informasi Perangkat Daerah harus disetujui oleh pemilik dari sistem dan/atau informasi tersebut;
    3) hak akses untuk kebutuhan audit harus dibatasi hanya hak akses *read only*; dan
    4) instalasi dari tools yang digunakan untuk proses audit hanya dapat dilakukan oleh personil yang berwenang yaitu administrator jaringan dan sistem Teknologi Informasi di Perangkat Daerah, dan harus segera dihapus setelah proses audit telah selesai dilakukan.

BAB XI
KEAMANAN KOMUNIKASI

1. **Tujuan**

   Tujuan dari kebijakan keamanan komunikasi adalah untuk:

   a. Memastikan perlindungan atas informasi pada jaringan komputer beserta fasilitas pendukung pengolahan informasi;
   b. Menjaga keamanan informasi yang dipertukarkan, baik di dalam Perangkat Daerah maupun antar Perangkat Daerah eksternal.

2. **Ruang Lingkup**

   Ruang lingkup dari kebijakan keamanan komunikasi adalah untuk:

   a. Pengendalian jaringan;
   b. Keamanan layanan jaringan;
   c. Pemisahan jaringan; dan
   d. Pertukaran informasi.

3. **Kebijakan**

   a. Jaringan internal Perangkat Daerah harus diamankan untuk menjamin:
      1) pencegahan akses tanpa izin ke jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan;
      2) keamanan dari informasi milik organisasi yang dikirimkan melalui jaringan; dan
      3) integritas dan ketersediaan dari layanan jaringan organisasi.
   b. Tugas dan tanggung jawab untuk pengelolaan jaringan dan keamanan harus dialokasikan dan apabila memungkinkan dipisahkan dari penanggung jawab operasional sistem aplikasi dan Data Center.
   c. Konfigurasi dari jaringan, perangkat aktif, dan perangkat keamanan jaringan harus ditinjau secara berkala untuk:
      1) memastikan kesesuaian dengan kondisi terkini; dan
      2) mengidentifikasi kerawanan pada jaringan, layanan jaringan, dan
      3) fasilitas pemrosesan informasi dalam jaringan.
   d. Jaringan internal Perangkat Daerah harus dipisahkan dari jaringan eksternal dengan menggunakan *security gateway* atau *firewall* dan harus dikonfigurasikan untuk:
      1) memfilter *traffic* tanpa izin maupun *traffic* yang mencurigakan; dan
      2) apabila memungkinkan memfilter dan mencegah infeksi *malware* ke jaringan internal.

e. Koneksi ke *security gateway* atau *firewall* harus diotentikasikan, diotorisasi dan diamankan dengan metode pengamanan yang sesuai, misalnya dengan *virtual private network (VPN*), *secure shell (SSH)* atau metode kriptografi.
f. Kebijakan dan log firewall harus ditinjau paling sedikit 1 (satu) kali dalam 6 (enam) bulan.
g. Koneksi eksternal harus diputuskan secara otomatis setelah tidak aktif selama 5 (lima) menit.
h. Akses dari jaringan eksternal yang dilakukan oleh vendor pihak ketiga hanya dapat diberikan untuk kebutuhan *troubleshooting* dan harus secara formal disetujui dan didokumentasikan dan harus dibatasi waktunya sesuai dengan kebutuhan dari akses.
i. Jaringan internal perusahaan harus disegmentasi baik secara fisik maupun *logical* untuk meningkatkan keamanan dan untuk mengendalikan akses dan *traffic* jaringan berdasarkan kritikalitas dari sistem dalam jaringan Perangkat Daerah.
j. Segmentasi jaringan harus ditinjau paling sedikit 1 (satu) kali dalam 6 (Enam) bulan untuk menjamin kesesuaian dengan prasyarat keamanan terkini.
k. *Routing* jaringan harus dilakukan berdasarkan pengendalian terhadap alamat sumber dan tujuan.
l. Tanggung jawab untuk merubah *routing* jaringan hanya diberikan kepada administrator jaringan yang diberi izin.
m. Aturan untuk *routing* harus ditinjau paling tidak 1 (satu) kali dalam 6 (Enam) bulan untuk mendeteksi dan mengoreksi adanya kesalahan atau *routing* tanpa otorisasi.
n. Perangkat jaringan harus ditempatkan pada lokasi yang aman untuk menghindari akses tanpa izin dan ancaman fisik maupun lingkungan.
o. Akses, baik fisik maupun logical ke perangkat jaringan harus dibatasi untuk tujuan administrasi dan pemeliharaan jaringan.
p. *Port* dan layanan jaringan, baik fisik maupun logical, yang tidak digunakan tidak boleh diaktifkan.
q. Akses ke *port* yang digunakan untuk kebutuhan *diagnostic* dan konfigurasi perangkat jaringan dan keamanan jaringan, seperti *console port*, harus sangat dibatasi dan diberikan kepada:
    a. administrator jaringan dan keamanan jaringan Perangkat Daerah;
    b. pihak ketiga yang telah disetujui dan bekerja untuk kepentingan Perangkat Daerah; dan

c. aplikasi monitoring jaringan dan keamanan jaringan yang telah disetujui.

r. Semua perangkat jaringan harus dapat diidentifikasi secara fisik maupun logical dengan penamaan yang disepakati dan konsisten.

s. Perangkat jaringan yang dimiliki oleh pihak eksternal harus secara memadai dipisahkan dari perangkat jaringan milik Perangkat Daerah.

t. Mekanisme keamanan, tingkat layanan, dan prasyarat lain untuk semua layanan jaringan harus diidentifikasi dan dimasukkan kedalam perjanjian layanan jaringan.

u. Akses ke layanan jaringan Perangkat Daerah hanya diberikan kepada personil yang terotorisasi berdasarkan prinsip *need to have*.

v. Penggunaan pihak kedua penyedia layanan jaringan harus dimonitor untuk menjamin kesesuaian dengan prasyarat keamanan Perangkat Daerah.

w. Layanan jaringan organisasi harus diamankan menggunakan metode yang dapat mencakup metode otentikasi atau metode kriptografi yang kuat untuk menjamin keamanan dari pengiriman informasi menggunakan jaringan dan layanan jaringan.

x. Terkait aspek pertukaran informasi melalui fasilitas jaringan komunikasi, Perangkat Daerah harus memperhatikan perjanjian kerahasiaan merupakan perikatan formal antara pemilik Aset Informasi dengan penerima informasi, yang ketentuan di dalamnya memuat:

   1) pemberian izin penggunaan informasi dari pemilik Aset Informasi kepada penerima informasi untuk keperluan dan periode waktu yang spesifik, dimana pihak penerima informasi wajib menjaga kerahasiaan informasi serta mengupayakan pencegahan terjadinya kebocoran atau penyebaran informasi secara tidak sah;
   2) hak dari pemilik Aset Informasi untuk melakukan audit dan pemantauan aktivitas penerima informasi berkaitan dengan penggunaan informasi sensitif; dan
   3) konsekuensi yang harus ditanggung penerima informasi apabila terjadi pelanggaran atas perjanjian kerahasiaan

BAB XII
AKUISISI, PENGEMBANGAN DAN PEMELIHARAAN SISTEM

1. **Tujuan**

   Tujuan dari kebijakan akuisisi, pengembangan, dan pemeliharaan sistem adalah untuk:

   a. Memastikan keamanan informasi sebagai bagian tak terpisahkan dari siklus hidup *(lifecycle*) Sistem Informasi. Termasuk persyaratan untuk Sistem Informasi yang menyediakan layanan melalui jaringan publik
   b. Memastikan keamanan informasi didesain dan diimplementasikan dalam siklus hidup *(lifecycle)* pengembangan dari Sistem Informasi.
   c. Memastikan perlindungan terhadap penggunaan data untuk pengujian.

2. **Ruang Lingkup**

   Ruang lingkup dari kebijakan keamanan komunikasi adalah untuk:

   1. Persyaratan keamanan Sistem Informasi;
   2. Keamanan dalam proses pengembangan dan support; dan
   3. Data pengujian.

3. **Kebijakan**

   a. Perangkat Daerah harus menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi yang relevan sebelum pengembangan, perluasan, atau pengadaan Sistem Informasi baru.
   b. Persyaratan keamanan harus diidentifikasi secara jelas di dalam dokumen persyaratan dan spesifikasi perangkat lunak *(software).*
   c. Spesifikasi ini harus disetujui oleh pemilik informasi, pemilik proses bisnis dan pengembang sistem, sebelum fase pengkodean *(coding)* dalam pengembangan sistem.
   d. Informasi yang digunakan oleh aplikasi Perangkat Daerah yang ditransmisikan melalui jaringan publik *(internet)* harus diamankan dari aktivitas penipuan, kemungkinan adanya perselisihan kontrak, dan pengungkapan dan/atau perubahan informasi tanpa izin.
   e. Pengamanan informasi terhadap informasi yang ditransmisikan melalui Sistem Informasi yang digunakan dapat mencakup namun tidak terbatas pada:
      1) proses otentikasi dan otorisasi terhadap Pengguna aplikasi;
      2) perlindungan untuk memastikan kerahasiaan dan integritas informasi yang dipertukarkan melalui jaringan publik;

3) perlindungan terhadap session transaksi untuk menghindari duplikasi dan/atau modifikasi; dan
4) mengamankan jalur komunikasi antara pihak-pihak yang terlibat

f. Keamanan dalam proses pengembangan dan dukungan yang perlu dipertimbangkan oleh Perangkat Daerah meliputi aturan untuk pengembangan sistem harus ditetapkan dan diimplementasikan untuk proses pengembangan sistem di Perangkat Daerah yang mencakup:
1) pengamanan dari lingkungan pengembangan, seperti pemisahan lingkungan pengembangan baik secara fisik dan/atau logical, pengendalian akses, pengelolaan perubahan;
2) panduan *secure coding*;
3) pengendalian versi aplikasi;
4) penyimpanan dari source code; dan
5) metode pengujian untuk mengidentifikasi dan memperbaiki vulnerability.

g. Perubahan terhadap sistem selama siklus pengembangan sistem harus dikendalikan melalui proses manajemen perubahan yang berlaku di Perangkat Daerah;

h. Apabila *platform* operasional, misalnya sistem operasi, database dan/atau *middleware*, dari Sistem Informasi Perangkat Daerah mengalami perubahan, aplikasi kritikal Perangkat Daerah harus ditinjau dan diuji untuk memastikan tidak ada dampak buruk terhadap operasional dan keamanan organisasi;

i. Perangkat Daerah harus menetapkan lingkungan pengembangan yang aman untuk pengembangan dan integrasi sistem Perangkat Daerah. Hal ini dapat mencakup namun tidak terbatas pada:
1) pemisahan lingkungan pengembangan baik secara fisik dan/atau *logical;*
2) pengendalian akses; dan
3) perpindahan data dari dan ke lingkungan pengembangan;

j. Perangkat Daerah harus mengawasi aktivitas pengembangan sistem yang dialihdayakan *(outsourced).* Hal ini dapat mencakup:
1) perjanjian terkait lisensi dan kepemilikan sistem;
2) pengujian penerimaan sistem untuk menguji kualitas dan akurasi dari sistem;
3) prasyarat dokumentasi untuk sistem;
4) perjanjian dengan pihak ketiga sebagai penjamin;

5) hak untuk melakukan audit proses pengembangan dan kontrol yang diimplementasikan oleh vendor.

k. Pengujian dari fitur keamanan sistem harus dilakukan pada saat pengembangan Sistem Informasi Perangkat Daerah;

l. Pengujian ini dilakukan berdasarkan prasyarat keamanan sistem yang telah ditetapkan;

m. Kriteria dan jadwal untuk pengujian penerimaan sistem harus ditetapkan untuk Sistem Informasi baru, *upgrade*, dan versi baru dari Sistem Informasi Perangkat Daerah;

n. Pengujian penerimaan sistem harus dilakukan sesuai dengan kriteria dan jadwal yang ditetapkan.

o. Pengamanan terhadap data hasil pengujian perlu diperhatikan sebagai berikut:

1) data untuk pengujian sistem harus dipilih secara hati-hati untuk menghindari pengungkapan atau perubahan informasi sensitif oleh pihak yang tidak berhak, serta melindungi dari kemungkinan kerusakan dan kehilangan informasi;

2) *masking data* harus dilakukan apabila data operasional yang sensitif digunakan untuk keperluan pengujian; dan

3) data operasional yang digunakan untuk keperluan pengujian harus dihapus segera setelah proses pengujian telah selesai dilaksanakan.

BAB XIII
PENANGANAN INSIDEN KEAMANAN INFORMASI

1. Tujuan

Tujuan dari kebijakan penanganan insiden keamanan informasi adalah untuk memastikan adanya pendekatan yang konsisten dan efektif atas penanganan insiden keamanan informasi.

2. Ruang Lingkup

Ruang lingkup Perangkat Daerah dari kebijakan penanganan insiden keamanan informasi adalah:

a. Tanggung jawab dan prosedur;
b. Pelaporan atas kejadian insiden keamanan informasi; dan
c. Pelaporan atas kelemahan keamanan informasi.
d. Tindakan pemulihan/ *Recovery System*

3. Kebijakan

a. Kejadian keamanan informasi adalah sebuah kejadian pada sistem, layanan ataupun jaringan yang dapat mengindikasikan adanya pelanggaran keamanan informasi atau kegagalan keamanan atau kejadian yang mungkin memiliki keterkaitan dengan keamanan informasi.
b. Kelemahan keamanan informasi adalah sebuah kelemahan yang teridentifikasi pada sistem, layanan atau jaringan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab dan dapat menyebabkan pelanggaran terhadap kebijakan keamanan informasi.
c. Insiden keamanan informasi adalah kejadian keamanan informasi yang tidak diinginkan dan tidak diperkirakan dimana kejadian tersebut menimbulkan gangguan terhadap operasional bisnis dan mengancam keamanan informasi.
d. Guna memastikan proses penanganan insiden yang responsive dan efektif, perlu dikembangkan berbagai prosedur yang mencakup:
    1) perencanaan dan persiapan penanganan insiden;
    2) pemantauan, analisis, dan pelaporan atas insiden;
    3) pencatatan atas aktivitas penanganan insiden;
    4) penanganan bukti forensik;
    5) penilaian dan pengambilan keputusan atas insiden dan kelemahan keamanan informasi; dan

6) pemulihan insiden.

e. Seluruh pegawai dan pihak ketiga wajib melaporkan berbagai kejadian insiden keamanan informasi maupun yang masih bersifat dugaan atas kelemahan keamanan informasi sesegera mungkin, sesuai prosedur pelaporan insiden yang berlaku.

f. Setiap kejadian insiden keamanan informasi harus dianalisis, diklasifikasikan, dan ditentukan skala prioritas penanganannya.

g. Penanganan insiden beserta pemulihannya dilakukan berdasarkan klasifikasi dan prioritas yang telah ditetapkan.

h. Perangkat Daerah harus mengklasifikasikan insiden keamanan informasi untuk memprioritaskan penanganan insiden. Klasifikasi insiden tersebut adalah sebagai berikut:

1) insiden keamanan informasi diklasifikasikan berdasarkan dampaknya menjadi berikut:
   - mayor, apabila insiden tersebut menyebabkan terhentinya proses operasional pekerjaan Perangkat Daerah; dan
   - minor, apabila insiden tersebut menyebabkan gangguan yang tidak menghentikan proses operasional pekerjaan Perangkat Daerah.

2) insiden keamanan informasi diklasifikasikan berdasarkan tingkat kepentingannya menjadi berikut:
   - *emergency*, apabila insiden tersebut dapat atau telah menghentikan proses operasional Perangkat Daerah dan/atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan Perangkat Daerah; dan
   - normal, apabila insiden tersebut insiden tersebut tidak menghentikan proses operasional Perangkat Daerah dan/atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan Perangkat Daerah.

i. Setiap insiden keamanan informasi harus ditangani dengan baik untuk mencegah meluasnya insiden, untuk memulihkan layanan atau informasi yang mungkin hilang dan untuk meminimalisasi dampak dari insiden.

j. Setiap tindakan yang diidentifikasi untuk menangani kejadian, kelemahan dan insiden keamanan informasi harus dikonsultasikan kepada koordinator Teknologi Informasi dan/atau personil yang kompeten dan relevan dengan kejadian, kelemahan, dan insiden keamanan informasi.
k. Setiap tindakan penanganan kejadian, kelemahan, dan insiden keamanan informasi harus didokumentasikan dengan baik.

BAB XIV

MANAJEMEN KEBERLANGSUNGAN BISNIS (*BUSINESS CONTINUITY*)

1. **Tujuan**

   Tujuan dari kebijakan mengenai kelangsungan usaha *(business continuity)* adalah untuk memastikan ketersediaan layanan TIK beserta fasilitas pengolahan informasi dalam kondisi darurat dan memulihkan layanan seperti sediakala dalam kondisi kembali normal.

2. **Ruang Lingkup**

   Ruang lingkup dari kebijakan mengenai kelangsungan usaha (*business continuity)* adalah:

   a. keberlanjutan keamanan informasi; dan
   b. redundansi fasilitas pengolahan informasi.

3. **Kebijakan**

   a. Perangkat Daerah harus menetapkan, mendokumentasikan, mengimplementasikan dan memelihara proses, prosedur, dan kontrol yang diperlukan untuk menjamin keberlanjutan keamanan informasi sesuai prasyarat yang telah ditetapkan pada saat dan setelah terjadinya gangguan besar atau bencana.
   b. Perangkat Daerah harus memverifikasi kontrol keberlanjutan keamanan informasi yang telah ditetapkan dan diimplementasikan secara berkala untuk menjamin kesesuaian dan efektivitasnya pada saat dan setelah terjadinya gangguan besar atau bencana.
   c. Perangkat Daerah harus menetapkan prasyarat untuk keberlanjutan keamanan informasi dan diintegrasikan dengan prasyarat keberlanjutan bisnis organisasi untuk menjamin keberlanjutan dari keamanan informasi di Perangkat Daerah, pada saat dan setelah terjadinya gangguan besar atau bencana.
   d. Prasyarat keamanan informasi dapat diintegrasikan pada siklus proses *Business Continuity Management (BCM)* yang mencakup:
      1) memahami kebutuhan organisasi;
      2) menentukan strategi BCM;
      3) mengembangkan dan mengimplementasikan rencana penanggulangan/keberlanjutan bisnis; dan
      4) pengujian, pemeliharaan, dan peninjauan rencana penanggulangan / keberlanjutan bisnis.

e. Aspek redundansi harus ditetapkan untuk fasilitas pengolahan informasi dan sarana pendukungnya untuk memastikan ketersediaan dari proses bisnis dan operasional Perangkat Daerah serta pemberian layanan Perangkat Daerah kepada pelanggan.
f. Apabila prasyarat redundan tidak dapat dipenuhi, maka proses alternatif perlu ditetapkan untuk menjamin ketersediaan dari proses bisnis dan operasional Perangkat Daerah serta *delivery* dari layanan Perangkat Daerah kepada pelanggan.
g. Fasilitas pengolahan informasi beserta sarana pendukungnya yang telah memenuhi aspek redundansi harus diuji secara berkala untuk menjamin kesesuaian dari fungsinya.
h. Guna menjamin ketersediaan layanan serta keamanan informasi dalam kondisi darurat (misalnya: bencana alam) pada lokasi utama, perlu adanya redundansi terhadap fasilitas pengolahan informasi yang disebut sebagai fasilitas backup site.
i. Backup site yang dimaksud dapat berupa lokasi kerja pengganti atau *Disaster Recovery Center* (DRC) bagi alternatif area Data Center.
j. Ketentuan dalam pengelolaan terkait Backup Site meliputi:
    1) lokasi *backup site* secara geografis memiliki probabilitas kejadian bencana alam yang minimal;
    2) *backup site* ditujukan sebagai media penyimpanan backup alternatif, serta sebagai fasilitas pengolahan informasi alternatif;
    3) terpenuhinya pemulihan layanan operasional sepenuhnya pada fasilitas backup site sesuai kerangka parameter *Recovery Time Objective* (RTO);
    4) pengelola backup site beserta Pemilik Aset Informasi melakukan uji keberlangsungan secara berkala dibawah koordinasi penanggung jawab kelangsungan bisnis, minimal 1 (satu) kali dalam setahun, untuk menguji kesiapan seluruh pihak dalam hal:
        - memindahkan operasional ke fasilitas backup site; dan
        - memulihkan operasional aplikasi beserta data sesuai parameter *Recovery Time Objective* (RTO) yang telah ditetapkan.

BAB XV
KEPATUHAN

1. **Tujuan**

   Tujuan dari kebijakan kepatuhan adalah untuk menghindari pelanggaran kewajiban hukum, undang-undang, peraturan, atau kontrak yang terkait keamanan informasi dan persyaratan keamanan dan untuk memastikan keamanan informasi diimplementasikan dan dioperasikan sesuai dengan prosedur dan kebijakan organisasi.

2. **Ruang Lingkup**

   Ruang lingkup dari kebijakan mengenai kepatuhan:

   a. kepatuhan dengan prasyarat hukum dan kontraktual; dan
   b. peninjauan keamanan informasi.

3. **Kebijakan**

   a. Pemerintah Daerah Kabupaten Bantul berkomitmen untuk menjaga kepatuhan terhadap setiap prasyarat keamanan informasi yang relevan. Prasyarat keamanan informasi yang dimaksud mencakup prasyarat hukum, regulasi, dan kontraktual.
   b. Seluruh prasyarat hukum, regulasi dan kontraktual yang terkait dengan keamanan informasi dan berlaku bagi Perangkat Daerah harus diidentifikasikan, didokumentasikan, dan dipelihara.
   c. Perangkat Daerah harus mematuhi hak atas kekayaan intelektual yang terkait dengan material yang digunakan oleh Perangkat Daerah seperti:
      1) penggunaan perangkat lunak dan material yang bersifat *proprietary* harus mematuhi undang-undang terkait Hak atas Kekayaan Intelektual (HAKI) yang berlaku;
      2) bukti dari lisensi atau izin resmi harus didapatkan dan disimpan untuk seluruh materi berlisensi/*copyright* yang di-install;
      3) lisensi yang bersifat berlangganan/harus diperbaharui dalam jangka waktu tertentu, harus dikelola untuk memastikan penggunaannya secara legal dan berkesinambungan; dan
      4) penggunaan lisensi dari materi berlisensi/*copyright* harus dikendalikan dengan baik.

d. Dokumen-dokumen penting Perangkat Daerah harus dilindungi dari kehilangan, pemalsuan, kerusakan, atau penyalahgunaan sesuai dengan peraturan perundangan, regulasi, dan persyaratan kontrak dan bisnis.
e. Perangkat Daerah harus memastikan privasi dan perlindungan terhadap informasi terkait dengan pribadi *(personally identifiable information)* sesuai dengan prasyarat hukum, perundang-undangan, regulasi, dan kontraktual.
f. Pimpinan Perangkat Daerah harus secara rutin memantau dan meninjau kepatuhan dari personil, proses kerja dan pemrosesan informasi dalam area tanggung jawabnya terhadap kebijakan dan standar keamanan informasi Perangkat Daerah serta prasyarat keamanan informasi yang berlaku.
g. Pada saat terjadi ketidaksesuaian, pimpinan Perangkat Daerah bertanggung jawab untuk menangani ketidaksesuaian yang terjadi sesuai dengan kebijakan terkait penanganan ketidaksesuaian dan peningkatan SMKI.
h. Sistem Informasi Perangkat Daerah harus ditinjau untuk menganalisis kepatuhan teknis dengan kebijakan dan standar keamanan yang berlaku serta dengan prasyarat keamanan informasi yang relevan dan berlaku, paling tidak 1 (satu) kali dalam 1 (satu) tahun.
i. Apabila diperlukan, peninjauan tersebut dapat melibatkan personil yang memiliki kualifikasi di bidang keamanan informasi untuk mendapatkan pemahaman yang mendalam mengenai risiko keamanan informasi yang mungkin muncul dari pengecualian tersebut

Daftar Istilah

Otentikasi

Pemberian jaminan bahwa karakteristik dari suatu entitas dapat dinyatakan benar

Otorisasi

Proses untuk memastikan bahwa permintaan aktivitas atau akses ke suatu objek diperbolehkan dengan mempertimbangkan hak dan privilege yang diberikan kepada identitas terotentikasi

Kerahasiaan

Karakteristik dari informasi bahwa informasi tersebut tidak disediakan atau diungkapkan kepada individu, entitas, atau proses yang tidak memiliki wewenang

Integritas

Karakteristik dalam melindungi akurasi dan kelengkapan asset Ketersediaan Karakteristik dari informasi bahwa informasi tersebut dapat diakses dan digunakan sesuai permintaan entitas yang memiliki wewenang

Rekaman

Suatu dokumen yang menyatakan hasil yang telah dicapati atau menyediakan bukti bahwa suatu aktivitas telah dilakukan

Risiko

Kombinasi dari probabilitas suatu kejadian dan konsekuensi dari kejadian-kejadian tersebut

Referensi

1. ISO/IEC 27001:2022 - *Information security management systems — Requirements*
2. ISO/IEC 27002:2022 - *Code of practice for information security management*
3. ISO/IEC 27005:2018 - Teknik keamanan — Manajemen risiko keamanan informasi
4. Indeks KAMI 4.2 – Indeks Keamanan Informasi

BUPATI BANTUL,

ttd

ABDUL HALIM MUSLIH