PEMERINTAH KABUPATEN KENDAL
SEKRETARIAT DAERAH
Jl. Soekarno-Hatta No. 193 Kendal 51313 Telp. (0294) 381251-381232 Fax. (0294) 381062
website : www.kendalkab.go.id

KEPUTUSAN SEKRETARIS DAERAH KABUPATEN KENDAL

NOMOR : 360.2/ 128/ 2023

TENTANG

PENETAPAN PROSEDUR PENGENDALIAN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN KENDAL

SEKRETARIS DAERAH,

Menimbang :

a. bahwa dalam rangka melindungi aset informasi dan penyelenggaraan Sistem Pemerintahan Berbasis Elektronik pada Pemerintah Kabupaten Kendal dari berbagai bentuk ancaman keamanan informasi baik dari dalam maupun luar lingkungan Pemerintah Kabupaten kendal, perlu melakukan pengelolaan keamanan informasi di lingkungan Pemerintah Kabupaten Kendal;

b. bahwa dalam rangka pengelolaan keamanan informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Kendal, perlu menyusun Prosedur Pengendalian Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Kendal;

c.. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan keputusan Sekretaris Daerah Kabupaten Kendal tentang Penetapan Prosedur Pengendalian Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Kendal;

Mengingat :

1. Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Djawa Tengah sebagaimana telah diubah dengan Undang-Undang Nomor 9 Tahun 1965 tentang Pembentukan Daerah Tingkat II Batang dengan mengubah Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Jawa Tengah (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 52, Tambahan Lembaran Negara Republik Indonesia Nomor 2757);
2. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun

2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);

3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
5. Peraturan Pemerintah Nomor 32 Tahun 1950 tentang Penetapan Mulai Berlakunya Undang-Undang 1950 Nomor 12, 13, 14 dan 15 dari Hal Pembentukan Daerah-Daerah Kabupaten di Jawa Timur/Tengah/Barat dan Daerah Istimewa Yogyakarta;
6. Peraturan Pemerintah Nomor 16 Tahun 1976 tentang Perluasan Kotamadya Daerah Tingkat II Semarang (Lembaran Negara Republik Indonesia Tahun 1976 Nomor 25, Tambahan Lembaran Negara Republik Indonesia Nomor 3079);
7. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2018 Nomor 182, Tambahan Berita Negara Republik Indonesia Nomor 4843);
9. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Berita Negara Republik Indonesia Tahun 2022 Nomor 129);
10. Peraturan Daerah Kabupaten Kendal Nomor 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Kendal (Lembaran Daerah Kabupaten Kendal Tahun 2016 Seri D No. 1, Tambahan Lembaran Daerah Kabupaten Kendal Nomor 159) sebagaimana telah diubah dengan Peraturan Daerah Kabupaten Kendal Nomor 3 Tahun 2020 tentang Perubahan Atas Peraturan Daerah Kabupaten Kendal Nomor 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Kendal (Lembaran Daerah

Kabupaten Kendal Tahun 2020 Nomor 3, Tambahan Lembaran Daerah Kabupaten Kendal Nomor 200);

11. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
12. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);
13. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
14. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
15. Peraturan Bupati Kendal Nomor 35 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Kendal (Berita Daerah Kabupaten Kendal Tahun 2021 Nomor 35);

Memperhatikan : SNI ISO/IEC 270001:2013 (Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi - Persyaratan);

MEMUTUSKAN:

Menetapkan :

KESATU : Prosedur Pengendalian Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Kendal sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan ini.

KEDUA : Prosedur Pengendalian Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Kendal sebagaimana dimaksud dalam Diktum KESATU digunakan sebagai pedoman atau standar dalam rangka melindungi aset informasi dan penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Kendal dari berbagai bentuk ancaman baik dari dalam maupun dari luar lingkungan Pemerintah Kabupaten Kendal dengan tujuan untuk menjamin kerahasiaan, keutuhan, ketersediaan, autentifikasi dan kenirsangkalan aset informasi.

KETIGA : Keputusan ini berlaku pada tanggal ditetapkan.

Ditetapkan di Kendal
pada tanggal 9 Januari 2023

SEKRETARIS DAERAH
KABUPATEN KENDAL,

SUGIONO

LAMPIRAN
KEPUTUSAN SEKRETARIS DAERAH
KABUPATEN KENDAL
NOMOR : 360.2/ 128/ 2023
TANGGAL : 9 Januari 2023

PROSEDUR PENGENDALIAN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN KENDAL

MANAJEMEN RISIKO

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian manajemen resiko adalah untuk mengelola risiko keamanan informasi yang dihadapi oleh organisasi dalam rangka untuk mempersiapkan diri terhadap terjadinya risiko beserta dampaknya.

B. Ruang Lingkup

Ruang lingkup dari manajemen risiko memastikan Perangkat Daerah dapat menerapkan proses Pengelolaan Risiko yang mencakup kegiatan:

1. Penerapan konteks;
2. Assessment risiko;
3. Penanganan risiko;
4. Pemantauan dan peninjauan risiko; dan
5. Komunikasi dan koordinasi risiko.

C. Prosedur Pengendalian

1. Kriteria penerimaan risiko dan penilaian keamanan informasi harus ditetapkan untuk memberikan arahan bagi Perangkat Daerah terhadap penanganan risiko yang harus dilakukan.
2. Perangkat Daerah harus menerapkan konteks terkait rencana perencanaan identifikasi Risiko yang meliputi isu-isu, pihak terkait dan prasyarat keamanan informasi internal dan eksternal yang terkait dengan keamanan informasi harus diidentifikasi dan ditetapkan sebagai pertimbangan dalam mengidentifikasi risiko keamanan informasi. Hal ini setidaknya mencakup:
   a. kegiatan utama yang dilakukan oleh organisasi;
   b. kebijakan internal organisasi;
   c. proses bisnis organisasi;
   d. kewajiban hukum, perundangan dan kewajiban kontrak yang dimiliki oleh organisasi;
   e. kondisi teknologi informasi dan keamanan informasi, baik internal maupun eksternal yang relevan dengan organisasi.
3. Perangkat Daerah harus melaksanakan penilaian risiko yang berpengaruh terhadap kegagalan sistem dan operasional TI terkait dengan aspek keamanan informasi yang mencakup aktivitas:

3.1 identifikasi risiko:
   a. mengidentifikasi ancaman, merupakan aktifitas untuk mengidentifikasi ancaman terhadap risiko keamanan informasi;
   b. ancaman didefinisikan sebagai potensi penyebab insiden yang tidak diinginkan yang dapat menyebabkan kerusakan/kerugian bagi organisasi dan sistemnya;
   c. sebuah ancaman tidak dapat dikatakan sebuah risiko apabila tanpa kombinasi dengan kelemahan yang dapat dieskplotasi;

d. mengidentifikasi kelemahan dilakukan setelah pengidentifikasian ancaman dilakukan;
e. kelemahan didefinisikan sebagai potensi kekurangan pada proses dan kontrol keamanan yang dapat dieksplotasi oleh satu ancaman atau lebih;
f. mengidentifikasi dampak merupakan aktifitas yang dilakukan untuk mengidentifikasi potensi dampak jika ancaman yang teridentifikasi, mengeksploitasi kelemahan yang ada;
g. risiko harus dialokasikan ke pemilik risiko; dan
h. pemilik risiko bertanggung jawab untuk mengelola risiko yang telah teridentifikasi.

3.2 analisis risiko:
a. menilai dampak potensial yang akan terjadi apabila risiko yang teridentifikasi terwujud;
b. kriteria dampak merupakan parameter untuk menentukan tingkat kerugian terhadap risiko yang terjadi.
Contoh kriteria dampak adalah sebagai berikut:

Tingkat Dampak	Operasional	Peraturan / Hukum	Aset Informasi	Reputasi
1 (Ringan)	Penundaan proses bisnis setengah hari	Tidak ada pelanggaran hukum	Tidak ada kebocoran atau kehilangan aset informasi	Tidak ada dampak terhadap reputasi Perangkat Daerah
2 (Sedang)	Penundaan proses bisnis 1 hari	Pelanggaran ringan dengan surat peringatan	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat PUBLIK	Mengganggu kepercayaan sebagian kecil pihak eksternal. Berdampak pada reputasi Perangkat Daerah naum reputasi dapat dipulihkan dalam waktu tidak terlalu lama
3 (Berat)	Penundaan proses bisnis 3 hari	Pelanggaran sedang yang dikenakan sanksi administratif	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat TERBATAS	Mengganggu kepercayaan sebagian besar pihak eksternal. Berdampak pada reputasi Perangkat Daerah dan pemulihan reputasi membutuhkan waktu lama
4 (Sangat Berat)	Penundaan lebih dari 3 hari	Pelanggaran berat dengan sanksi hukum	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat RAHASIA	Mengganggu kepercayaan sebagian besar pihak eksternal, Berdampak pada reputasi Perangkat Daerah dan sangat sulit dilakukan pemulihan reputasi

Tabel 1. Tabel dampak risiko

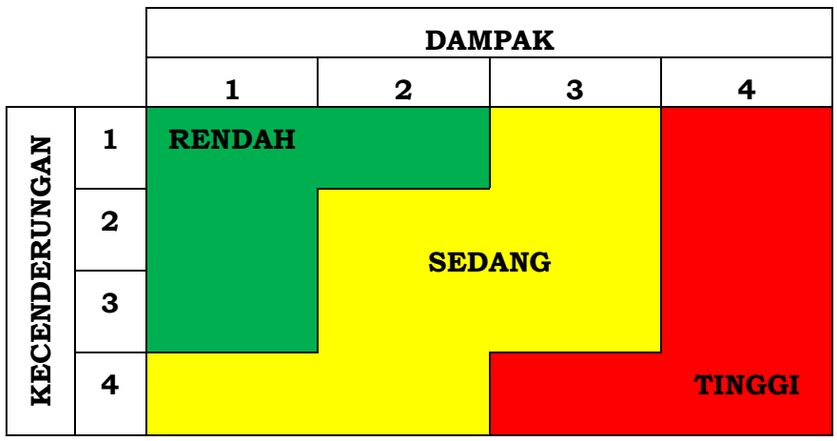
c. Menilai kemungkinan realistis terjadinya risiko yang teridentifikasi; dan
d. Kriteria kecenderungan merupakan parameter untuk menentukan tingkat kejadian terhadap Risiko.
Contoh kriteria kecenderungan adalah sebagai berikut:

Nilai	Tingkat	Kriteria Kecenderungan
		Frekuensi terjadinya
1	Rendah	Kejadian tidak lebih dari 2 kali / tahun
2	Sedang	Kejadian lebih dari 2 kali / tahun, namun tidak lebih dari 5 kali / tahun
3	Tinggi	Kejadian lebih dari 5 kali / tahun, namun tidak lebih dari 10 kali / tahun
4	Ekstrim	Kejadian lebih dari 10 kali / tahun

Tabel 2. Tabel kecenderungan risiko

e. Evaluasi risiko:
1) membandingkan hasil analisis risiko dengan kriteria risiko yang sudah ditetapkan;
2) risiko yang masuk dalam kriteria penerimaan risiko akan diterima;
3) risiko yang tidak masuk dalam kriteria penerimaan risiko perlu mendapatkan penanganan; dan
4) setiap penanganan risiko harus diberikan prioritas.

4. Hasil evaluasi risiko harus dianalisis terkait risiko tersebut dapat diterima dalam level tertentu berdasarkan kriteria penerimaan risiko yang telah ditetapkan atau memerlukan penanganan risiko lebih lanjut.
Tabel risiko adalah matriks antara nilai dari dampak dan kecenderungan yang menghasilkan tingkat risiko.
Contoh tabel risiko adalah sebagai berikut:



Tabel 3. Tabel nilai risiko

5. Dalam hal risiko tersebut tidak dapat diterima, Perangkat Daerah harus menerapkan penanganan risiko yang diperlukan yang mencakup:
a. mengendalikan/*control* adalah merupakan tindakan pengendalian risiko dengan mengurangi dampak maupun kemungkinan terjadinya risiko melalui menerapkan suatu sistem atau aturan;
b. menghindari/*avoid* adalah tindakan pengendalian risiko dengan tidak melakukan suatu aktivitas atau memilih aktivitas lain dengan output yang sama untuk menghindari terjadinya risiko;
c. mengalihkan/*transfer* adalah tindakan pengendalian risiko dengan mengalihkan seluruh atau sebagian tanggung jawab pelaksanaan suatu proses kepada pihak ketiga.

6. Penanganan risiko harus memadai untuk mengurangi risiko ke tingkat yang dapat diterima berdasarkan kriteria penerimaan risiko.
7. Pemilik risiko harus memastikan setiap rencana penanganan risiko telah memadai dan relevan bagi risiko yang ada.
8. Setiap rencana penanganan risiko harus diberikan prioritas oleh pemilik risiko.
9. Setiap keputusan terkait dengan penanganan risiko dan kontrol keamanan risiko yang relevan harus disetujui oleh Pimpinan Perangkat Daerah terkait.
10. Perangkat Daerah harus melakukan proses pemantauan dan peninjauan risiko untuk memastikan efektifitas kontrol yang dilakukan yang mencakup:
    a. proses pemantauan dan peninjauan risiko adalah proses berkesinambungan untuk memastikan bahwa:
        1) risiko baru telah terindentifikasi, di-*assess* dan ditangani;
        2) setiap perubahan terhadap risiko yang sudah ada telah teridentifikasi, di-*assess* dan ditangani;
        3) kontrol keamanan yang sudah ada telah memadai dan efektif dalam menangani risiko.
    b. proses pemantauan dan peninjauan risiko harus dilakukan secara formal dan rutin;
    c. Perangkat Daerah harus menentukan frekuensi pemantauan dan peninjauan risiko.
11. Perangkat Daerah harus melakukan proses komunikasi dan koordinasi risiko untuk memastikan pengelolaan penanganan kontrol terkendali dan efektif dalam mengurangi tingkat Risiko yang diharapkan.
12. Metode komunikasi dan koordinasi risiko harus ditetapkan yang meliputi:
    a. proses komunikasi dan koordinasi risiko merupakan proses berkesinambungan untuk mengkomunikasi dan mengkoordinasikan setiap informasi, aktifitas dan keputusan terkait dengan risiko keamanan informasi dan proses manajemen risiko;
    b. setiap informasi, aktifitas dan keputusan harus dikomunikasikan dan dikoordinasikan dengan pemilik risiko, personil terkait dan Kepala Perangkat Daerah; dan
    c. setiap komunikasi dan koordinasi eksternal terkait risiko keamanan informasi dan manajemen risiko harus disetujui oleh Kepala Perangkat Daerah.

KELANGSUNGAN BISNIS DAN PEMULIHAN BENCANA

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian kelangsungan bisnis dan pemulihan bencana adalah untuk:

1. Memberi panduan tentang tata cara mempersiapkan, menyediakan, dan memelihara kontrol dan kemampuan untuk menghadapi gangguan atau bencana yang mungkin terjadi.
2. Menjamin kelangsungan operasional bisnis dan layanan pada Pemerintah Kabupaten Kendal selama dan/atau setelah terjadi gangguan atau bencana yang berpotensi mengganggu proses kerja Pemerintah Kabupaten Kendal.

B. Ruang Lingkup

Prosedur pengendalian ini berlaku untuk seluruh aset teknologi informasi dan sarana pendukungnya yang digunakan dalam penyelenggaraan layanan teknologi informasi di lingkungan Pemerintah Kabupaten Kendal, yang meliputi:

1. Informasi, meliputi dokumen penawaran penyedia, data penyedia, kebijakan dan prosedur teknologi informasi, konfigurasi LAN, hasil pengkajian risiko (*risk register*), hasil audit log, hasil monitoring penggunaan bandwidth jaringan, dan lain sebagainya.
2. Perangkat lunak, meliputi aplikasi (misal: aplikasi *e-government*, SPSE, sistem operasi, MS Office, *software antivirus, tool/software monitoring,* dan perangkat lunak lainnya yang mendukung pelaksanaan kegiatan di lingkungan Pemerintah Kabupaten Kendal).
3. Perangkat keras dan infranstuktur jaringan, meliputi: PC/Laptop, *server, router,* kabel LAN, *modem, storage, flashdisk,* dan lain sebagainnya.
4. Sarana pendukung, meliputi: sumber daya listrik PLN, UPS, Genset, A/C, CCTV, alat pemadam kebakaran, alat pengukur suhu dan kelembaban, gedung penyelenggara layanan teknologi informasi, dan sarana lainnya yang mendukung penyelenggaraan layanan teknologi informasi di lingkungan Pemerintah Kabupaten Kabupaten Kendal.
5. Sumber daya manusia, meliputi: sistem administrator, pengembang (*programmer*) dan penyedia jasa (*vendor/pihak ketiga*).

C. Kebijakan Umum

1. Dalam proses manajemen kelangsungan bisnis, aspek-aspek keamanan informasi terutama terkait aspek kerahasiaan, integritas dan ketersediaan dari informasi merupakan bagian yang tidak terpisahkan dan harus selalu dipertimbangkan.
2. Struktur pengembangan manajemen kelangsungan bisnis di setiap Perangkat Daerah Kabupaten Kendal sesuai dengan struktur PDCA (*Plan-Do-Check-Act*).
3. Struktur PDCA pada manajemen kelangsungan bisnis terdiri dari:
   a. *Plan* – Membuat kajian, tujuan, kontrol, proses, dan prosedur kelangsungan bisnis yang relevan untuk meningkatkan kelangsungan bisnis guna memberikan hasil yang sesuai dengan kebijakan dan tujuan keseluruhan organisasi.
   b. *Do* – Mengimplementasikan dan mengoperasikan kebijakan, kontrol, proses dan prosedur kelangsungan bisnis.
   c. *Check* – Memantau dan mengevaluasi kinerja terhadap tujuan, kebijakan dan prosedur kelangsungan bisnis, kemudian melaporkan hasilnya kepada manajemen untuk diperiksa, menentukan dan

memberikan wewenang tindakan untuk perbaikan dan pengingkatan.

d. *Act* – Memelihara dan meningkatkan manajemen kelangsungan bisnis dengan mengambil tindakan korektif, berdasarkan hasil tinjauan manajemen dan menilai kembali lingkup manajemen kelangsungan bisnis dan kebijakan maupun tujuan kelangsungan bisnis.

4. Setiap Perangkat Daerah harus menetapkan, mendokumentasikan, mengimplementasikan dan memelihara proses, prosedur dan kontrol yang diperlukan untuk menjamin kelangsungan keamanan informasi sesuai prasyarat yang telah ditetapkan pada saat dan setelah terjadinya gangguan besar atau bencana.
5. Setiap Perangkat Daerah berkewajiban melaksanakan verifikasi kontrol kelangsungan keamanan informasi yang telah ditetapkan dan diimplementasikan secara berkala untuk menjamin kesesuaian dan efektivitasnya pada saat dan setelah terjadinya gangguan besar atau bencana.
6. Setiap Perangkat Daerah menerapkan dan memelihara proses untuk mengidentifikasi, akses dan menilai persyaratan hukum dan peraturan yang berlaku terkait kelangsungan bisnis.

D. Prosedur Pengendalian

1. Analisa Dampak Bisnis (*Business Impact Analysis /* BIA) merupakan proses untuk mengukur tingkat kerugian atau kerusakan suatu operasi atau layanan apabila terdapat aset yang tidak tersedia untuk mendukung proses bisnis kritis dan juga efek yang didapat untuk fungsi bisnis.
2. Analisa Dampak Bisnis merupakan siklus yang membutuhkan masukan (*input*) dan menghasilkan keluaran (*output*). Siklus ini bersifat layaknya sebuah proyek yang memiliki waktu mulai dan selesai yang telah didefinisikan sejak awal.
3. Masukan (*input*) daru siklus BIA adalah cakupan dan konteks yang telah ditentukan, peran dan tanggung jawab yang telah ditentukan dan dikomunikasikan, adanya komitmen dari pimpinan dan alokasi sumber daya yang cukup.
4. Keluaran (*output*) dari siklus BIA merupakan kebutuhan untuk kelangsungan bisnis yang akan digunakan untuk proses pemeliharaan strategi kelangsungan bisnis dalam manajemen kelangsungan bisnis.
5. Proses manajemen kelangsungan bisnis mencakup:
   a. Analisis Risiko dengan beberapa tahapan yaitu:
      1) Mengidentifikasi ancaman atau bencana pada kelangsungan dan proses dari fungsi bisnis utama, sistem informasi, aset, sumber daya manusia, dan pihak ketiga.
      2) Menganalisa dampak dari gangguan melakukan pengukuran sesuai dengan dokumen risk register.
      3) Melakukan evaluasi terhadap gangguan berdasarkan risiko yang perlu ditindaklanjuti.
      4) Mengidentifikas tindakan yang akan dilakukan sesuai dengan tujuan manajemen kelangsungan bisnis
   b. Analisa Dampak Bisnis mencakup:
      1) Mengidentifikasi proses bisnis kritikal.
      2) Mengidentifikasi dampak dari gangguan terhadap proses bisnis kritikal.
      3) Analisa dampak bisnis dapat disesuaikan dengan Dokumen Kebijakan Manajemen Risiko dan Dokumen *Risk Register*.
      4) Mengatur dan menentukan waktu maksimal organisasi tersebut

dapat bertahan tanpa sistem pada saat terjadinya gangguan.
Waktu pemulihan akan dianalisis menjadi 2 yaitu:
***Maximum Torerable Downtime* (MTD)**
Merupakan jumlah waktu maksimal yang dapat ditoleransi oleh instansi terhadap kegagalan bisnis.
***Recovery Time Objective* (RTO)**
Merupakan jumlah waktu lumpuh maksimal untuk seluruh sumber daya sistem yang ada, sebelum terjadi dampak lain kepada sumber daya lainnya. Jika waktu penanggulangan gangguan atau bencana melebiji RTO dapat menyebabkan dampak yang lebih besar bagi organisasi.

MTD dapat diidentifikasi dengan cara mengidentifikasi:

a) Jangka waktu maksimal setelah terjadinya (*starting point*) gangguan dimana aktivitas normal dari layanan harus sudah dimulai.
b) Identifikasi prioritas untuk pemulihan aktivitas/proses bisnis.
c) Identifikasi ketergantungan yang dimiliki oleh proses/aktivitas bisnis kritikal tersebut baik internal maupun eksternal. Hal ini mencakup layanan, infrastruktur, pihak ketiga penyedia jasa atau *stakeholder* lainnya.
d) Bagi pihak pihak ketiga atau pihak ketiga penyedia jasa, perlu dipastikan bahwa pengaturan kelangsungan bisnis juga mencakup untuk layanan produk dan jasa yang mereka sediakan untuk instansi.
e) Menetapkan *recovery time objective* yang merupakan target waktu pemulihan aktivitas bisnis kritikal. RTO yang ditetapkan harus lebih kecil atau paling tidak sama dengan MTD.
f) Memperkirakan sumber daya yang dibutuhkan untuk setiap aktivitas kritikal yang dibutuhkan untuk memulihkan proses/aktivitas bisnis kritikal tersebut.
Yang disebut sebagai sumber daya dapat mencakup namun tidak terbatas pada:
- Perangkat keras.
- Perangkat lunak (s*oftware*/aplikasi).
- Sumber daya manusia (personil).
- Data/informasi.
- Sarana pendukung (*utilities*).

c. Penilaian risiko, proses ini dilakukan dengan cara:
   1) Mengidentifikasi ancaman terhadap dan kerawanan pada proses/aktivitas bisnis kritikal tersebut.
   2) Mengidentifikasi dampak apabila ancaman dan kerawanan tersebut terwujud dan menimbulkan gangguan terhadap proses bisnis tersebut.
d. Mengidentifikasi, menetapkan serta mengimplementasikan penanganan risiko bagi risiko yang telah teridentifikasi. Penanganan risiko tersebut dapat mencakup:
   1) Mengurangi kemungkinan terjadinya gangguan.
   2) Mengurangi jangka waktu gangguan
   3) Mengurangi dampak gangguan.

6. Proses yang menentukan strategi manajemen kelangsungan bisnis, yang mencakup
   a. Menetapkan struktur organisasi dan proses untuk memungkinkan proses tanggap darurat dan pemulihan secara cepat dan efektif.

b. Menetapkan cara/metode untuk memulihkan aktivitas kritikal dalam jangka waktu *recovery time objective* yang telah ditetapkan. Hal ini mencakup sumber daya yang dibutuhkan, baik internal maupun eksternal.
c. Menetapkan cara komunikasi dengan *stakeholder* yang terkait dengan proses/aktivitas bisnis kritikal tersebut.

7. Mengembangkan dan mengimplementasikan rencana penanggulangan/kelangsungan bisnis yang mencakup:
   a. Menetapkan struktur organisasi dan proses untuk proses tanggap darurat/gangguan berikut alokasi personil yang kompeten sebagai penanggung jawab untuk proses:
      1) Mengkonfirmasi tipe dan cakupan dari kondisi darurat/gangguan tersebut.
      2) Memutuskan untuk mengaktifkan rencana tanggap darurat.
      3) Mengkoordinasikan serta menjalankan rencana tanggap darurat tersebut.
      4) Menyediakan sumber daya yang dibutuhkan untuk proses tanggap darurat.
      5) Mengkomunikasikan kondisi tersebut kepada para pemangku kepentungan (*stakeholder*).
   b. Menetapkan rencana tanggap darurat dan rencana kelangsungan bisnis yang mencakup:
      1) Penentuan personil yang terlibat beserta tugas dan tanggung jawab serta jalur komunikasi antar personil, beserta personil alternatifnya.
      2) Otoritas yang dimiliki oleh personil dalam ruang lingkup rencana tersebut.
      3) Kondisi dan metode untuk pemberlakuan rencana tersebut.
      4) Lokasi pertemuan beserta alternatifnya.
      5) Kondisi dan metode untuk menghubungi *stakeholder* instansi beserta informasi kontak.
      6) Aktivitas yang harus dilakukan pada kondisi darurat dengan titik berat pada proses pengelolaan dampak dari kondisi darurat yang mencakup:
         a) Keselamatan manusia.
         b) Aktivitas strategis dan operasional untuk menanggulangi kondisi darurat.
         c) Mencegah kerugian atau kehilangan aktivitas kritikal tambahan.
         d) Memungkinkan pemulihan dan melanjutkan proses/aktivitas bisnis kritikal.
      7) Informasi yang perlu dicatat terkait dengan gangguan beserta keputusan dan tindakan yang diambil.
      8) Sumber daya yang perlu disediakan untuk proses pemulihan dan kelajutan proses bisnis kritikal.
      9) Proses-proses bisnis kritikal yang perlu dipulihkan beserta jangka waktu dan tingkat pemulihan. Hal ini perlu disesuaikan dengan skala prioritas yang telah disusun dalam proses analisa dampak bisnis.

8. Proses pengujian,pemeliharaan dan peninjauan rencana penanggulangan/kelangsungan bisnis bertujuan untuk memverifikasi kesesuaian dan efektivitas dari proses *Business Continuity Plan* yang mencakup juga rencana tanggap darurat dan kelangsungan bisnis yang telah ditetapkan. Proses ini juga dilakukan untuk memberikan keyakinan bahwa proses/aktivitas kritikal instansi dapat dipulihkan sesuai dengan prasyarat yang telah ditetapkan. Proses ini mencakup:

a. Pengujian rencana penanggulangan/kelangsungan bisnis, yang mencakup aktivitas berikut:
   1) Penyusunan rencana pengujian untuk rencana penanggulangan/kelangsungan bisnis yang mencakup:
      a) Jadwal.
      b) Pihak yang terlibat.
      c) Skenario pengujian.
      d) Aspek yang diukur dalam proses pengujian beserta metriks pengukuran yang digunakan.
      e) Laporan tertulis sebagai hasil pengujian rencana penanggulangan/kelangsungan bisnis.
   2) Pelaksanaan pengujian rencana penanggulangan/kelangsungan bisnis pengujian rencana ini bertujuan untuk:
      a) Menguji dan melatih persiapan pelaksanaan rencana penanggulangan/kelangsungan bisnis.
      b) Membandingkan rencana penanggulangan/kelangsungan bisnis dengan pelaksanaan.

b. Pemeliharaan dan peninjauan rencana penanggulangan/kelangsungan bisnis. Proses ini bertujuan untuk:
   1) Memastikan kesesuaian, kecukupan dan efektivitas dari rencana penanggulangan/kelangsungan bisnis yang telah disusun.
   2) Mengidentifikasi peningkatan dan perubahan dalam rencana penanggulangan/kelangsungan bisnis.

9. Proses pengujian, pemeliharaan, dan peninjauan ini perlu dilakukan minimal satu kali dalam satu tahun atau apabila terdapat perubahan besar dalam proses manajemen kelangsungan bisnis dan instansi.
10. Dokumentasi proses pengujian, pemeliharaan dan peninjauan harus dibuat dan dipelihara.
11. Proses pengujian dilakukan dengan memperhatikan kritikalitas dari proses yang rencana penanggulangan/kelangsungan bisnis akan diuji.
12. Proses pengujian dapat mencakup namun tidak terbatas pada proses:
    a. *Walkthrough*, di mana pengujian dilakukan dengan cara mendiskusikan rencana penanggulangan/keberlansungan bisnis yang telah disusun untuk memastikan bahwa rencana tersebut masih relevan dan dapat digunakan.
    b. Simulasi, di mana pengujian dilakukan melalui proses diskusi bersama untuk melihat pemahaman pihak pelaksana rencana penanggulangan/kelangsungan bisnis dengan cara melihat tanggapan pihak pelaksana terhadap skenario pengujian.
    c. *Partial test*, di mana pengujian dilakukan terhadap salah satu/sebagian komponen dari rencana penanggulangan/ kelangsungan bisnis.
    d. *Full test*, di mana pengujian dilakukan terhadap seluruh komponen dari rencana penanggulangan/kelangsungan bisnis.

AUDIT INTERNAL KEAMANAN SPBE

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian audit internal keamanan SPBE adalah sebagai pedoman bagi Perangkat Daerah dalam melakukan audit internal keamanan SPBE yang sesuai dengan peraturan yang berlaku.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian audit internal keamanan SPBE adalah proses audit internal keamanan SPBE yang dilaksanakan di lingkungan Pemerintah Kabupaten Kendal.

C. Prosedur Pengendalian

1. Setiap Perangkat Daerah yang memiliki dan/atau mengelola aplikasi serta infrastruktur SPBE secara mandiri wajib melakukan audit internal keamanan SPBE.
2. Kriteria audit internal keamanan SPBE di lingkungan Pemerintah Kabupaten Kendal harus dilaksanakan miminal satu kali dalam satu tahun dan harus mencakup seluruh ruang lingkup Manajemen Keamanan Informasi SPBE.
3. Audit internal keamanan SPBE dilakukan untuk memberikan informasi terkait kesesuaian manajemen keamanan informasi SPBE dengan:
   a. Prasyarat organisasi terkait keamanan informasi;
   b. Prasyarat dari standar ISO/IEC 27001:2013.
4. Audit internal keamanan SPBE juga dilaksanakan untuk memberikan informasi terkait efektivitas dari implementasi manajemen keamanan informasi SPBE pada organisasi.
5. Audit internal keamanan SPBE harus dilakukan oleh auditor yang memiliki kompetensi yang memadai serta memiliki objektivitas dan imparsialitas terhadap proses audit.
6. Auditor yang dipilih untuk proses audit harus ditunjuk secara formal oleh ketua tim manajemen keamanan informasi SPBE.
7. Sebuah program audit tahunan manajemen keamanan informasi SPBE harus ditetapkan oleh koordinator audit internal dan harus dikomunikasikan kepada ketua tim manajemen keamanan informasi SPBE.
8. Program audit tahunan keamanan SPBE harus disetujui oleh koordinator audit internal dan ketua tim manajemen keamanan informasi SPBE..
9. Program audit tahunan keamanan SPBE harus mencakup audit internal dan bila dimungkinkan audit eksternal keamanan SPBE.
10. Program audit yang telah ditetapkan harus dikomunikasikan kepada Perangkat Daerah pemilik dan/atau pengelola layanan SPBE sebagai *auditee*.
11. Program audit harus mencakup jadwal, metode, kriteria dan ruang lingkup, tanggung jawab serta prasyarat pelaporan dari audit.
12. Proses audit harus dilakukan sesuai dengan program audit yang telah ditetapkan secara formal.
13. Koordinator audit internal dan *auditee* bertanggung jawab untuk membantu proses audit dan menyediakan informasi yang akurat dan relevan kepada auditor sesuai dengan kriteria dan ruang lingkup audit.
14. Temuan audit harus diklasifikasikan berdasarkan kritikalitas dan cakupan dari temuan tersebut menjadi:

a. Major, ketidaksesuaian ini mengindikasikan tidak berjalannya sama sekali sebuah proses manajemen keamanan informasi SPBE atau kontrol keamanan informasi, atau apabila sebuah temuan dapat menyebabkan dampak buruk terhadap proses atau sistem kritikal organisasi.
b. Minor, ketidaksesuaian ini mengindikasikan sebuah kealpaan/problem kecil yang tidak mengindikasikan bahwa sebuah proses manajemen keamanan informasi SPBE atau kontrol keamanan informasi tidak berjalan sama sekali, atau apabila sebuah temuan tidak akan menyebabkan dampak buruk terhadap proses atau sistem kritikal organisasi.
c. Peluang untuk perbaikan, kategori temuan ini bukan merupakan sebuah ketidaksesuaian namun mengindikasikan bahwa sebuah area dapat diperbaiki untuk meningkatkan kinerja dari proses atau sistem tersebut.

15. Setiap ketidaksesuaian dan/atau peluang untuk perbaikan yang ditemukan dalam proses audit harus dicatat secara formal oleh auditor dan diterima oleh *auditee*.
16. Setiap ketidaksesuaian harus dikoreksi dan ditingkatkan oleh *auditee* dalam jangka waktu yang disepakati dengan cara merencanakan dan melaksanakan koreksi dan tindakan korektif.
17. Panduan untuk koreksi dan peningkatan terkait dengan ketidaksesuaian diberikan dalam Kebijakan dan Operasional Prosedur Pemenuhan Standar Manajemen Keamanan Informasi dan Peningkatan Standar Keamanan Informasi.
18. Sebuah laporan formal hasil audit harus disiapkan oleh koordinator audit internal setelah setiap proses audit.
19. Laporan audit harus dilaporkan kepada ketua tim manajemen keamanan informasi SPBE dan dikomunikasikan kepada pengelola manajemen keamanan informasi SPBE.
20. Pengelola manajemen keamanan informasi SPBE dan auditor internal keamanan SPBE bertanggung jawab untuk memantau dan memverifikasi koreksi, tindakan korektif maupun peningkatan terkait ketidaksesuaian yang ditemukan dalam audit.
21. Verifikasi dari auditor internal keamanan SPBE dibutuhkan sebelum ketidaksesuaian yang ditemukan dapat dinyatakan ditutup secara formal.

KEAMANAN SUMBER DAYA MANUSIA

A. Maksud dan Tujuan

Prosedur pengendalian keamanan sumber daya manusia ditetapkan untuk memberikan pedoman dalam mengelola keamanan sumber daya manusia dalam ruang lingkup manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah Kabupaten Kendal.

B. Ruang Lingkup

Ruang lingkup prosedur pengendalian keamanan sumber daya manusia terdiri
dari:

1. pegawai dalam lingkungan Pemerintah Daerah Kabupaten Kendal;
2. pegawai dari pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke aset informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Daerah Kabupaten Kendal.

C. Prosedur Pengendalian

1. Calon pegawai di lingkungan Pemerintah Daerah Kabupaten Kendal dan pegawai dari pihak eksternal, harus melalui proses *screening* untuk memastikan bahwa mereka sesuai dengan tugas dan tanggung jawab yang akan mereka dapatkan.
2. Proses *screening* perlu mencakup verifikasi terhadap latar belakang kandidat sesuai dengan peraturan hukum perundang-undangan serta etika yang ada.
3. Pegawai dalam lingkungan Pemerintah Daerah Kabupaten Kendal 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 Kendal harus menandatangani perjanjian kerahasiaan (*non-disclosure agreement*) dengan memperhatikan tingkat sensitivitas dari aset yang diakses.
4. Setiap pegawai internal maupun eksternal harus mematuhi seluruh kebijakan dan prosedur Perangkat Daerah terkait keamanan informasi.
5. Setiap pegawai internal maupun eksternal harus diberikan informasi yang memadai terkait tugas dan tanggung jawab terkait keamanan informasi yang mereka miliki.
6. Program peningkatan kesadaran keamanan informasi (*awareness*) secara berkelanjutan untuk menjaga dan meningkatkan kesadaran keamanan informasi dari pegawai harus dilaksanakan.
7. Setiap pelanggaran terhadap kebijakan dan prosedur terkait keamanan informasi harus ditindaklanjuti dan apabila diperlukan, tindakan pendisiplinan harus diambil sesuai dengan peraturan yang berlaku.
8. 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.
9. Hal ini mencakup tanggung jawab keamanan informasi yang tercakup dalam perjanjian kerja seperti:
    a. Seluruh aset organisasi harus dikembalikan setelah pemberhentian kepegawaian;
    b. Seluruh hak akses organisasi harus dinonaktifkan atau dihapus setelah pemberhentian kepegawaian; dan
    c. Seluruh hak akses organisasi harus disesuaikan setelah perubahan status kepegawaian.

KEAMANAN DENGAN PIHAK KETIGA

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian keamanan dengan pihak ketiga adalah untuk memastikan perlindungan atas aset Perangkat Daerah dalam jangkauan akses pihak ketiga dan memelihara tingkat layanan yang disetujui dari keamanan informasi sesuai dengan perjanjian dengan pihak ketiga.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian keamanan dengan pihak ketiga adalah para pihak ketiga dalam lingkungan Pemerintah Daerah Kabupaten Kendal.

C. Prosedur Pengendalian

1. Perangkat Daerah harus mempertimbangkan aspek keamanan informasi dalam hubungan dengan pihak ketiga mulai dari pemilihan, penunjukan, monitoring, evaluasi, sampai dengan terminasi.
2. Pemilihan dari penyedia jasa, Perangkat Daerah harus mengikuti kriteria berikut:
   a. kompetensi, pengalaman dan catatan dari organisasi;
   b. kepastian dari kemampuan penyedia jasa untuk menyediakan layanan;
   c. kepastian dari kemampuan penyedia jasa untuk menjaga ketersediaan dari penyediaan layanan pada saat kondisi normal atau kondisi bencana (apabila terjadi bencana alam atau kegagalan dalam penyediaan layanan);
3. Berdasarkan pengelompokan pihak ketiga yang telah bekerjasama, Perangkat Daerah wajib mendefinisikan pembatasan aset dan aset informasi apa saja yang diperbolehkan untuk diakses oleh setiap kelompok pihak ketiga, serta senantiasa memantau akses yang telah dilakukan.
4. Perangkat Daerah menetapkan persyaratan keamanan informasi bagi setiap pihak ketiga yang mengakses aset informasi, serta senantiasa memantau kepatuhan pihak ketiga terhadap persyaratan tersebut. Pihak ketiga yang menangani aset informasi dengan klasifikasi rahasia perlu menandatangani Perjanjian Kerahasiaan.
5. Kewajiban pihak ketiga dan tingkat layanan harus ditetapkan secara formal dalam kontrak kerja;
6. Perangkat Daerah harus memastikan pengelolaan *delivery* layanan dari pihak ketiga dengan memperhatikan:
   a. layanan yang diserahkan kepada Perangkat Daerah oleh pihak ketiga harus secara berkala dipantau, dan ditinjau;
   b. proses pemantauan dilakukan untuk memverifikasi kesesuaian dari tingkat layanan yang diberian dan prasyarat keamanan informasi dengan perjanjian kerja;
   c. proses peninjauan dilakukan untuk mengidentifikasi problem terkait penyediaan layanan dan aspek keamanan informasi dalam penyediaan layanan oleh pihak ketiga;
   d. peninjauan dari penyediaan layanan oleh pihak ketiga harus dilaksanakan paling sedikit satu kali dalam tiga bulan;
7. Perangkat Daerah dapat melakukan audit terhadap penyediaan layanan yang diberikan pihak ketiga;
8. Ketentuan dalam pelaksanaan audit kepada pihak ketiga sebagai berikut:

a. tanggung jawab untuk mengaudit tingkat layanan dimiliki oleh pihak, baik internal maupun eksternal, yang memiliki independensi dari pengguna layanan yang diberikan oleh pihak ketiga dan ditunjuk secara formal;
b. audit terhadap penyediaan layanan oleh pihak ketiga harus dilakukan paling sedikit satu kali dalam satu tahun;
c. setiap ketidaksesuaian yang ditemukan dalam proses peninjauan dan audit harus dikelola dan ditindaklanjuti;

9. Perubahan terhadap layanan yang diberikan oleh pihak ketiga harus dikelola, dengan memperhatikan kritikalitas dari proses bisnis pengguna layanan dan layanan yang diberikan oleh pihak ketiga;
10. Perubahan terhadap layanan yang diberikan oleh pihak ketiga harus dipastikan tidak akan mengganggu aspek kerahasiaan dari informasi serta integritas dan ketersediaan dari informasi dan layanan Perangkat Daerah;
11. Perubahan terhadap layanan yang diberikan oleh pihak ketiga harus disetujui oleh manajemen Perangkat Daerah yang relevan dan diformalisasikan dalam kontrak kerja.

PENGELOLAAN ASET

A. Maksud dan Tujuan

Maksud dan tujuan dari pengendalian prosedur pengelolaan aset informasi adalah untuk memberikan pedoman dalam mengelola aset yang terkait informasi serta fasilitas fisik pengolahan informasi, sehingga aset informasi mendapatkan perlindungan yang sesuai dengan tingkat kepentingannya.

B. Ruang Lingkup

Ruang lingkup kebijakan terkait pengelolaan aset terdiri dari:

1. klasifikasi, pelabelan dan penanganan informasi dalam ruang lingkup Peraturan Bupati Kendal terkait Manajemen Keamanan Informasi SPBE;
2. penanganan aset pengolahan dan penyimpanan informasi dalam ruang lingkup Peraturan Bupati Kendal; dan
3. seluruh aset informasi SPBE.

C. Prosedur Pengendalian

1. Anggota tim manajemen keamanan informasi SPBE menetapkan pemilik aset informasi di setiap unit Perangkat Daerah, beserta perangkat fisik pengolah informasi yang terkait.
2. Pemilik aset informasi memiliki tanggung jawab untuk:
   a. mengidentifikasi seluruh aset informasi dan fasilitas pengolahan dan penyimpanan informasi;
   b. mendokumentasikannya dalam daftar inventaris aset SPBE, serta senantiasa memperbaharui daftar inventaris aset SPBE tersebut sesuai kondisi terkini; dan
   c. memastikan bahwa setiap aset telah diklasifikasikan dan dilindungi secara memadai.
3. Aset pengolahan dan penyimpanan informasi yang diinventaris adalah aset dalam bentuk:
   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*, *harddisk 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.

4. Pemilik aset dapat mendelegasikan tugas pengamanan dan pemeliharaan aset kepada kustodian aset, namun tanggung jawab akhir terhadap aset tetap berada pada pemilik aset.
5. Aset pengolahan dan penyimpanan informasi harus secara berkala dipelihara dengan memadai.
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.
7. dalam proses penghapusan aset harus dilakukan secara aman dengan metode yang dapat mencegah kebocoran informasi seperti menghancurkan secara fisik *hard drive*.
8. Semua aset informasi dan pengolahan dan penyimpanan informasi milik Pemerintah Daerah Kabupaten Kendal harus dikembalikan setelah personil pengguna tidak memiliki hubungan kepegawaian lagi dengan Pemerintah Daerah Kabupaten Kendal, misalnya karena pengunduran diri, pensiun.
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.
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 sensitif yang tersimpan dalam aset tersebut.
11. Perangkat Daerah harus mendefinisikan klasifikasi aset informasi dengan mempertimbangkan sebagai berikut:
    a. Aset informasi diklasifikasikan berdasarkan tingkat sensitivitas informasi serta tingkat kritikalitas sistem, yang meliputi:
       1) klasifikasi aset informasi secara berkala; dan
       2) pengguna yang diijinkan mengakses aset informasi.
    b. pemberian label klasifikasi informasi harus dilakukan secara konsisten terhadap seluruh aset informasi;
    c. klasifikasi aset informasi dan seberapa tingkat kerahasiaan aset informasi, didefinisikan sesuai ketentuan peraturan perundang-undangan, diuraikan sesuai tabel berikut:

Klasifikasi Aset Informasi	**Deskripsi**
Rahasia (*Confidential*)	Aset informasi yang sangat peka dan berisiko tinggi yang pembocoran atau penyalahgunaan akses terhadapnya bisa mengganggu kelancaran oeprasional secara temporer atau mengganggu citra dan reputasi instansi.
Internal (*Internal Use Only*)	Informasi yang telah terdistribusi secara luas di lingkungan internal instansi/lembaga yang penyebarannya secara internal tidak lagi

	memerlukan izin dari pemilik informasi dan risiko penyebarannya tidak menimbulkan kerugian signifikan.
Publik	Aset informasi yang secara sengaja dipublikasikan secara luas, merupakan informasi yang wajib disediakan dan diumumkan secara berkala, informasi yang wajib diumumkan secara serta-merta, dan informasi yang wajib tersedia setiap saat.

Tabel 4. Tabel klasifikasi aset informasi

12. Untuk kepentingan penyelenggaraan pengelolaan aset informasi dalam Kebijakan Sistem Manajemen Keamanan Informasi perlu diberikan penjelasan contoh-contoh aset informasi rahasia dan internal, yaitu:

Klasifikasi Aset Informasi	**Contoh**
Rahasia (*Confidential*)	*User ID*, *Password*, *Personal Identification Number* (*PIN*), *Log* sistem, hasil *penetration test*, data konfigurasi sistem, *Internet Protocol Address* (IP *Address*)
Internal (*Internal Use Only*)	Panduan penggunaan sistem dan aplikasi, kebijakan dan prosedur SMKI, dokumen Kebijakan Manajemen Risiko, dokumen *risk register*

Tabel 5. Tabel contoh aset informasi

13. 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.
14. Panduan terkait pelabelan dan penanganan aset informasi berdasarkan klasifikasi aset informasi adalah sebagai berikut:

Klasifikasi Tipe	**Publik**	**Internal**	**Rahasia**
Dokumen dan catatan (*record*) dalam bentuk non elektronik (*hardcopy*).	Tidak diperlukan penanganan khusus	Diberi label "***Internal***"	Diberi label "***Rahasia***"
Map penyimpanan dokumen	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Diberi label "***Rahasia***"

Amplop pengiriman surat internal (di dalam kantor)	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Amplop diberi label "***Rahasia***"
Amplop untuk surat eksternal (ke luar kantor)	Tidak diperlukan penanganan khusus	Pada amplop ditandai "*Internal*"	• Menggunakan 2 amplop, dimana amplop pertama dimasukan kedalam amplop kedua; • Pada amplop pertama ditandai "Rahasia", dan pada amplop kedua tidak diberikan tanda apapun.
Dokumen dan catatan (*record*) dalam bentuk elektronik (softcopy)	Tidak diperlukan penanganan khusus	Memberikan label "Internal" pada bagian awal dari nama *file* atau pada bagian tertentu dari *file properties*.	Memberikan label "Rahasia" pada bagian awal dari nama *file* atau pada bagian tertentu dari *file properties*.
Publikasi / Distribusi	Tidak ada pembatasan	• Tersedia untuk personil internal PERANGKAT DAERAH pemilik informasi. • Distribusi kepada pihak eksternal dibatasi berdasarkan kebutuhan bisnis maupun operasional di lingkungan Pemda Kabupaten Kendal. • Distribusi kepada pihak eksternal perlu seijin pemilik informasi. • Sensitifitas dan kritikalitas informasi perlu diberitahukan kepada pihak eksternal.	• Distribusi kepada pihak eksternal sangat dibatasi untuk kebutuhan pekerjaan • Apabila memungkinkan, informasi rahasia tidak disalin oleh pihak eksternal (*eyes only*). • Distribusi kepada pihak eksternal perlu seijin pemilik informasi. • Sensitifitas dan kritikalitas informasi perlu diberitahukan kepada pihak eksternal. • Pihak ketiga harus disertai perjanjian kerahasiaan (NDA – *non disclosure agreement*).
Pencetakan Informasi	Tidak ada pembatasan	Dibatasi hanya untuk kebutuhan internal	Pencetakan hanya pada *printer* organisasi dan diusahakan tidak mencetak menggunakan jasa

			pencetakan eksternal
Surat menyurat internal (di dalam kantor)	Pastikan nama dan alamat tujuan sudah benar	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat internal.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat internal. • Menginformasikan kepada penerima akan pengiriman informasi tersebut. • Mengkonfirmasi kepada penerima bahwa informasi yang dikirim sudah diterima.
Surat menyurat eksternal (di luar kantor)	Pastikan nama dan alamat tujuan sudah benar	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat eksternal. • Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat eksternal. • Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman. • Menginformasikan kepada penerima akan pengiriman informasi tersebut. • Mengkonfirmasi kepada penerima bahwa informasi yang dikirim sudah diterima.
Pengiriman ke pihak internal melalui *email*	• Pengiriman *email* harus menggunakan akun *email* Perangkat Daerah. • Tidak diperlukan penanganan khusus	• Pengiriman *email* harus menggunakan akun *email* Perangkat Daerah. • Pastikan alamat *email* tujuan sudah benar. • Pengiriman informasi, termasuk *forwarding* / meneruskan *email* hanya boleh dilakukan oleh pemilik informasi.	• Pengiriman *email* harus menggunakan akun *email* Perangkat Daerah. • Memberi *password* pada informasi yang dikirim melalui *email* dan *password* diinformasikan kepada penerima secara terpisah. • Tidak mencantumkan

			informasi rahasia *body text email*. • Pengiriman informasi, termasuk *forwarding* / meneruskan *email* hanya boleh dilakukan oleh pemilik informasi.
Pengiriman ke pihak eksternal melalui *email*	• Pengiriman *email* harus menggunakan akun *email* Perangkat Daerah. • Tidak diperlukan penanganan khusus	• Pengiriman *email* harus menggunakan akun *email* Perangkat Daerah. • Pastikan alamat *email* tujuan sudah benar.	• Tidak disarankan menggunakan *email* untuk mengirim informasi dengan klasifikasi ini. • Pengiriman *email* harus menggunakan akun *email* Perangkat Daerah. • Pastikan alamat *email* tujuan sudah benar. • Memberi *password* pada informasi yang dikirim melalui *email* dan *password* diinformasikan kepada penerima secara terpisah.
Penyimpanan informasi *hardcopy*	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Disimpan secara aman dalam tempat penyimpanan yang terkunci.
Penyimpanan informasi *softcopy*	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	• Penyimpanan pada komputer atau media penyimpanan yang menggunakan *password*. • *File* yang disimpan harus diberi *password*. • Media penyimpanan eksternal (*external harddisk*, atau *flashdisk*) harus disimpan pada tempat penyimpanan yang terkunci.
Penyimpanan pada pihak ketiga	Tidak diperlukan penanganan khusus	Harus disertai dengan perjanjian kerahasiaan (*non*	Harus disertai dengan perjanjian kerahasiaan (*non*

		disclosure agreement - NDA)	*disclosure agreement* - NDA)
Penghancuran (*disposal*)	• Tidak diperlukan penanganan khusus. • Masih dapat digunakan kembali sebagai kertas untuk pekerjaan (*scrap paper*).	• Memperhatikan masa retensi informasi yang disetujui oleh pemilik informasi. • Masih dapat digunakan kembali untuk kebutuhan mencetak informasi dengan klasifikasi yang sama.	• Memperhatikan masa retensi informasi yang disetujui oleh pemilik informasi. • Dihancurkan dengan metode pemusnahan dan informasi tidak dapat diakses kembali (dihancurkan secara fisik atau *secure format*).
Pengamanan pada komputer penyimpanan informasi	Tidak diperlukan penanganan khusus	• *Screen saverlock* harus aktif jika meninggalkan komputer / terminal. • *Sign-off* komputer / terminal jika tidak digunakan atau pulang kerja.	• *Screen saverlock* harus aktif jika meninggalkan komputer / terminal. • *Sign-off* komputer / terminal jika tidak digunakan atau pulang kerja. • *File* perlu dienkripsi / *password*.
Kehilangan atau kebocoran informasi	Tidak diperlukan penanganan khusus	Harus dilaporkan kepada pemilik informasi	Harus dilaporkan kepada pemilik informasi dan unit kerja pengelola insiden keamanan informasi di lingkungan Pemerintah Daerah Kabupaten Kendal.

Tabel 6. Tabel panduan pelabelan dan pengamanan aset informasi

15. informasi yang dianggap kritikal oleh Perangkat Daerah harus di-*backup* secara memadai untuk menjamin ketersediaannya.
16. 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.

17. Perangkat Daerah menyediakan akses *internet* dan *email* kepada pegawainya hanya untuk kebutuhan pekerjaan dan operasional Pemerintah Daerah Kabupaten Kendal.
18. Ketentuan dalam pengguaan *internet* dan *email* adalah sebagai berikut:
    a. pengguna dilarang menggunakan akses *internet* dan *email* Perangkat Daerah untuk kegiatan melanggar hukum dan aktifitas yang dapat membahayakan keamanan jaringan Pemerintah Daerah Kabupaten Kendal;
    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 musik 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 Daerah Kabupaten Kendal.
19. pengguna disarankan untuk tidak membagi informasi pribadi melalui situs *internet* atau media sosial.
20. pengguna dilarang untuk mendistribusikan informasi Pemerintah Daerah Kabupaten Kendal yang bersifat rahasia tanpa izin dari pemilik informasi.
21. 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 Kabupaten Kendal tidak bertanggung jawab untuk pengiriman informasi ini secara lengkap dan tepat dan juga tidak bertanggung jawab untuk keterlambatan dalam pengiriman email ini."*
22. unit kerja yang mengelola akun *email* Perangkat Daerah berhak untuk mem-*block* akun *email* Pemerintah Daerah Kabupaten Kendal pada saat terdapat bukti memadai terkait penyalahgunaan dan/atau pelanggaran keamanan.

PELINDUNGAN DATA PRIBADI

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian pelindungan data pribadi adalah untuk melindungi keamanan data pribadi yang mencakup namun tidak terbatas pada data pribadi bersifat umum, data pribadi bersifat spesifik, subjek data pribadi, pengendali data pribadi, prosesor data pribadi serta proses pemrosesan data pribadi.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian pelindungan data pribadi adalah seluruh data pribadi yang dikendalikan dan diproses di lingkungan Pemerintah Daerah Kabupaten Kendal.

C. Ketentuan Umum

1. Data pribadi adalah data tentang ora.ng perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.
2. Pengendali data pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi.
3. Prosesor data pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan data pribadi atas nama pengendali data pribadi.
4. Subjek data pribadi adalah orang perseorangan yang pada dirinya melekat data pribadi.

D. Prosedur Pengendalian

1. Setiap perangkat daerah yang bertindak sebagai pengendali data pribadi maupun prosesor data pribadi wajib melindungi hak-hak subjek data pribadi.
2. Setiap perangkat daerah yang bertindak sebagai pengendali data pribadi maupun prosesor data pribadi wajib melindungi dan memastikan keamanan data pribadi.
3. Setiap perangkat daerah yang bertindak sebagai pengendali data pribadi maupun prosesor data pribadi wajib melakukan perekaman seluruh kegiatan pemrosesan data pribadi.
4. Setiap pemrosesan data pribadi wajib memiliki dasar dan tujuan pemrosesan data pribadi.
5. Setiap pemrosesan data pribadi wajib dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggung jawabkan.
6. Setiap pemrosesan data pribadi wajib dilakukan dengan melindungi keamanan data pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, penyalahgunaan, perusakan, dan/atau penghilangan data pribadi.
7. Data pribadi wajib dimusnahkan dan/atau dihapus setelah masa retensi berahir atau berdasarkan permintaan subjek data pribadi.
8. Setiap pemrosesan data pribadi wajib dilakukan secara bertanggung jawab dan dapat dibuktikan secara jelas.
9. Setiap perangkat daerah yang bertindak sebagai pengendali data pribadi wajib melakukan pemrosesan data pribadi secara terbatas dan spesifik, sah secara hukum, dan transparan.

10. Setiap perangkat daerah yang bertindak sebagai pengendali data pribadi wajib memberikan akses kepada subjek data pribadi terhadap data pribadi yang diproses beserta rekam jejak pemrosesan data pribadi sesuai dengan jangka waktu penyimpanan data pribadi.
11. Setiap perangkat daerah yang bertindak sebagai pengendali data pribadi wajib melakukan penilaian dampak pelindungan data pribadi dalam hal pemrosesan data pribadi memiliki potensi risiko tinggi terhadap subjek data pribadi.
12. Setiap perangkat daerah yang bertindak sebagai pengendali data pribadi wajib melindungi dan memastikan keamanan data pribadi yang diprosesnya, dengan melakukan:
    a. penyusunan dan penerapan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan data pribadi; dan
    b. penentuan tingkat keamanan data pribadi dengan memperhatikan sifat dan risiko dari data pribadi yang harus dilindungi dalam pemrosesan data pribadi.
13. Setiap perangkat daerah yang bertindak sebagai pengendali data pribadi wajib melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data pribadi di bawah kendali pengendali data pribadi.
14. Setiap perangkat daerah yang bertindak sebagai pengendali data pribadi wajib melindungi data pribadi dari pemrosesan yang tidak sah.
15. Setiap perangkat daerah yang bertindak sebagai pengendali data pribadi wajib bertanggung jawab atas pemrosesan data pribadi dan menunjukan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip pelindungan data pribadi.

KEAMANAN JARINGAN

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian keamanan jaringan adalah untuk memastikan keamanan pengiriman data terlindungi dari kehilangan, kerusakan dan akses oleh pihak yang tidak berwenang.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian keamanan jaringan adalah Jaringan Intra pemerintah dan jaringan intra instansi pusat dan daerah di lingkungan Pemerintah Daerah Kabupaten Kendal.

C. Prosedur Pengendalian

1. Perangkat Daerah diharuskan memenuhi standar teknis keamanan Jaringan Intra yang meliputi:
   a. aspek administrasi keamanan Jaringan Intra;
   b. kontrol akses dan autentikasi;
   c. persyaratan perangkat dan aplikasi keamanan Jaringan Intra;
   d. kontrol keamanan *gateway*;
   e. kontrol keamanan *access point* pada jaringan nirkabel; dan
   f. kontrol konfigurasi *access point* pada jaringan nirkabel.
2. Aspek administrasi keamanan Jaringan Intra dilakukan dengan prosedur sebagai berikut:
   a. menyusun dan mengevaluasi dokumen arsitektur Jaringan Intra;
   b. mengidentifikasi seluruh aset infrastruktur jaringan;
   c. menyusun dan menetapkan standar operasional prosedur terkait pemeliharaan keamanan Jaringan Intra; dan
   d. membuat laporan pengawasan keamanan jaringan secara periodik.
3. Kontrol akses dan autentikasi dilakukan dengan prosedur sebagai berikut:
   a. menempatkan perangkat infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah;
   b. menggunakan autentikasi untuk mengakses Jaringan Intra;
   c. menerapkan pembatasan akses dalam Jaringan Intra;
   d. mematikan atau membatasi *protocol*, *port*, dan layanan yang tidak digunakan;
   e. menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya;
   f. menerapkan fungsi *honeypot* untuk menganalisis celah keamanan berdasarkan jenis serangan;
   g. menerapkan *virtual private network* dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan;
   h. memberikan kewenangan hanya kepada administrator untuk menginstal perangkat lunak dan/atau mengubah konfigurasi sistem dalam Jaringan Intra;
   i. menerapkan *secure endpoints*;
   j. memblokir layanan yang tidak dikenal;
   k. menerapkan *secure socket layer* (SSL) atau *transport layer security* (TLS) versi terkini pada jalur akses Jaringan Intra; dan
   l. menerapkan *server* perantara saat *client* mengakses *server database* dalam rangka pemeliharaan.
4. Persyaratan perangkat dan aplikasi keamanan Jaringan Intra dilakukan dengan prosedur sebagai berikut:
   a. menggunakan perangkat *security information and event management* untuk *network logging* dan *monitoring*;

b. menerapkan sistem deteksi dini kerentanan keamanan perangkat jaringan;
c. menggunakan perangkat *firewall*;
d. menggunakan perangkat *intrusion detection systems* dan *intrusion prevention systems*;
e. menerapkan *virtual private network* terenkripsi untuk penggunaan akses jarak jauh secara terbatas;
f. menerapkan kontrol *update patching* pada infrastruktur Jaringan Intra dan sistem komputer;
g. menggunakan perangkat *web application firewall*;
h. menggunakan perangkat *load balancer* untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi;
i. memperbarui teknologi keamanan perangkat keras dan perangkat lunak untuk meminimalisasi celah peretas;
j. mengunduh perangkat lunak melalui *enterprise software distribution system*; dan
k. menerapkan sertifikat elektronik.

5. Kontrol keamanan *gateway* dilakukan dengan prosedur sebagai berikut:
   a. menerapkan *content filtering*;
   b. menerapkan *inspection packet filtering* untuk memeriksa *packet* yang masuk pada Jaringan Intra;
   c. menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat *gateway*;
   d. memastikan perangkat *gateway* yang menghubungkan antar Jaringan Intra tidak terkoneksi langsung dengan jaringan publik;
   e. melaksanakan manajemen *traffic gateway*; dan
   f. memastikan *port* tidak dibuka secara *default*.
6. Kontrol keamanan *access point* pada jaringan nirkabel dilakukan dengan prosedur sebagai berikut:
   a. menerapkan protokol keamanan *access point* nirkabel dan teknologi enkripsi terkini;
   b. menerapkan media *access control* pada *address filtering*;
   c. menerapkan *dedicated service set identifier*;
   d. menerapkan pembatasan jangkauan radio transmisi dan pengguna jaringan;
   e. menerapkan pembatasan terkait penambahan perangkat nirkabel yang dipasang secara tidak sah;
   f. menerapkan manajemen *vulnerability* secara berkala dan berkelanjutan; dan
   g. melakukan *patching firmware* secara rutin.
7. Kontrol konfigurasi *access point* pada jaringan nirkabel dilakukan dengan prosedur sebagai berikut:
   a. menggunakan kata sandi yang kuat;
   b. menggunakan protokol model *authentication authorization* dan *accounting* pada perangkat infrastruktur jaringan untuk *management user* atau otentikasi *administrator access point*;
   c. memastikan fitur akses konfigurasi jarak jauh hanya dapat digunakan dalam kondisi darurat dengan menerapkan kontrol keamanan;
   d. mengisolasi atau melakukan segmentasi jaringan area lokal nirkabel; dan
   e. menonaktifkan antarmuka nirkabel, layanan, dan aplikasi yang tidak digunakan.

KEAMANAN PUSAT DATA

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian pusat data adalah untuk memastikan keamanan seluruh data terlindungi dari kehilangan, kerusakan dan akses oleh pihak yang tidak berwenang.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian keamanan pusat data adalah pusat data di lingkungan Pemerintah Daerah Kabupaten Kendal.

C. Prosedur Pengendalian

1. Perangkat Daerah yang mengelola pusat data secara mandiri wajib memenuhi kriteria keamanan fisik dan lingkungan pusat data.
2. Perangkat Daerah wajib menerapkan kontrol akses fisik dan *logic* pusat data.
3. Memastikan hanya personil yang berwenang yang mendapat akses di area pusat data.
4. Memastikan hanya personil yang berwenang yang boleh menggunakan komputer di area pusat data.
5. Memastikan keamanan perangkat yang terhubung ke pusat data.
6. Memutus akses fisik dan *logic* dari perangkat yang tidak terotorisasi.
7. Memastikan akses tingkat administrator ke *server* dan perangkat jaringan utama tidak boleh dilakukan secara remote.
8. Melakukan *backup* informasi dan perangkat lunak yang berada di pusat data secara berkala.
9. Memastikan perangkat komputer pusat data terbebas dari virus dan *malware*.
10. Melakukan pembatasan akses pemanfaatan *removable media* di pusat data.
11. Memastikan pengaktifan konfigurasi *port universal serial bus* telah mendapatkan izin dari personil yang berwenang.
12. Memastikan setiap perangkat yang akan terkoneksi ke infrastruktur pusat data menggunakan *internet protocol address* dan *hostname* yang sudah ditentukan.
13. Menerapkan *server* perantara saat *client* mengakses *server database* dalam rangka pemeliharaan.

KEAMANAN PERANGKAT *ENDPOINT*

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian keamanan perangkat *endpoint* adalah untuk memastikan keamanan setiap perangkat *endpoint* di lingkungan Pemerintah Kabupaten Kendal.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian keamanan perangkat *endpoint* adalah setiap perangkat *endpoint* yang ada di lingkungan Pemerintah Daerah Kabupaten Kendal.

C. Prosedur Pengendalian

1. Endpoint merupakan perangkat fisik yang terhubung dan bertukar informasi dengan beberapa jaringan komputer. Contoh dari perangkat endpoint seperti perangkat seluler, *laptop*, komputer desktop, *virtual machine* (VM), dan *server* serta perangkat *internet of things* (IoT) seperti printer, televisi pintar, lampu, cctv dan lain sebagainya.
2. Setiap perangkat *endpoint* yang terhubung dengan jaringan intra Pemerintah Kabupaten Kendal harus terlindungi dari ancaman serangan siber.
3. Setiap perangkat endpoint diharuskan memasang *anti-virus* dan *anti-malware* ataupun *endpoint detection response*.
4. Setiap perangkat *enpoint* yang terhubung dengan jaringan intra pemerintah kabupaten kendal harus dilakukan kontrol oleh pengelola jaringan intra pada tiap Perangkat Daerah.
5. Seluruh *operating system* (OS), *driver*, dan aplikasi pada tiap perangkat *endpoint* diharuskan melakukan pembaruan versi dan pembaruan *patch* keamanan terbaru.
6. Menggunakan enkripsi pada perangkat maupun data yang bersifat sensitif.
7. Setiap perangkat daerah wajib melakukan peningkatan pengetahuan kesadaran keamanan perangkat *endpoint* pada seluruh karyawan.

KEAMANAN PENYIMPANAN ELEKTRONIK

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian keamanan penyimpanan elektronik adalah untuk memastikan keamanan sistem penyimpanan elektronik di lingkungan Pemerintah Kabupaten Kendal.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian keamanan penyimpanan elektronik adalah setiap penyimpanan elektronik tak terbatas pada penyimpanan berbasis *network* maupun *local* yang ada di lingkungan Pemerintah Daerah Kabupaten Kendal.

C. Prosedur Pengendalian

1. Setiap perangkat penyimpanan elektronik baik itu *data storage*, *server*, *Hard disk, Flash disk*, *Cloud storage,* kartu memori dan lain-lain harus terjamin keamanannya dari *virus*, *malware*, *ransomware* dan ancaman keamanan siber lainnya.
2. Penyimpanan elektronik yang digunakan untuk *server* harus menggunakan teknologi RAID untuk meminimalisir risiko kehilangan data ketika terjadi kegagalan perangkat penyimpanan elektronik.
3. Setiap akses ke penyimpanan elektronik secara fisik maupun *logic* untuk data dan informasi yang bersifat data pribadi wajib dilakukan oleh personil yang bertanggung jawab.
4. Setiap melakukan akses ke penyimpanan elektronik secara *remote* diwajibkan menggunakan *virtual private network* (VPN) terenkripsi AES-256 yang disediakan masing-masing Perangkat Daerah.
5. Setiap aktivitas yang dilakukan ke penyimpanan elektronik baik fisik maupun *logic* harus tercatat oleh sistem *logging* maupun buku catatan kunjungan.
6. Setiap data dan informasi penting yang tersimpan di penyimpanan elektronik harus di-*backup* secara rutin.
7. Hasil *backup* data dan informasi penting harus dilindungi oleh pengamanan fisik maupun *logic*.

KEAMANAN FISIK DAN LINGKUNGAN

A. Maksud dan Tujuan

Maksud dan tujuan dari kebijakan keamanan fisik dan lingkungan adalah untuk:

1. Mencegah akses atas aset informasi dan aset pengolahan dan penyimpanan informasi secara fisik oleh pihak yang tidak berwenang pada lingkungan Pemerintah Daerah Kabupaten Kendal; dan
2. Mencegah terjadinya kerusakan atau gangguan pada aset informasi dan aset pengolahan dan penyimpanan informasi pada lingkungan Pemerintah Daerah Kabupaten Kendal karena ancaman dari kondisi lingkungan.

B. Ruang Lingkup

Ruang lingkup kebijakan keamanan fisik dan lingkungan adalah pengamanan fisik dan lingkungan bagi area kerja dan penyimpanan perangkat pengolahan dan penyimpanan informasi, seperti Pusat Data, pusat data cadangan atau ruang arsip.

C. Prosedur Pengendalian

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 pusat data, pusat data cadangan 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 pusat data, pusat data cadangan dan ruang arsip Pemerintah Daerah Kabupaten Kendal; dan
   g. *delivery* dari barang harus dilaporkan dan diperiksa sebelum barang tersebut dapat dipindahkan dari area bongkar muat atau penerimaan barang ke pusat data, pusat data cadangan dan ruang arsip Pemerintah Daerah Kabupaten Kendal.
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 ketiga, harus dilaksanakan sesuai dengan kesepakatan tingkat layanan (*service level agreement/ SLA*) yang menjabarkan tingkat pemeliharaan dan kinerja yang harus dipenuhi pihak ketiga;
   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 Kendal, 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 pusat data 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 pusat data harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang kompeten dan berwenang sesuai dengan rekomendasi dari pembuat perangkat tersebut;
   c. pusat data harus dilengkapi dengan ups, generator listrik cadangan, perangkat pemadam kebakaran, dan diusahakan terdapat perlindungan kejut listrik (petir, tegangan tidak stabil);
   d. pusat data dan pusat data cadangan dilengkapi dengan sistem sensor deteksi asap, air, suhu dan kelembaban, yang dapat terpantau;
   e. parameter temperatur dan kelembaban berikut perlu dijaga untuk pusat data meliputi:
      1) temperatur antara 18° - 26° Celcius;
      2) kelembaban (rh) antara 40% - 60%.
   f. kabel listrik dan jaringan telekomunikasi yang membawa data atau mendukung layanan sistem informasi harus dilindungi dari penyambungan yang tidak sah (penyadapan) atau kerusakan

KEAMANAN AKSES KONTROL

A. Maksud dan Tujuan

Maksud dan tujuan dari keamanan akses kontrol adalah untuk:

1. membatasi akses terhadap informasi serta fasilitas fisik (pusat data);
2. memastikan sistem dan aplikasi diakses oleh pengguna yang telah diotorisasi, serta mencegah akses oleh yang tidak berhak; dan
3. memastikan pengguna bertanggung jawab untuk melindungi informasi otentikasi sensitif masing-masing.

B. Ruang Lingkup

Ruang lingkup dari keamanan akses kontrol adalah akses ke aset informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Daerah Kabupaten Kendal yang mencakup :

1. persyaratan pengendalian akses;
2. pengendalian akses jaringan;
3. pengelolaan akses pengguna;
4. tanggung jawab pengguna; dan
5. pengendalian akses atas sistem dan aplikasi.

C. Prosedur Pengendalian

1. Persyaratan pengendalian akses pada suatu sistem meliputi:
   a. akses ke aset informasi serta aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Daerah Kabupaten Kendal 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 Kendal 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 hukum perundang-undangan, kontraktual serta keamanan yang relevan;
      4) didasarkan atas prinsip *need to know* dan *need to use*, yaitu disesuaikan dengan kebutuhan pekerjaan dan operasional dalam lingkungan Pemerintah Daerah Kabupaten Kendal;
   e. aturan pemberian akses harus dikembangkan dan didokumentasikan oleh setiap pemilik system 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.
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. aringan 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 WAN, dilakukan melalui mekanisme formal.

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:
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:
g. pemilik Aset harus melakukan tinjauan secara berkala atas seluruh hak akses pengguna secara berkala, dengan tambahan tinjauan insidental yang dilakukan pada saat:
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 di-*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 Kendal harus diaktifkan.

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 simbol;
      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 Kendal harus diganti paling sedikit setiap 3 (tiga) bulan sekali;
   f. pada saat penggantian, *password* sebelumnya tidak boleh digunakan kembali sampai setelah 3 siklus pergantian *password*;
   g. prosedur *login* dari sistem harus menjamin keamanan dari *password* dengan cara:
      1) tidak menampilkan *password* yang dimasukkan;
      2) tidak menyediakan pesan bantuan pada saat proses *login* yang dapat membantu pengguna yang tidak berwenang;
   h. pengguna wajib menggunakan kata sandi yang berbeda untuk keperluan ketugasan dan pribadi.
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;
      3) membantu memberikan rekomendasi kata sandi yang berkualitas;
      4) mewajibkan pengguna untuk mengganti kata sandi pada saat pertama kali *login*;
      5) mewajibkan pengguna untuk mengganti kata sandi secara berkala;

6) menyimpan riwayat kata sandi pengguna dan mencegah agar pengguna tidak menggunakan kata sandi yang sebelumnya telah digunakan;
7) tidak menampilkan kata sandi saat sedang dientrikan; dan
8) 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;
4) adanya pembatasan jumlah akses pengguna yang sama secara simultan;

e. parameter otentikasi pengguna disesuaikan dengan klasifikasi aset informasi sebagai berikut:

Parameter Otentikasi	**Rahasia & Internal**	**Publik**
Jumlah gagal *login* sebelum penguncian	3	10
Durasi *timeout* sebelum terminasi sesi otomatis	5 menit	15 menit

Tabel 7. Tabel parameter otentikasi

6. 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.
7. 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.
8. Apabila *source code* dari penyedia jasa aplikasi tidak dapat diserahkan kepada pengelola aplikasi, Perangkat Daerah bersama penyedia jasa aplikasi tersebut harus mempertimbangkan *escrow aggreeement* untuk memastikan kelangsungan operasional sistem aplikasi jika ada pengembangan selanjutnya.
9. Pengendalian terhadap akses ke *source code* aplikasi sebagai berikut:
   a. 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.
   b. Pengendalian tersebut mencakup:
      1) Tidak menyimpan *source code* pada sistem operasional;
      2) Menyimpan *source code* pada lokasi fisik yang aman dari ancaman akses tanpa izin maupun ancaman kerusakan karena kondisi lingkungan;
      3) Membatasi akses secara fisik maupun *logical* ke *source code* program hanya kepada pengembang dan personil yang berwenang;
      4) Mengimplementasikan metode *versioning* dan proses manajemen perubahan untuk menjamin integritas dari *source code* aplikasi.

KEAMANAN APLIKASI SPBE

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian keamanan aplikasi SPBE adalah untuk memastikan keamanan dari setiap aplikasi SPBE serta keamanan pembangunan dan pengembangan aplikasi SPBE.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian keamanan aplikasi SPBE adalah setiap aplikasi SPBE berbasis web dan aplikasi SPBE berbasis *mobile* di lingkungan Pemerintah Daerah Kabupaten Kendal.

C. Prosedur Pengendalian

1. Prosedur pengendalian keamanan aplikasi SPBE diterapkan pada aplikasi berbasis web dan aplikasi berbasis *mobile*.
2. Aplikasi berbasis merupakan aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet.
3. Aplikasi berbasis *mobile* merupakan aplikasi yang dalam pengoperasiannya dapat berjalan diperangkat bergerak, dan memiliki sistem operasi yang mendukung perangkat lunak secara *standalone.*
4. Aplikasi SPBE harus dilakukan pengujian keamanan setiap periode tertentu yang dilakukan dengan:
   a. mengidentifikasi persyaratan minimum keamanan yang belum diterapkan;
   b. memastikan pengkodean pemrograman aplikasi yang dibuat tidak memiliki kerawanan;
   c. melakukan pemindaian otomatis dan/atau pengujian penetrasi sistem;
   d. mengidentifikasi kerentanan dan mengelola ancaman sejak awal siklus pengembangan Aplikasi SPBE; dan
   e. menganalisis kerentanan.

C.1 Keamanan Aplikasi Berbasis Web

1. Perangkat daerah diharuskan memenuhi prosedur pengendalian keamanan aplikasi berbasis web dengan terpenuhinya fungsi:
   a. autentikasi;
   b. manajemen sesi;
   c. persyaratan kontrol akses;
   d. validasi input;
   e. kriptografi pada verifikasi statis;
   f. penanganan eror dan pencatatan log;
   g. proteksi data;
   h. keamanan komunikasi;
   i. pengendalian kode berbahaya;
   j. logika bisnis;
   k. *file*;
   l. keamanan API dan *web service*; dan
   m. keamanan konfigurasi.
2. Terpenuhinya fungsi autentikasi dilakukan dengan prosedur sebagai berikut:
   a. menggunakan manajemen kata sandi untuk proses autentikasi;
   b. menerapkan verifikasi kata sandi pada sisi server;
   c. mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;

d. mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;
e. mengatur mekanisme pemulihan kata sandi;
f. menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi; dan
g. menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.

3. Terpenuhinya fungsi manajemen sesi dilakukan dengan prosedur sebagai berikut:
   a. menggunakan pengendali sesi untuk proses manajemen sesi;
   b. menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;
   c. mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi;
   d. mengatur kondisi dan jangka waktu habis sesi;
   e. validasi dan pencantuman *session id*;
   f. pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi; dan
   g. pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna.
4. Terpenuhinya fungsi persyaratan kontrol akses dilakukan dengan prosedur sebagai berikut:
   a. menetapkan otorisasi pengguna untuk membatasi kontrol akses;
   b. mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi;
   c. mengatur antarmuka pada sisi administrator; dan
   d. mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan.
5. Terpenuhinya fungsi validasi input dilakukan dengan prosedur sebagai berikut:
   a. menerapkan fungsi validasi input pada sisi server;
   b. menerapkan mekanisme penolakan input jika terjadi kesalahan validasi;
   c. memastikan *runtime environment* aplikasi tidak rentan terhadap serangan validasi input;
   d. melakukan validasi positif pada seluruh input;
   e. melakukan filter terhadap data yang tidak dipercaya;
   f. menggunakan fitur kode dinamis;
   g. melakukan pelindungan terhadap akses yang mengandung konten skrip; dan
   h. melakukan pelindungan dari serangan injeksi basis data.
6. Terpenuhinya fungsi kriptografi pada verifikasi statis dilakukan dengan prosedur sebagai berikut:
   a. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan;
   b. melakukan autentikasi data yang dienkripsi;
   c. menerapkan manajemen kunci kriptografi; dan
   d. membuat angka acak yang menggunakan generator angka acak kriptografi.
7. Terpenuhinya fungsi penanganan eror dan pencatatan log dilakukan dengan prosedur sebagai berikut:
   a. mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;

b. menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani;
c. tidak mencantumkan informasi yang dikecualikan dalam pencatatan log;
d. mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;
e. mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah;
f. melakukan enkripsi pada data yang disimpan untuk mencegah injeksi log; dan
g. melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.

8. Terpenuhinya fungsi proteksi data dilakukan dengan prosedur sebagai berikut:
   a. melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;
   b. melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi;
   c. melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan;
   d. melakukan penentuan jumlah parameter;
   e. memastikan data disimpan dengan aman;
   f. menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna; dan
   g. membersihkan memori setelah tidak diperlukan.
9. Terpenuhinya fungsi keamanan komunikasi dilakukan dengan prosedur sebagai berikut:
   a. menggunakan komunikasi terenkripsi;
   b. mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna;
   c. mengatur jenis algoritma yang digunakan dan alat pengujiannya; dan
   d. mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik.
10. Terpenuhinya fungsi pengendalian kode berbahaya dilakukan dengan prosedur sebagai berikut:
    a. menggunakan analisis kode dalam kontrol kode berbahaya;
    b. memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan;
    c. mengatur izin terkait fitur atau sensor terkait privasi;
    d. mengatur pelindungan integritas; dan
    e. mengatur mekanisme fitur pembaruan.
11. Terpenuhinya fungsi logika bisnis dilakukan dengan prosedur sebagai berikut:
    a. memproses alur logika bisnis dalam urutan langkah dan waktu yang realistis;
    b. memastikan logika bisnis memiliki batasan dan validasi;
    c. memonitor aktivitas yang tidak biasa;
    d. membantu dalam kontrol antiotomatisasi; dan
    e. memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.
12. Terpenuhinya fungsi *file* dilakukan dengan prosedur sebagai berikut:

a. mengatur jumlah *file* untuk setiap pengguna dan kuota ukuran *file* yang diunggah;
b. melakukan validasi *file* sesuai dengan tipe konten yang diharapkan;
c. melakukan pelindungan terhadap metadata input dan metadata *file*;
d. melakukan pemindaian *file* yang diperoleh dari sumber yang tidak dipercaya; dan
e. melakukan konfigurasi server untuk mengunduh *file* sesuai ekstensi yang ditentukan.

13. Terpenuhinya fungsi keamanan API dan *web service* dilakukan dengan prosedur sebagai berikut:
    a. melakukan konfigurasi layanan web;
    b. memverifikasi *uniform resource identifier* API tidak menampilkan informasi yang berpotensi sebagai celah keamanan;
    c. membuat keputusan otorisasi;
    d. menampilkan metode RESTful *hypertext transfer protocol* apabila input pengguna dinyatakan valid;
    e. menggunakan validasi skema dan verifikasi sebelum menerima input;
    f. menggunakan metode pelindungan layanan berbasis web; dan
    g. menerapkan kontrol antiotomatisasi.
14. Terpenuhinya fungsi keamanan konfigurasi dilakukan dengan prosedur sebagai berikut:
    a. mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan;
    b. mendokumentasi, menyalin konfigurasi, dan semua dependensi;
    c. menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan;
    d. memvalidasi integritas aset jika aset aplikasi diakses secara eksternal; dan
    e. menggunakan respons aplikasi dan konten yang aman.

C.2 Keamanan Aplikasi Berbasis Mobile

1. Perangkat daerah diharuskan memenuhi prosedur pengendalian keamanan aplikasi berbasis *mobile* dengan terpenuhinya fungsi:
    a. penyimpanan data dan persyaratan privasi;
    b. kriptografi;
    c. autentikasi dan manajemen sesi;
    d. komunikasi jaringan;
    e. interaksi platform;
    f. kualitas kode dan pengaturan *build*; dan
    g. ketahanan.
2. Terpenuhinya fungsi penyimpanan data dan persyaratan privasi dilakukan dengan prosedur sebagai berikut:
    a. menyimpan seluruh data dan informasi yang dikecualikan hanya dalam fasilitas penyimpanan kredensial sistem;
    b. membatasi pertukaran data dan informasi yang dikecualikan dengan *third party*;
    c. menonaktifkan *cache keyboard* pada saat memasukkan data dan informasi yang dikecualikan;
    d. melindungi informasi yang dikecualikan saat terjadi *inter process communication*; dan
    e. melindungi data dan informasi yang dikecualikan yang dimasukkan melalui antarmuka pengguna.

3. Terpenuhinya fungsi kriptografi dilakukan dengan prosedur sebagai berikut:
   a. menghindari penggunaan kriptografi simetrik dengan *hardcoded key*;
   b. mengimplementasikan metode kriptografi yang sudah teruji sesuai kebutuhan;
   c. menghindari penggunaan protokol kriptografi atau algoritma kriptografi yang obsolet;
   d. menghindari penggunaan kunci kriptografi yang sama; dan
   e. menggunakan pembangkit kunci acak yang memenuhi kriteria keacakan kunci.
4. Terpenuhinya fungsi autentikasi dan manajemen sesi dilakukan dengan prosedur sebagai berikut:
   a. menerapkan autentikasi pada *remote endpoint* terhadap aplikasi yang menyediakan akses pengguna untuk layanan jarak jauh;
   b. menggunakan *session identifier* yang acak tanpa perlu mengirimkan kredensial pengguna apabila menggunakan *stateful* manajemen sesi;
   c. memastikan server menyediakan token yang telah ditandatangani menggunakan algoritma yang aman apabila menggunakan autentikasi *stateless* berbasis token;
   d. memastikan remote endpoint memutus sesi yang ada saat pengguna *log out*;
   e. menerapkan pengaturan sandi pada *remote endpoint*;
   f. membatasi jumlah percobaan *log in* pada *remote endpoint*;
   g. menentukan masa berlaku sesi dan masa kedaluwarsa token pada *remote endpoint*; dan
   h. melakukan otorisasi pada *remote endpoint*.
5. Terpenuhinya fungsi komunikasi jaringan dilakukan dengan prosedur sebagai berikut:
   a. menerapkan *secure socket layer* atau *transport layer security* yang tidak obsolet secara konsisten; dan
   b. memverifikasi sertifikat *remote endpoint*.
6. Terpenuhinya fungsi interaksi platform dilakukan dengan prosedur sebagai berikut:
   a. memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan;
   b. melakukan validasi terhadap seluruh input dari sumber eksternal dan pengguna;
   c. menghindari pengiriman fungsionalitas sensitif melalui skema *custom uniform resource locator* dan fasilitas *inter process communication*;
   d. menghindari penggunaan *JavaScript* dalam *WebView*;
   e. menggunakan protokol *hypertext transfer protocol secure* pada *WebView*; dan
   f. mengimplementasikan penggunaan serialisasi API yang aman.
7. Terpenuhinya fungsi kualitas kode dan penguatan *build* dilakukan dengan prosedur sebagai berikut:
   a. menandatangani aplikasi dengan sertifikat yang valid;
   b. memastikan aplikasi dalam mode rilis;
   c. menghapus simbol *debugging* dari *native binary*;
   d. menghapus kode *debugging* dan kode bantuan pengembang;
   e. mengidentifikasi kelemahan seluruh komponen *third party*;
   f. menentukan mekanisme penanganan eror;

g. mengelola memori secara aman; dan
h. mengaktifkan fitur keamanan yang tersedia.

8. Terpenuhinya fungsi ketahanan dilakukan dengan prosedur sebagai berikut:
   a. mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi yang tidak sah;
   b. mendeteksi dan merespons *debugger*;
   c. mencegah *executable file* melakukan perubahan pada sumber daya perangkat;
   d. mendeteksi dan merespons keberadaan perangkat *reverse engineering*;
   e. mencegah aplikasi berjalan dalam *emulator*;
   f. mendeteksi perubahan kode dan data di ruang memori;
   g. menerapkan fungsi *device binding* dengan menggunakan *property* unik pada perangkat;
   h. melindungi seluruh *file* dan *library* pada aplikasi; dan
   i. menerapkan metode *obfuscation*.

KEAMANAN SISTEM PENGHUBUNG LAYANAN

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian keamanan sistem penghubung layanan adalah untuk memastikan keamanan dari sistem penghubung layanan yang ada di lingkungan Pemerintah Kabupaten Kendal.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian keamanan sistem penghubung layanan adalah seluruh sistem penghubung layanan di lingkungan Pemerintah Daerah Kabupaten Kendal.

C. Prosedur Pengendalian

1. Setiap Perangkat daerah diharuskan memenuhi prosedur pengendalian keamanan sistem penghubung layanan dengan terpenuhinya fungsi:
   a. keamanan interoperabilitas data dan informasi;
   b. kontrol sistem integrasi;
   c. kontrol perangkat integrator;
   d. keamanan API dan *web service*; dan
   e. keamanan migrasi data.
2. Terpenuhinya fungsi keamanan interoperabilitas data dan informasi dilakukan dengan prosedur sebagai berikut:
   a. menerapkan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik;
   b. menerapkan sistem enkripsi data;
   c. memastikan data dan informasi selalu dapat diakses sesuai otoritasnya; dan
   d. menerapkan sistem *hash function* pada *file*.
3. Terpenuhinya kontrol sistem integrasi dilakukan dengan prosedur sebagai berikut:
   a. menerapkan protokol *secure socket layer* atau protokol *transport layer security* versi terkini pada sesi pengiriman data dan informasi;
   b. menerapkan *internet protocol security* untuk mengamankan transmisi data dalam jaringan berbasis *transmission control protocol/ internet protocol*;
   c. menerapkan sistem anti *distributed denial of service*;
   d. menerapkan autentikasi untuk memverifikasi identitas eksternal antar Layanan SPBE yang terhubung;
   e. menerapkan manajemen keamanan sesi;
   f. menerapkan pembatasan akses pengguna berdasarkan otorisasi yang telah ditetapkan;
   g. menerapkan validasi input;
   h. menerapkan kriptografi pada verifikasi statis;
   i. menerapkan sertifikat elektronik pada *web authentication*;
   j. menerapkan penanganan eror dan pencatatan *log*;
   k. menerapkan proteksi data dan jalur komunikasi;
   l. menerapkan pendeteksi virus untuk memeriksa beberapa konten *file*;
   m. menetapkan perjanjian tingkat layanan dengan standar paling rendah 95% (sembilan puluh lima per seratus); dan
   n. memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.
4. Terpenuhinya fungsi kontrol perangkat integrator dilakukan dengan prosedur sebagai berikut:

a. menggunakan sistem operasi dan perangkat lunak dengan *security patches* terkini;
b. menggunakan anti virus dan anti-*spyware* terkini;
c. mengaktifkan fitur keamanan pada peramban web;
d. menerapkan *firewall* dan *host-based intrusion detection systems*;
e. mencegah instalasi perangkat lunak yang belum terverifikasi;
f. mencegah akses terhadap situs yang tidak sah; dan
g. mengaktifkan sistem *recovery* dan *restore* pada perangkat integrator.

5. Terpenuhinya fungsi keamanan API dan *web service* dilakukan dengan prosedur sebagai berikut:
   a. menerapkan protokol *secure socket layer* atau protokol *transport layer security* diantara pengirim dan penerima API;
   b. menerapkan protokol *open authorization* versi terkini untuk menjembatani interaksi antara *resource owner*, *resource server* dan/atau *third party*;
   c. menampilkan metode *RESTful hypertext transfer protocol* apabila input pengguna dinyatakan valid;
   d. melindungi layanan web *RESTful* yang menggunakan *cookie* dari *cross-site request forgery*; dan
   e. memvalidasi parameter yang masuk oleh penerima API untuk memastikan data yang diterima valid dan tidak menyebabkan kerusakan.
6. Terpenuhinya fungsi keamanan migrasi data dilakukan dengan prosedur sebagai berikut:
   a. memastikan migrasi data dilakukan secara bertahap dan terprogram oleh sistem;
   b. memastikan aplikasi yang menggunakan sistem basis data lama tetap dipertahankan sampai sistem pendukung basis data baru dapat berjalan atau berfungsi dengan normal;
   c. mendokumentasikan format sistem basis data lama secara rinci;
   d. melakukan pencadangan seluruh data yang tersimpan pada sistem sebelum melakukan migrasi data;
   e. menerapkan teknik kriptografi pada proses penyimpanan dan pengambilan data; dan
   f. melakukan validasi data ketika proses migrasi data selesai.

KEAMANAN KOMUNIKASI

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian keamanan komunikasi adalah untuk:

1. memastikan perlindungan atas informasi pada jaringan komputer beserta fasilitas pendukung pengolahan informasi;
2. menjaga keamanan informasi yang dipertukarkan, baik di dalam Perangkat Daerah maupun antar Perangkat Daerah eksternal.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian keamanan komunikasi adalah untuk:

1. pengendalian jaringan;
2. keamanan layanan jaringan;
3. pemisahan jaringan; dan
4. pertukaran informasi.

C. Prosedur Pengendalian

1. Jaringan internal Perangkat Daerah harus diamankan untuk menjamin:
   a. pencegahan akses tanpa izin ke jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan;
   b. keamanan dari informasi milik organisasi yang dikirimkan melalui jaringan; dan
   c. integritas dan ketersediaan dari layanan jaringan organisasi.
2. Tugas dan tanggung jawab untuk pengelolaan jaringan dan keamanan harus dialokasikan dan apabila memungkinkan dipisahkan dari penanggung jawab opersional sistem aplikasi dan Pusat Data.
3. Konfigurasi dari jaringan, perangkat aktif dan perangkat keamanan jaringan harus ditinjau secara berkala untuk:
   a. memastikan kesesuaian dengan kondisi terkini; dan
   b. mengidentifikasi kerawanan pada jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan.
4. Jaringan internal Perangkat Daerah harus dipisahkan dari jaringan eksternal dengan menggunakan *security gateway* atau *firewall* dan harus dikonfigurasikan untuk:
   a. memfilter *traffic* tanpa izin maupun *traffic* yang mencurigakan; dan
   b. apabila memungkinkan memfilter dan mencegah infeksi *malware* ke jaringan internal.
5. 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.
6. Kebijakan dan *log firewall* harus ditinjau paling sedikit 1 (satu) kali dalam tiga bulan.
7. Koneksi eksternal harus diputuskan secara otomatis setelah tidak aktif selama 5 menit.
8. 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.
9. 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.

10. Segmentasi jaringan harus ditinjau paling sedikit 1 (satu) kali dalam tiga bulan untuk menjamin kesesuaian dengan prasyarat keamanan terkini.
11. *Routing* jaringan harus dilakukan berdasarkan pengendalian terhadap alamat sumber dan tujuan.
12. Tanggung jawab untuk merubah *routing* jaringan hanya diberikan kepada administrator jaringan yang diberi izin.
13. Aturan untuk *routing* harus ditinjau paling tidak satu kali dalam tiga bulan untuk mendeteksi dan mengkoreksi adanya kesalahan atau *routing* tanpa otorisasi.
14. Perangkat jaringan harus ditempatkan pada lokasi yang aman untuk menghindari akses tanpa izin dan ancaman fisik maupun lingkungan.
15. Akses, baik fisik maupun *logical* ke perangkat jaringan harus dibatasi untuk tujuan administrasi dan pemeliharaan jaringan.
16. *Port* dan layanan jaringan, baik fisik maupun *logical*, yang tidak digunakan tidak boleh diaktifkan.
17. 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 OPD
    c. aplikasi monitoring jaringan dan keamanan jaringan yang telah disetujui.
18. Semua perangkat jaringan harus dapat diidentifikasi secara fisik maupun *logical* dengan penamaan yang disepakati dan konsisten.
19. Perangkat jaringan yang dimiliki oleh pihak eksternal harus secara memadai dipisahkan dari perangkat jaringan milik Perangkat Daerah.
20. Mekanisme keamanan, tingkat layanan dan prasyarat lain untuk semua layanan jaringan harus diidentifikasi dan dimasukkan kedalam perjanjian layanan jaringan.
21. Akses ke layanan jaringan Perangkat Daerah hanya diberikan kepada personil yang terotorisasi berdasarkan prinsip *need to have*.
22. Penggunaan pihak ketiga penyedia layanan jaringan harus dimonitor untuk menjamin kesesuaian dengan prasyarat keamanan Perangkat Daerah.
23. 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.
24. 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 didalamnya memuat:
    a. 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;
    b. hak dari pemilik aset informasi untuk melakukan audit dan pemantauan aktivitas penerima informasi berkaitan dengan penggunaan informasi sensitif; dan
    c. konsekuensi yang harus ditanggung penerima informasi apabila terjadi pelanggaran atas perjanjian kerahasiaan.

KEAMANAN DALAM PROSES AKUISISI, PENGEMBANGAN DAN PEMELIHARAAN SISTEM INFORMASI

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi adalah untuk:

1. Memastikan keamanan informasi sebagai bagian tak terpisahkan dari siklus hidup (*lifecycle*) sistem informasi. Termasuk persyaratan untuk sistem informasi yang menyediakan layanan melalui jaringan publik
2. Memastikan keamanan informasi didesain dan diimplementasikan dalam siklus hidup (*lifecycle*) pengembangan dari sistem informasi.
3. Memastikan perlindungan terhadap penggunaan data untuk pengujian.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi adalah untuk:

1. persyaratan keamanan sistem informasi;
2. keamanan dalam proses pengembangan dan *support*;
3. data pengujian.

C. Prosedur Pengendalian

1. Perangkat Daerah harus menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi yang relevan sebelum pengembangan, perluasan, atau pengadaan sistem informasi baru.
2. Persyaratan keamanan harus diidentifikasi secara jelas di dalam dokumen persyaratan dan spesifikasi perangkat lunak (*Software Requirement and Specification*).
3. Spesifikasi ini harus disetujui oleh pemilik informasi, pemilik proses bisnis dan pengembang sistem, sebelum fase pengkodean (*coding*) dalam pengembangan sistem.
4. Informasi yang digunakan oleh aplikasi Perangkat Daerah yang ditransimisikan melalui jaringan publik (internet) harus diamankan dari aktivitas penipuan, kemungkinan adanya perselisihan kontrak, dan pengungkapan dan/atau perubahan informasi tanpa izin.
5. Pengamanan informasi terhadap informasi yang ditransmisikan melalui sistem informasi yang digunakan dapat mencakup namun tidak terbatas pada:
   a. Proses otentikasi dan otorisasi terhadap pengguna aplikasi;
   b. Perlindungan untuk memastikan kerahasiaan dan integritas informasi yang dipertukarkan melalui jaringan publik;
   c. Perlindungan terhadap *session* transaksi untuk menghindari duplikasi dan/atau modifikasi;
   d. Mengamankan jalur komunikasi antara pihak-pihak yang terlibat.
6. Keamanan dalam proses pengembangan dan dukungan yang perlu dipertimbangkan oleh Perangkat Daerah meliputi:
   a. 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) pengedalian versi aplikasi;
      4) penyimpanan dari *source code*;

5) metode pengujian untuk mengidentifikasi dan memperbaiki *vulnerability*.

7. Perubahan terhadap sistem selama siklus pengembangan sistem harus dikendalikan melalui proses manajemen perubahan yang berlaku di Perangkat Daerah;
8. 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;
9. Perangkat Daerah harus menetapkan lingkungan pengembangan yang aman untuk pengembangan dan integrasi sistem Perangkat Daerah. Hal ini dapat mencakup namun tidak terbatas pada:
    a. Pemisahan lingkungan pengembangan baik secara fisik dan/atau *logical*;
    b. Pengendalian akses;
    c. Perpindahan data dari dan ke lingkungan pengembangan;
10. Perangkat Daerah harus mengawasi aktivitas pengembangan sistem yang dialihdayakan (*outsourced*). Hal ini dapat mencakup:
    a. perjanjian terkait lisensi dan kepemilikan sistem;
    b. pengujian penerimaan sistem untuk menguji kualitas dan akurasi dari sistem;
    c. prasyarat dokumentasi untuk sistem;
    d. perjanjian dengan pihak ketiga sebagai penjamin;
    e. hak untuk melakukan audit proses pengembangan dan kontrol yang diimplementasikan oleh vendor.
11. Pengujian dari fitur keamanan sistem harus dilakukan pada saat pengembangan sistem informasi Perangkat Daerah;
12. Pengujian ini dilakukan berdasarkan prasyarat keamanan sistem yang telah ditetapkan;
13. Kriteria dan jadwal untuk pengujian penerimaan sistem harus ditetapkan untuk sistem informasi baru, *upgrade* dan versi baru dari sistem informasi Perangkat Daerah;
14. Pengujian penerimaan sistem harus dilakukan sesuai dengan kriteria dan jadwal yang ditetapkan.
15. Pengamanan terhadap data hasil pengujian perlu diperhatikan sebagai berikut:
    a. data untuk pengujian sistem harus dipilih secara hati-hati untuk menghindari pengungkapan atau perubahan informasi sensitif oleh pihak yang tidak berhak, serta melindung dari kemungkinan kerusakan dan kehilangan informasi;
    b. *masking* data harus dilakukan apabila data operasional yang sensitif digunakan untuk keperluan pengujian;
    c. data operasional yang digunakan untuk keperluan pengujian harus dihapus segera setelah proses pengujian telah selesai dilaksanakan.

KRIPTOGRAFI

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian terkait teknologi kriptografi adalah untuk memastikan penggunaan teknologi kriptograpi yang sesuai dan efektif untuk melindungi kerahasiaan, keaslian dan/atau integritas dari informasi dalam lingkungan Pemerintah Daerah Kabupaten Kendal.

B. Ruang Lingkup

Ruang lingkup prosedur pngendalian terkait teknologi kriptografi adalah penggunaan teknologi kriptografi dalam pengolahan dan penyimpanan informasi di lingkungan Pemerintah Daerah Kabupaten Kendal.

C. Prosedur Pengendalian

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;
   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 kontrol 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 *dual custody* untuk mengurangi risiko penyalahgunaan.

PENANGANAN INSIDEN KEAMANAN INFORMASI

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian penanganan insiden keamanan informasi adalah untuk memastikan adanya pendekatan yang konsisten dan efektif atas penanganan insiden keamanan informasi.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian penanganan insiden keamanan informasi adalah:

1. tanggung jawab dan prosedur;
2. pelaporan atas kejadian insiden keamanan informasi; dan
3. pelaporan atas kelemahan keamanan informasi.

C. Prosedur Pengendalian

1. 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.
2. 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.
3. 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.
4. Guna memastikan proses penanganan insiden yang responsif dan efektif, perlu dikembangkan berbagai prosedur yang mencakup:
   a. perencanaan dan persiapan penanganan insiden;
   b. pemantauan, analisis, dan pelaporan atas insiden;
   c. pencatatan atas aktivitas penanganan insiden;
   d. penanganan bukti forensik;
   e. penilaian dan pengambilan keputusan atas insiden dan kelemahan keamanan informasi; dan
   f. pemulihan insiden.
5. 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.
6. Setiap kejadian insiden keamanan informasi harus dianalisis, diklasifikasikan,dan ditentukan skala prioritas penanganannya. Penanganan insiden beserta pemulihannya dilakukan berdasarkan klasifikasi dan prioritas yang telah ditetapkan.
7. Perangkat Daerah harus mengklasifikasikan insiden keamanan informasi untuk memprioritaskan penanganan insiden. Klasifikasi insiden tersebut adalah sebagai berikut:
   a. insiden keamanan informasi diklasifikasikan berdasarkan dampaknya menjadi berikut:
      1) mayor, apabila insiden tersebut menyebabkan terhentinya proses operasional pekerjaan Perangkat Daerah;
      2) minor, apabila insiden tersebut menyebabkan gangguan yang tidak menghentikan proses operasional pekerjaan Perangkat Daerah.

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

8. 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.
9. Setiap tindakan yang diidentifikasi untuk menangani kejadian, kelemahan dan insiden keamanan informasi harus dikonsultasikan kepada koordinator Tim Tanggap Insiden Siber (CSIRT) dan/atau personil yang kompeten dan relevan dengan kejadian, kelemahan dan insiden keamanan informasi.
10. Setiap tindakan penanganan kejadian, kelemahan dan insiden keamanan informasi harus didokumentasikan dengan baik.

KEAMANAN OPERASIONAL SISTEM INFORMASI

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian keamanan operasional sistem informasi adalah untuk:

1. memastikan pengoperasian aset pengolahan dan penyimpanan informasi di Pemerintah Daerah Kabupaten Kendal secara benar dan aman;
2. memastikan terlindunginya aset informasi beserta aset pengolahan dan penyimpanan informasi di Pemerintah Daerah Kabupaten Kendal dari ancaman *malware*;
3. melindungi terjadinya kehilangan atas aset informasi;
4. tersedianya catatan (*log*) atas aktivitas sistem informasi sebagai barang bukti; dan
5. mencegah terjadinya eksploitasi atas kelemahan sistem informasi pada Pemerintah Daerah Kabupaten Kendal.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian keamanan operasional sistem informasi adalah pengoperasian aset pengolahan dan penyimpanan informasi di lingkungan Pemerintah Daerah Kabupaten Kendal.

C. Prosedur Pengendalian

1. aktivitas operasional terkait fasilitas pengolahan informasi serta fasilitas komunikasi harus memiliki prosedur yang terdokumentasi dengan baik;
2. prosedur operasional tersebut harus tersedia bagi pengguna yang memerlukannya;
3. seluruh perubahan pada fasilitas pengolahan informasi yang dapat berimplikasi pada keamanan informasi, perlu diperlakukan secara terkendali, mencakup antara lain:
   a. menyusun perencanaan mengenai perubahan yang mungkin terjadi serta melakukan pengujian terkait terpenuhinya persyaratan keamanan;
   b. melakukan kajian atas implikasi keamanan informasi yang mungkin terjadi;
   c. mengajukan persetujuan secara formal atas perubahan yang akan dilakukan; dan
   d. mencatat seluruh perubahan yang telah dilakukan.
4. 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.
5. untuk mengurangi risiko perubahan tanpa izin atau penyalahgunaan hak akses, pemisahan fasilitas pengembangan, pengujian, dan operasional harus dilakukan.
6. setiap sistem informasi di lingkungan Perangkat Daerah harus terlindungi dari *malware* secara memadai melalui:
   a. instalasi dari perangkat lunak *antivirus* pada sistem informasi;
   b. mem-*block* akses ke *website* yang dapat menimbulkan ancaman kepada sistem informasi;
   c. program peningkatan kesadaran bagi personil organisasi untuk menangani ancaman *malware*; dan
   d. setiap insiden terkait dengan *malware* harus dilaporkan kepada *administrator* sistem dan dikategorikan sebagai insiden keamanan informasi.

7. seluruh aset informasi yang berada di dalam fasilitas pengolahan informasi wajib dilakukan *backup*, dengan persyaratan berikut:
   a. *backup* mencakup aplikasi, *database*, dan *system image*;
   b. frekuensi backup dilakukan secara harian, bulanan, dan tahunan;
   c. salinan *backup* harus disimpan secara aman sesuai dengan periode retensi. periode retensi *backup* adalah 1 tahun, dimana:
      1) *backup* harian disimpan selama 31 hari;
      2) *backup* bulanan disimpan selama 12 bulan;
   d. seluruh hasil *backup* harus dilakukan uji *restore* secara berkala;
   e. media *backup* disimpan pada perangkat *storage* yang terpisah dari perangkat pengolahan informasi utama;
   f. *backup* merupakan tanggung jawab pengelola pusat data, sedangkan pengujian *restore* merupakan tanggung jawab pemilik aset informasi;
   g. parameter *backup* disesuaikan dengan klasifikasi sistem sebagai berikut:

Parameter *Backup*	**Klasifikasi Sistem**	
	Vital	***Sensitive/ Non-Sensitive***
Cakupan *Backup*	Aplikasi, *Database*	Aplikasi, *Database*
Frekuensi *Backup* (*Recovery Point Objective*)	Harian	Bulanan
Pengujian *Restore*	Triwulan	Semesteran

Tabel 8. Tabel parameter backup sesuai klasifikasi

8. 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.
9. fasilitas pencatatan *log* dan informasi *log* yang dicatat harus dilindungi dari penghapusan dan akses oleh pihak yang tidak berwenang.
10. semua fasilitas pemrosesan informasi yang terhubung ke jaringan internal Perangkat Daerah harus disinkronisasi dengan sumber waktu yang akurat dan telah disepakati.
11. proses dan prosedur untuk mengendalikan instalasi perangkat lunak pada sistem operasional harus ditetapkan dan diimplementasikan untuk memastikan terjaganya kerahasiaan, integritas dan keterseiaan informasi.
12. instalasi perangkat lunak harus dilakukan oleh administrator sistem yang relevan.
13. 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 resiko atas hilangnya aset informasi. Tindakan pengendalian dapat berupa penonaktifan fitur tertentu, perbaikan/upgrade sistem, aplikasi, atau *patching*.
14. 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:
    a. harus direncanakan dan dikelola dengan baik untuk meminimalisasi gangguan terhadap proses bisnis;
    b. setiap proses audit yang membutuhkan akses kepada sistem informasi dan/atau informasi Perangkat Daerah harus disetujui oleh pemilik dari sistem dan/atau informasi tersebut;

c. hak akses untuk kebutuhan audit harus dibatasi hanya hak akses *read only*; dan
d. instalasi dari *tools* yang digunakan untuk proses audit hanya dapat dilakukan oleh personil yang berwenang yaitu administrator jaringan dan sistem TI di Perangkat Daerah, dan harus segera dihapus setelah proses audit telah selesai dilakukan.

KEPATUHAN

A. Maksud dan Tujuan

Maksud dan tujuan dari prosedur pengendalian 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.

B. Ruang Lingkup

Ruang lingkup dari prosedur pengendalian kepatuhan adalah:

1. kepatuhan dengan prasyarat hukum dan kontraktual;
2. peninjauan keamanan informasi.

C. Prosedur Pengendalian

1. Pemerintah Daerah Kabupaten Kendal berkomitmen untuk menjaga kepatuhan terhadap setiap prasyarat keamanan informasi yang relevan. Prasyarat keamanan informasi yang dimaksud mencakup prasyarat hukum, regulasi dan kontraktual;
2. Seluruh prasyarat hukum, regulasi dan kontraktual yang terkait dengan keamanan informasi dan berlaku bagi Perangkat Daerah harus diidentifikasikan, didokumentasikan dan dipelihara;
3. Perangkat Daerah harus mematuhi hak atas kekayaan intelektual yang terkait dengan material yang digunakan oleh Perangkat Daerah seperti:
   a. penggunaan perangkat lunak dan material yang bersifat *proprietary* harus mematuhi undang-undang terkait hak atas kekayaan intelektual (haki) yang berlaku;
   b. bukti dari lisensi atau izin resmi harus didapatkan dan disimpan untuk seluruh materi berlisensi /*copyright* yang di-*install*;
   c. lisensi yang bersifat berlangganan/harus diperbaharui dalam jangka waktu tertentu, harus dikelola untuk memastikan penggunaannya secara legal dan berkesinambungan;
   d. penggunaan lisensi dari materi berlisensi/*copyright* harus dikendalikan dengan baik;
4. Dokumen-dokumen penting Perangkat Daerah harus dilindungi dari kehilangan, pemalsuan, kerusakan, atau penyalahgunaan sesuai dengan peraturan perundangan, regulasi, dan persyaratan kontrak dan bisnis;
5. Perangkat Daerah harus memastikan privasi dan perlindungan terhadap informasi terkait dengan pribadi (*personally identifiable information*) sesuai dengan prasyarat hukum, perundangan, regulasi dan kontraktual;
6. Pimpinan Perangkat Daerah harus secara rutin memantau dan meninjau kepatuhan dari personil, proses kerja dan pemrosesan informasi dalam area tanggung jawabnya terhadap kebijakan dan standard keamanan informasi Perangkat Daerah serta prasyarat keamanan informasi yang berlaku;
7. Pada saat terjadi ketidaksesuaian, pimpinan Perangkat Daerah bertanggung jawab untuk menangani ketidaksesuaian yang terjadi sesuai dengan kebijakan terkait penanganan ketidaksesuaian dan peningkatan manajemen keamanan informasi SPBE;
8. Sistem informasi Perangkat Daerah harus ditinjau untuk menganalisis kepatuhan teknis dengan kebijakan dan standard keamanan yang berlaku serta dengan prasyarat keamanan informasi yang relevan dan berlaku, paling tidak satu kali dalam satu tahun;

9. 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.

SEKRETARIS DAERAH
KABUPATEN KENDAL,

SUGIONO