PEMERINTAH KOTA BATAM
DINAS KOMUNIKASI DAN INFORMATIKA
Jl. Engku Putri No. 1
Telepon : (0778) 462164, Faksimile : (0778) 461349
Email : *kominfo@batam.go.id*, Website : *https://kominfo.batam.go.id*
B A T A M
Kode Pos : 29464

SURAT KEPUTUSAN

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA KOTA BATAM
NOMOR: 105 /KI.01.04/VIII/2022

TENTANG

KEBIJAKAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PIMPINAN TINGGI PRATAMA

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA KOTA BATAM

Menimbang : Untuk memberikan arahan kepada manajemen dan memberikan dukungan untuk keamanan informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) sesuai dengan kebutuhan bisnis serta hukum dan peraturan yang relevan, maka perlu dibuat Kebijakan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Pimpinan Tinggi Pratama.

Mengingat :

1. Undang-Undang Nomor 53 Tahun 1999 tentang Pembentukan Kabupaten Pelalawan, Kabupaten Rokan Hulu, Kabupaten Rokan Hilir, Kabupaten Siak, Kabupaten Karimun, Kabupaten Natuna, Kabupaten Singingi dan Kota Batam (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 181, Tambahan Lembaran Negara Republik Indonesia Nomor 3902) sebagaimana telah diubah dengan Undang-Undang Nomor 13 Tahun 2000 tentang Pembentukan Kabupaten Pelalawan, Kabupaten Rokan Hulu, Kabupaten Rokan Hilir, Kabupaten Siak, Kabupaten Karimun, Kabupaten Natuna, Kabupaten Singingi dan Kota Batam (Lembaran Negara Republik Indonesia Tahun 2000 Nomor 80, Tambahan Lembaran Negara Republik Indonesia Nomor 3968);

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 4443);

3. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

4. Peraturan Wali Kota Batam Nomor 78 Tahun 2021 tentang Susunan Organisasi dan Tata Kerja Dinas Daerah;

5. Peraturan Wali Kota Batam Nomor 27 Tahun 2022 tentang Tugas Pokok, Fungsi dan Uraian Tugas Dinas Komunikasi dan Informatika;

6. Peraturan Wali Kota Batam Nomor 40 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Batam;

7. Peraturan Wali Kota Batam Nomor 65 Tahun 2022 tentang Penyelenggaran Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Batam;

8. Keputusan Wali Kota Batam Nomor 324 Tahun 2022 tentang Penanggung Jawab dan Pelaksana Teknis Kebijakan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Batam.

MEMUTUSKAN

Menetapkan : KEBIJAKAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PIMPINAN TINGGI PRATAMA

PERTAMA : Kebijakan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Pimpinan Tinggi Pratama sebagaimana tercantum dalam Lampiran Keputusan ini.

KEDUA : Kebijakan sebagaimana dimaksud pada DIKTUM PERTAMA tidak terpisahkan dengan Keputusan ini.

KETIGA : Keputusan ini berlaku pada tanggal ditetapkan.

Ditetapkan di Batam
Pada tanggal 4 Agustus 2022

KEPALA DINAS
KOMUNIKASI DAN INFORMATIKA
KOTA BATAM

PEMERINTAH DAERAH KOTA BATAM
DINAS KOMUNIKASI DAN INFORMATIKA

AZRIL APRIANSYAH, S.T., M.T.
Pembina Tingkat I
NIP. 19730408 200212 1 005

Lampiran I Keputusan Kepala Dinas Komunikasi dan Informatika Kota Batam
Nomor : 105 /KI.01.04/VIII/2022
Tanggal : 4 Agustus 2022

KEBIJAKAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

PIMPINAN TINGGI PRATAMA

DINAS KOMUNIKASI DAN INFORMATIKA
KOTA BATAM.
2022

RIWAYAT REVISI (REVISION HISTORY)

Revisi	Tanggal	Ringkasan Perubahan	Pembuat
00	1 Agustus 2022	Terbitan Pertama	Bidang Pengelolaan Informasi Publik dan Persandian

DAFTAR ISI

1. Kebijakan dan Cakupan Sistem Manajemen Keamanan Informasi SPBE

1.1 Tujuan

Untuk memberikan arahan kepada manajemen dan memberikan dukungan untuk keamanan informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) sesuai dengan kebutuhan bisnis serta hukum dan peraturan yang relevan.

1.2 Penerapan

1.1.1 Pemerintah Kota Batam menyadari bahwa informasi merupakan aset Pemerintah Kota Batam yang harus dijaga. Oleh sebab itu, Pemerintah Kota Batam berkomitmen mengimplementasikan Sistem Manajemen Keamanan Informasi (SMKI) SPBE yang bertujuan untuk memberikan perlindungan terhadap keamanan informasi SPBE sehingga terjamin kerahasiaan, keutuhan serta ketersediaannya yang berstandar internasional. Untuk mencapai hal di atas, Manajemen Puncak Pemerintah Kota Batam harus menetapkan Rencana SMKI SPBE di Lingkungan Pemerintah Kota Batam yang didasarkan atas hal-hal berikut ini:

a. Peraturan UU No. 11 Th. 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).
b. Peraturan Menteri Kominfo No.4/2016 tentang Sistem Manajemen Pengamanan Informasi.
c. Peraturan Pemerintah No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
d. Peraturan Wali Kota Batam Nomor 40 Tahun 2021 Tentang Sistem Penyelenggaraan Pemerintah Berbasis Elektronik di Lingkungan Pemerintah Kota Batam.
e. Peraturan Wali Kota Batam Nomor 65 Tahun 2022 Tentang Penyelenggaraan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Batam
f. Standar Internasional ISO/IEC 27001.
g. Hasil Kajian Keamanan Informasi SPBE.
h. Kebutuhan internal terhadap pengamanan informasi dengan sudut pandang bahwa informasi adalah aset yang harus dilindungi.

1.2.3 Untuk mendukung suksesnya implementasi SMKI SPBE di Pemerintah Kota Batam, Pimpinan Tinggi Pratama menetapkan hal-hal berikut:

a. Manajemen harus menetapkan sasaran keamanan informasi tahunan, yang merupakan bagian yang tidak terpisahkan dari Sistem Manajemen Kinerja Pemerintah Kota Batam.
b. Memastikan dipatuhinya segala peraturan dan perundangan yang berlaku terkait dengan keamanan informasi SPBE.
c. Memastikan dilakukannya asesmen risiko keamanan informasi SPBE secara berkala.
d. Memastikan bahwa tersedianya dokumentasi pendukung yang diperlukan untuk mengimplementasikan bab-bab ketentuan keamanan informasi yang tertulis dalam dokumen ini.
e. Menyediakan sumber daya yang diperlukan agar implementasi SMKI SPBE dapat berlangsung secara efektif.
f. Melakukan pemantauan terhadap pencapaian sasaran keamanan informasi.

g. Memastikan terselenggaranya audit internal SMKI SPBE yang dilaksanakan sesuai dengan ketentuan Pemerintah Kota Batam.
h. Memastikan dilaksanakannya tinjauan manajemen SMKI SPBE, setidaknya satu kali dalam setiap tahun.
i. Memastikan bahwa peningkatan berkelanjutan terhadap implementasi SMKI SPBE akan selalu dilaksanakan.

1.2.4 Ruang lingkup dari implementasi SMKI SPBE ini mencakup :
a. Organisasi : Pemerintah Kota Batam
b. Lokasi : Kantor Dinas Komunikasi dan Informatika Kota Batam
c. Proses bisnis / Layanan : Sistem Penyelenggaraan Pemerintah Berbasis Elektronik.
d. Aset :
1. Data / Informasi:
Dokumen pengadaan dan kontrak vendor perangkat infrastruktur, data user internet, dokumen teknis & konfigurasi jaringan, hasil *penetration test*, prosedur operasional, rekaman operasional penggunaan TI, BCP dan hasil audit, dsb.
2. Software:
Aplikasi *monitoring*, syslog, aplikasi *user management* , *captive portal*, aplikasi *dns filter* dan *resolver*, *windows server* 2012, MSSQL *server*, aplikasi *remote* perangkat.
3. Hardware:
Server monitoring, *server syslog*, *server user management*, *server captive portal*, *server DNS filter* dan *resolver*, laptop, media penyimpanan data.
4. Perangkat Jaringan Telekomunikasi:
Router BGP, *firewall data center*, *firewall user*, *switch* publik, *router core*, *switch core*, *switch distribution*.
5. Sumber Daya Manusia:
Aparatur Sipil Negara (pranata komputer, persandian dan manggala informatika).
6. Fasilitas Pendukung:
Rak *network center*, rak *network distribution*, ruang NOC, UPS, PAC, CCTV, *access door*, *fire extinguisher*.

1.2.5 Pengecualian terhadap pelaksanaan kebijakan SMKI SPBE disampaikan secara tertulis kepada Pimpinan Tinggi Pratama.

2. Standar Penerapan Sistem Manajemen Keamanan Informasi SPBE

2.1 Tujuan

Standar ini bertujuan memberikan panduan dalam melakukan implementasi SMKI SPBE di lingkungan Pemerintah Kota Batam dengan menggunakan proses siklus P-D-C-A (*Plan-Do-Check-Act*) berbasis ISO/IEC 27001:2013, sehingga aset informasi Pemerintah Kota Batam dapat terlindungi dari aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

2.2 Penerapan

2.2.1 Proses perencanaan (*Plan*), meliputi kegiatan:

a. Menentukan isu internal dan eksternal yang dapat mempengaruhi proses implementasi SMKI SPBE;
b. Menentukan pihak-pihak terkait proses implementasi SMKI SPBE serta mengidentifikasi persyaratan dan kebutuhan keamanan informasinya;
c. Menentukan ruang lingkup penerapan SMKI SPBE;
d. Menetapkan suatu komitmen manajemen terhadap penerapan SMKI SPBE;
e. Mengkomunikasikan dan mensosialisasikan pedoman keamanan informasi SPBE.
f. Melakukan asesmen risiko keamanan informasi SPBE;
g. Menyusun Rencana Mitigasi Risiko Keamanan Informasi SPBE;
h. Menentukan sasaran penerapan SMKI SPBE; dan
i. Menentukan sumber daya yang diperlukan untuk penerapan SMKI SPBE.

2.2.2 Proses Pelaksanaan (*Do*), meliputi kegiatan:

a. Pendokumentasian proses pelaksanaan SMKI SPBE;
b. Menilai risiko keamanan informasi ketika ada penambahan risiko baru atau terdapat perubahan signifikan yang dapat mempengaruhi keamanan informasi SPBE;
c. Melaksanakan *awareness* dan pelatihan SMKI SPBE;
d. Melakukan pengadaan dan pengelolaan sumber daya untuk mendukung pelaksanaan penerapan SMKI SPBE; dan
e. Menjalankan penerapan SMKI SPBE sesuai sasaran yang telah ditetapkan pada proses perencanaan (*plan*).

2.2.3 Proses Evaluasi (*Check*), meliputi kegiatan:

a. Menilai keefektifan implementasi pengendalian keamanan informasi SPBE sekurang-kurangnya dilakukan satu kali dalam satu tahun.
b. Memantau dan melaporkan pencapaian sasaran SMKI SPBE sekurang- kurangnya dilakukan satu kali dalam satu tahun.
c. Mereviu hasil asesmen risiko minimal setiap enam bulan sekali.
d. Melakukan audit internal penerapan SMKI SPBE yang dilakukan minimal satu kali dalam satu tahun.
e. Melakukan Tinjauan Manajemen terhadap penerapan SMKI SPBE yang dilakukan sekurang-kurangnya satu kali dalam satu tahun.

2.2.4 Proses Tindak Lanjut (*Act*), meliputi kegiatan:

a. Memantau penerapan rencana tindakan perbaikan hasil audit internal.
b. Melakukan peningkatan berkelanjutan terhadap penerapan SMKI SPBE setiap tahunnya dengan melakukan perencanaan (*plan*) kembali.

2.3 Dokumen Terkait

2.3.1 Dokumen Rencana Strategis Dinas Komunikasi dan Informatika Kota Batam.
2.3.2 Dokumen *Integrated Management System Plan*.
2.3.3 Dokumen Laporan Audit Internal dan/atau Eksternal.

3. Penggunaan Sumber Daya TIK

3.1 Tujuan

3.1.1 Terciptanya kesamaan persepsi dalam pengembangan dan pengelolaan TIK di lingkungan Pemerintah Kota Batam;

3.1.2 Meningkatnya penerapan *E-Government* dalam rangka peningkatan kualitas penyelenggaraan pemerintahan dan pelayanan masyarakat;

3.1.3 Mengatur penataan sistem jaringan internet dan intranet sebagai fasilitas utama dalam konektivitas data dan informasi di seluruh OPD;

3.1.4 Mengatur tata kelola dan pemanfaatan TIK di lingkungan Pemerintah Kota Batam secara terintegrasi, terpadu dan terdistribusi secara optimal;

3.1.5 Meningkatkan kualitas layanan publik melalui optimalisasi pemanfaatan TIK;

3.1.6 Meningkatkan kelancaran dan keamanan lalu lintas data dan informasi;

3.1.7 Meningkatkan kualitas perencanaan pengembangan TIK; dan

3.1.8 Melindungi dan mengamankan data, informasi, perangkat keras, perangkat lunas serta produk TIK lainnya.

3.2 Penerapan

3.2.1 Menjadi acuan dalam pengembangan dan penerapan tata kelola TIK di lingkungan Pemerintah Kota Batam;

3.2.2 Mendorong terlaksananya pemanfaatan TIK secara benar, efisien, efektif dan sesuai dengan perkembangan teknologi;

3.2.3 Menjamin terselenggaranya *E-Government* pada Pemerintah Kota Batam sebagai upaya mewujudkan pelayanan prima dan tata kelola Pemerintahan yang profesional, efektif, efisien dan transparan; dan

3.2.4 Menjamin terwujudnya integrasi data dan informasi, infrastruktur jaringan, sistem informasi, serta manajemen pengambilan kebijakan TIK secara terencana, terukur dan terpadu.

3.3 Dokumen Terkait

3.3.1 Rincian Teknis Tata Kelola Sumber Daya TIK.

4. Manajemen Risiko Keamanan Informasi SPBE

4.1 Tujuan

Untuk memberikan panduan dalam melakukan penilaian risiko dan mengevaluasi kecukupan risiko keamanan informasi SPBE berdasarkan kriteria yang ditentukan yaitu kerahasiaan, keabsahan dan ketersediaan (CIA: *Confidentiality*, *Integrity*, *and Availability*).

4.2 Penerapan

4.2.1 Pelaksanaan penilaian risiko keamanan informasi SPBE dan pendokumentasiannya dapat meminta bantuan ke instansi terkait yang menangani keamanan informasi SPBE dan pihak ketiga yang diakui memiliki kemampuan oleh instansi berwenang untuk melakukan penilaian risiko keamanan informasi SPBE.

4.2.2 Penilaian risiko keamanan informasi SPBE membantu mengidentifikasi risiko-risiko terkait keamanan informasi SPBE seperti informasi data pribadi dan memungkinkan untuk melakukan mitigasi terhadap risiko tersebut dengan menggunakan pengendalian yang sesuai. Dari hasil penilaian risiko keamanan informasi SPBE tersebut dapat ditentukan prioritas serta tindakan yang tepat dalam menerapkan pengendalian keamanan informasi SPBE berdasarkan suatu tingkat risiko yang dapat diterima (ARL, *acceptable risk level*) oleh Pemerintah Kota Batam. Manajemen SMKI mengevaluasi kecukupan risiko keamanan informasi SPBE berdasarkan kriteria sebagai berikut:

a. Kendala-kendala keuangan dan sumber daya pada saat ini;
b. Rekomendasi dari pihak yang terkait;
c. Hasil-hasil audit SMKI serta audit sistem informasi; dan
d. Kecenderungan insiden keamanan yang terjadi di masa lalu.

4.2.3 Tingkat risiko keamanan informasi SPBE yang dapat diterima (ARL, *acceptable risk level*) harus dikaji ulang setiap tahun dan digunakan sebagai bagian dari masukan untuk manajemen risiko Pemerintah Kota Batam. Maksud untuk penyelarasan dengan manajemen risiko strategis adalah untuk mengkoordinasikan keputusan risiko jangka panjang dengan unit-unit bisnis dan untuk meningkatkan kesadaran terhadap persoalan-persoalan yang sedang dihadapi.

4.2.4 Penyelenggaraan Proses Manajemen Risiko SPBE dalam rangka penerapan Manajemen Risiko SPBE perlu dilakukan melalui tahapan sebagai berikut :

a. komunikasi dan konsultasi;
b. penetapan konteks;
c. penilaian risiko yang melalui identifikasi risiko, analisis risiko dan evaluasi risiko;
d. penanganan risiko; dan
e. pemantauan dan reviu.

4.2.5 Proses Manajemen Risiko SPBE wajib dilaksanakan oleh Unit Pemilik Risiko (UPR) dalam suatu siklus berkelanjutan dan mempunyai periode penerapan selama 1 (satu) tahun.

4.2.6 Pelaksanaan Proses Manajemen Risiko dituangkan dalam Piagam Manajemen Risiko yang ditetapkan oleh UPR paling lambat tanggal 31 Januari tahun berjalan.

4.3 Dokumen Terkait

4.3.1 Dokumen Pedoman Pengelolaan Risiko.

4.3.2 Dokumen *Risk Register*.

4.3.3 Petunjuk Teknis Pelaksanaan Proses Manajemen Risiko.

5. Struktur Tata Kelola Dokumentasi SMKI SPBE

5.1 Tujuan

5.1.1 Untuk menjabarkan struktur dokumentasi yang diterapkan oleh Pemerintah Kota Batam.

5.1.2 Mengidentifikasi aset TI yang digunakan dalam penyelenggaraan layanan TI di Pemerintah Kota Batam.

5.2 Penerapan

5.2.1 Dengan menggunakan peta dokumentasi ISMS, pedoman-pedoman khusus, standar-standar khusus dan prosedur-prosedur khusus diidentifikasi. Penerapan dokumentasi ini adalah khusus untuk lingkungan yang telah ditetapkan.

5.3 Dokumen Terkait

5.3.1 Prosedur Pengendalian Informasi Terdokumentasi

Jenis Dokumen	Definisi
Kebijakan	Dokumen kebijakan teknologi informasi di Pemerintah Kota Batam.
Pedoman	Dokumen yang memberikan pedoman dalam implementasi keamanan informasi SPBE
Standar	Dokumen yang berisi persyaratan minimum dan ditetapkan berdasarkan konsensus para pemangku kepentingan dalam implementasi keamanan informasi SPBE
Prosedur	Dokumen yang berisi tata cara untuk menjalankan proses implementasi keamanan informasi SPBE
Formulir	Dokumen untuk merekam semua kegiatan implementasi keamanan informasi SPBE agar hasilnya dapat didokumentasikan

6. Organisasi Keamanan Informasi SPBE

6.1 Tujuan

6.1.1 Untuk mendirikan sebuah *framework* manajemen untuk memulai dan mengendalikan proses implementasi dan operasional dari keamanan informasi SPBE dalam Pemerintah Kota Batam.

6.2 Penerapan

6.2.1 Semua tanggung jawab keamanan informasi SPBE harus ditetapkan dan dialokasikan.

6.2.2 Tugas yang bertentangan dan area tanggung jawab harus dipisahkan untuk mengurangi peluang bagi modifikasi yang tidak sah atau tidak disengaja atau penyalahgunaan aset Pemerintah Kota Batam.

6.2.3 Mengidentifikasi dan menjalin kerjasama dengan pihak berwenang serta komunitas keamanan informasi SPBE diluar Pemerintah Kota Batam.

6.2.4 Pengendalian terhadap keamanan informasi SPBE harus diterapkan dalam pengelolaan proyek dan harus diaplikasikan pada seluruh fase dalam metodologi pengelolaan proyek.

6.3 Dokumen Terkait

6.3.1 Dokumen SOTK dan *Job Description*.

6.3.2 Eviden kerjasama dengan pihak berwenang dan/atau keikutsertaan dalam komunitas keamanan informasi.

6.3.3 Dokumen proses pengelolaan proyek (Prosedur, Instruksi Kerja, Standar, Aturan).

7. Keamanan Sumber Daya Manusia

7.1 Tujuan

7.1.1 Untuk memastikan bahwa para pegawai dan pekerja kontrak mengerti akan peran dan tanggung jawab dari pekerjaan mereka dan sesuai terhadap peran dan tanggung jawab yang mereka ambil.

7.1.2 Untuk memastikan bahwa para pegawai dan pekerja kontrak mengetahui dan melaksanakan peran dan tanggung jawab terhadap keamanan informasi SPBE.

7.1.3 Untuk melindungi kepentingan Pemerintah Kota Batam sebagai bagian dari proses penerimaan, perubahan/mutasi dan pemutusan tenaga kerja.

7.2 Penerapan

7.2.1 Pemeriksaan latar belakang pada semua calon pegawai dan pekerja kontrak harus dilakukan sesuai dengan hukum, peraturan dan etika yang berlaku.

7.2.2 Perjanjian kontrak dengan pegawai dan pekerja kontrak harus menyatakan peran dan tanggung jawab mereka terhadap keamanan informasi SPBE.

7.2.3 Manajemen harus mensyaratkan seluruh pegawai dan pekerja kontrak untuk menerapkan keamanan informasi SPBE sesuai dengan kebijakan dan prosedur yang berlaku di institusi.

7.2.4 Seluruh pegawai dan pekerja kontrak di Pemerintah Kota Batam perlu diberikan pendidikan, sosialisasi dan pelatihan terkait keamanan informasi SPBE sesuai dengan fungsi pekerjaan mereka.

7.2.5 Harus ada proses pemberian sanksi yang formal dan dikomunikasikan untuk mengambil tindakan terhadap pegawai yang melakukan pelanggaran keamanan informasi SPBE, sesuai dengan kebijakan dan prosedur yang berlaku di institusi.

7.2.6 Perlu dipastikan bahwa peran dan tanggung jawab keamanan informasi SPBE tetap diterapkan apabila terjadi perubahan atau terminasi terhadap pegawai.

7.2.7 Standar Kompetensi Pelaksana Keamanan informasi SPBE.

7.2.8 Peningkatan kompetensi dan keahlian pelaksana keamanan informasi SPBE.

7.3 Dokumen Terkait

7.3.1 Surat Keterangan Catatan Kepolisian.
7.3.2 Dokumen NDA Pegawai dan Pihak Ketiga.
7.3.3 Dokumen Laporan *Training* Pegawai.
7.3.4 *Awareness* Keamanan Informasi.
7.3.5 Aplikasi Penilaian Kinerja.

8. Manajemen Pengelolaan Aset

8.1 Tujuan

8.1.1 Untuk mengidentifikasi aset-aset milik Pemerintah Kota Batam dan menetapkan tanggung jawab terhadap perlindungan yang tepat dari aset-aset tersebut.

8.1.2 Untuk memastikan keamanan informasi SPBE tepat sesuai dengan tingkat kepentingan informasi.

8.1.3 Untuk mencegah kebocoran, modifikasi, penghapusan, dan penghancuran informasi yang disimpan oleh pihak yang tidak berwenang.

8.2 Penerapan

8.2.1 Aset terkait dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi dan diinventarisasi. Inventarisasi aset ini harus dibuat dan dipelihara secara berkala, serta ditetapkan penanggung jawab masing-masing aset tersebut.

8.2.2 Pemilik aset TI bertanggung jawab menetapkan dan menerapkan kontrol-kontrol pengamanan atas aset TI yang dikelolanya untuk melindungi aset TI tersebut dari ancaman kerahasiaan, keutuhan dan ketersediaan selama siklus masa berlakunya.

8.2.3 Menerapkan aturan terhadap penggunaan informasi dan aset pada Pemerintah Kota Batam.

8.2.4 Semua pegawai dan pengguna pihak eksternal harus mengembalikan seluruh aset milik Pemerintah Kota Batam yang mereka gunakan ketika terjadi pemutusan hubungan kerja, kontrak atau perjanjian.

8.2.5 Aset informasi diklasifikasikan sesuai tingkat kerahasiaan, nilai, tingkat kritikalitas, serta aspek hukumnya.

Klasifikasi	Definisi
Rahasia	Informasi yang membutuhkan pengamanan tinggi/ketat dan hanya boleh diketahui oleh pimpinan dan /atau personil tertentu yang ditetapkan. Pembocoran informasi ini secara tidak berwenang dapat menimbulkan risiko yang TINGGI/BESAR bagi Pemerintah Kota Batam, seperti antara lain: • kehilangan reputasi; • ketidakpatuhan terhadap regulasi; • kerugian finansial yang besar; atau • terganggunya layanan TI dalam jangka lama. Jenis informasi yang termasuk klasifikasi ini antara lain: • Topologi jaringan dengan *IP Address*; • hasil *penetration test*;

	• hasil penilaian kinerja pegawai; • *log system administrator*; dan • informasi rahasia lainnya.
Terbatas	Informasi yang telah terdistribusi di lingkungan internal Pemerintah Kota Batam yang penyebarannya secara internal tidak memerlukan persetujuan dari pemilik informasi. Risiko kebocoran informasi secara tak berwenang ke pihak luar berkategori SEDANG/ MENENGAH, tidak sebesar risiko informasi berklasifikasi “Rahasia”. Jenis informasi yang termasuk klasifikasi ini antara lain: • Kebijakan dan prosedur; • laporan audit (internal/eksternal); • hasil kajian risiko; • risalah rapat internal; • laporan operasional layanan TI yang tidak bersifat “Rahasia”; • dokumen kontrak; dan • informasi lain yang diklasifikasi "Terbatas".
Biasa	Informasi yang tidak memerlukan pengamanan dari aspek kerahasiaan atau informasi yang secara sengaja disediakan bagi publik. Jenis informasi yang termasuk klasifikasi ini antara lain: • Brosur layanan; • website dengan domain batam.go.id; dan • informasi lainnya yang disediakan bagi publik.

8.2.6 Pemberian label klasifikasi aset informasi harus dilakukan secara konsisten terhadap seluruh aset informasi.

8.2.7 Aset informasi harus ditangani sesuai dengan skema klasifikasi informasi yang diadopsi.

8.2.8 Menetapkan aturan untuk pengelolaan *removable media* sesuai dengan skema klasifikasi yang diadopsi.

8.2.9 Media penyimpanan yang memuat informasi harus dibuang/dihancurkan dengan metode yang aman ketika tidak lagi diperlukan.

8.2.10 Pengiriman media penyimpanan yang memuat informasi harus dilindungi terhadap akses yang tidak sah serta penyalahgunaan selama proses pengiriman.

8.2.11 Proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi).

Parameter Perubahan	**Klasifikasi Perubahan**		
	Sistem	**Proses Bisnis**	**Konfigurasi**
Cakupan Perubahan	Aplikasi, Database, Sistem Operasi, Domain	Kebijakan, Aturan, SOP	Aplikasi, Database, Sistem Operasi, Domain
Frekuensi Perubahan	Sesuai Kondisi	Sesuai Kondisi	Sesuai Kondisi
Pengujian Perubahan	Sesuai Kondisi	Sesuai Kondisi	Sesuai Kondisi

8.2.12 Pemilik Aset Informasi bertanggung jawab untuk mengimplementasikan tata kelola keamanan informasi pada informasi yang dimilikinya. Pemilik Aset Informasi mempunyai peran sebagai berikut.

a. Melakukan proses klasifikasi dan perlindungan aset informasi secara tepat;
b. Menentukan dan memberikan pendanaan pada kendali protektif yang sesuai;
c. Memberikan hak akses pada aset informasi yang sesuai dengan klasifikasi dan kebutuhan organisasi;
d. Melakukan atau memberikan kuasa kepada pihak ketiga terkait proses penilaian resiko keamanan informasi untuk memastikan kebutuhan keamanan informasi didefinisikan dan didokumentasi secara tepat;
e. Memastikan proses peninjauan akses sistem/data diselesaikan tepat waktu;
f. Memantau kepatuhan kebijakan keamanan informasi yang akan berpengaruh terhadap aset informasi Pemerintah Kota Batam.

8.3 Dokumen Terkait

8.3.1 Panduan Pengelolaan Aset dan Klasifikasi Informasi.
8.3.2 Daftar Aset Teknologi Informasi.
8.3.3 Prosedur Manajemen Perubahan.
8.3.4 Prosedur *Release Management*.
8.3.5 Prosedur Pengelolaan Konfigurasi.
8.3.6 Pernyataan Tanggung Jawab Aset TI Untuk Masing-Masing Individu.
8.3.7 Dokumen Pengelolaan Persyaratan Hak Akses dan Pertukaran Informasi.
8.3.8 Dokumen Tata tertib pengamanan dan penggunaan aset TI.
8.3.9 Dokumen Kebijakan terkait instalasi piranti lunak di aset TI.
8.3.10 Prosedur Penghancuran Aset TI.
8.3.11 Prosedur Pemindahan Aset TI.

9. Pengendalian Akses

9.1 Tujuan

9.1.1 Untuk membatasi akses terhadap informasi dan perangkat pemrosesan informasi.

9.1.2 Untuk memastikan hanya pengguna yang berwenang yang dapat mengakses informasi dan untuk mencegah pihak yang tidak berwenang masuk ke dalam sistem dan layanan.

9.1.3 Untuk memastikan pengguna bertanggung jawab dalam menjaga otentikasi terhadap informasi.

9.1.4 Memastikan dan mencegah adanya akses secara tidak berwenang terhadap informasi dan fasilitas sistem informasi baik aplikasi, sistem operasi, internet dan akses ruang server (*data center* dan *network center*).

9.2 Penerapan

9.2.1 Sebuah aturan terkait pengendalian akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan bisnis dan informasi.

9.2.2 Pengguna hanya boleh disediakan akses ke layanan jaringan dan jaringan yang telah secara khusus diizinkan bagi mereka untuk digunakan.

9.2.3 Proses pendaftaran dan penghapusan akses pengguna harus diterapkan.

9.2.4 Proses penyediaan akses pengguna terhadap sumber informasi harus diterapkan untuk semua jenis pengguna pada semua sistem dan layanan.

9.2.5 Alokasi dan penggunaan hak akses khusus harus dibatasi dan dikontrol.

9.2.6 Alokasi terhadap informasi otentikasi rahasia (seperti kata sandi) harus dikendalikan melalui proses pengelolaan secara formal.

9.2.7 Pemilik aset harus meninjau hak akses pengguna secara berkala.

9.2.8 Hak akses dari seluruh pegawai dan pengguna pihak eksternal terhadap informasi dan fasilitas pengolahan informasi harus dihapus setelah pemutusan hubungan kerja mereka, pemutusan kontrak atau perjanjian.

9.2.9 Pengguna wajib mematuhi peraturan penggunaan informasi otentikasi rahasia (seperti kata sandi).

9.2.10 Akses terhadap sistem informasi dan aplikasi harus dibatasi sesuai dengan peraturan pengendalian akses yang berlaku.

9.2.11 Akses ke sistem dan aplikasi harus dikendalikan dengan menggunakan metodologi *log-on* yang aman.

9.2.12 Mekanisme pengelolaan kata sandi harus interaktif dan harus memastikan kata sandi yang berkualitas.

9.2.13 Penggunaan program utilitas/alat bantu yang mungkin mampu meng-*override* sistem dan aplikasi harus dibatasi dan dikendalikan dengan ketat.

9.2.14 Akses ke kode sumber (*source code*) program harus dibatasi.

9.2.15 Hak akses, baik lojik maupun fisik (*data center*, *network center* dan seluruh ruangan pegawai di Dinas Kominfo) diberikan secara terbatas sesuai tugas pokok dan kewenangan pengguna. Pemberian hak akses tentunya harus disetujui minimum oleh Kepala Bidang yang berwenang.

9.2.16 Akses yang tingkatnya tinggi seperti administrator, hanya digunakan untuk kegiatan yang memerlukan pengguna administrator saja. Akses administrator tidak digunakan untuk melakukan pekerjaan operasional biasa. Untuk itu pegawai yang mendapatkan akses administrator bersifat terbatas.

9.3 Dokumen Terkait

9.3.1 Matriks Hak Akses.

9.3.2 Prosedur penggunaan akses dan Langkah pembenahan.

9.3.3 Prosedur Pengendalian Hak Akses terkait SDM yang mutasi/keluar dan tenaga kontrak/*outsource* yang habis masa Kerja.

10. Penggunaan Kriptografi

10.1 Tujuan

Tujuannya adalah untuk memastikan penggunaan yang tepat dan efektif terhadap kriptografi untuk melindungi kerahasiaan, keabsahan, dan integritas dari informasi.

10.2 Penerapan

10.2.1 Sebuah standar tentang penggunaan pengendalian kriptografi untuk perlindungan informasi harus dikembangkan dan diterapkan.

10.2.2 Menetapkan dan menerapkan standar untuk penggunaan dan perlindungan terhadap kunci kriptografi.

10.3 Dokumen Terkait

10.3.1 *Evidence* enkripsi pada aplikasi / trafik data.

11. Pengelolaan Keamanan Fisik dan Lingkungan

11.1 Tujuan

11.1.1 Untuk mencegah akses, kerusakan, dan campur tangan terhadap informasi dan perangkat pemrosesan informasi di Pemerintah Kota Batam oleh pihak yang tidak berwenang.

11.1.2 Untuk mencegah terjadinya kerugian, kerusakan, pencurian atau hal-hal yang dapat membahayakan aset serta interupsi terhadap operasional di Pemerintah Kota Batam.

11.2 Penerapan

11.2.1 Parameter keamanan harus ditetapkan dan digunakan untuk melindungi daerah-daerah yang berisi informasi dan fasilitas pengolahan informasi yang sensitif atau kritis.

11.2.2 Area aman harus dilindungi oleh pengendalian masuk yang tepat untuk menjamin bahwa hanya personil berwenang yang diperbolehkan untuk mengakses.

11.2.3 Keamanan fisik untuk kantor, ruangan dan fasilitas harus dirancang dan diterapkan.

11.2.4 Perlindungan fisik terhadap bencana alam, serangan berbahaya atau kecelakaan harus dirancang dan diterapkan.

11.2.5 Aturan untuk bekerja di area aman harus dirancang dan diterapkan.

11.2.6 Jalur akses seperti area pengiriman dan area bongkar muat di mana orang yang tidak berwenang bisa memasuki tempat tersebut harus dikendalikan dan, jika mungkin, diisolasi dari fasilitas pengolahan informasi untuk menghindari akses yang tidak sah.

11.2.7 Peralatan harus diletakkan dan dilindungi untuk mengurangi risiko dari ancaman lingkungan dan bahaya, dan kesempatan terhadap akses oleh yang tidak berwenang.

11.2.8 Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam fasilitas pendukung.

11.2.9 Kabel daya dan kabel telekomunikasi yang dilalui data harus dilindungi dari intersepsi, gangguan atau kerusakan.

11.2.10 Peralatan harus dipelihara dengan benar untuk memastikan aspek ketersediaan dan integritas.

11.2.11 Peralatan, informasi atau perangkat lunak tidak boleh dibawa keluar lokasi tanpa izin sebelumnya.

11.2.12 Keamanan harus diterapkan untuk aset yang berada diluar lokasi dengan memperhitungkan risiko yang berbeda dari bekerja di luar tempat Pemerintah Kota Batam.

11.2.13 Semua peralatan yang mengandung media penyimpanan harus diverifikasi untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa secara aman sebelum dibuang atau digunakan kembali.

11.2.14 Pengguna harus memastikan bahwa perangkat pengolah informasi yang ditinggal tanpa pengawasan memiliki perlindungan dari akses yang tidak berwenang.

11.2.15 Menetapkan aturan mengenai kebersihan area kerja dari dokumen kertas dan media penyimpanan *removable* dan fasilitas pengolahan informasi.

11.3 Dokumen Terkait

11.3.1 Peta Area Fisik Keamanan Informasi.
11.3.2 Buku *Access Log* ruang NOC dan *Data Center*.
11.3.3 Ketentuan Ruang Kerja.
11.3.4 Prosedur pengamanan lokasi kerja.

12. *Clear Desk Clear Screen*

12.1 Tujuan

12.1.1 Melindungi informasi dan sistem informasi dari kesalahan penggunaan atau penyebaran secara tidak berwenang pada perangkat kerja.

12.1.2 Memandu tata cara pengamanan informasi dan sistem informasi di Pemerintah Kota Batam terutama di area kerja.

12.1.3 Mencegah dan mengendalikan risiko yang timbul karena kesalahan pegawai dalam menggunakan perangkat pengolahan informasi.

12.2 Penerapan

12.2.1 Semua perangkat komputasi maupun pengolahan data harus dalam keadaan *log off* atau dilindungi dengan *screensaver* yang aktif pada batas waktu tertentu (contohnya 5 menit) atau mekanisme penguncian akses jika tidak sedang digunakan. Pengamanan perangkat dapat menggunakan salah satu atau lebih mekanisme yaitu menggunakan *password*, *PIN*, *fingerprint*, *pattern* atau *face lock*. Hal ini termasuk pada perangkat komputer, laptop, tablet dan *smartphone* yang digunakan untuk menunjang pekerjaan.

12.2.2 Saat menampilkan informasi rahasia pada layar, pegawai harus memperhatikan keadaan sekitar dan memastikan tidak ada pihak yang tidak berkepentingan yang dapat melihat informasi yang ditampilkan.

12.2.3 Setiap informasi rahasia atau kritikal yang menyangkut keberlangsungan bisnis, contohnya yang terdapat di kertas maupun perangkat penyimpanan harus diamankan, terutama saat staf tidak berada di tempat kerja.

12.2.4 Kertas yang menyantumkan informasi rahasia atau kritikal harus segera diambil dari perangkat cetak.

12.2.5 Setiap informasi rahasia maupun kritikal yang terdapat di media kertas maupun media penyimpanan elektronik harus segera dihancurkan jika sudah tidak terpakai, atau disimpan di tempat yang aman sampai dengan informasi tersebut bisa dihancurkan atau dihapus.

12.3 Dokumen Terkait

12.3.1 -

13. Keamanan Operasional

13.1 Tujuan

13.1.1 Untuk memastikan proses yang benar dan aman terhadap operasional perangkat pemrosesan informasi.

13.1.2 Untuk memastikan bahwa informasi serta perangkat pemrosesan informasi terlindungi dari ancaman *malware* (virus, trojan, dsb).

13.1.3 Untuk melindungi dari kehilangan data.

13.1.4 Untuk mencatat kejadian (*event*) pada perangkat pengolah informasi.

13.1.5 Untuk memastikan integritas dari sistem informasi.

13.1.6 Untuk mencegah eksploitasi terhadap kerentanan teknis (*Technical Vulnerabilities*).

13.1.7 Untuk meminimalisir dampak dari aktifitas audit terhadap sistem operasional.

13.1.8 Untuk memastikan keamanan terhadap penggunaan *Teleworking* (bekerja jarak jauh) dan penggunaan *Mobile Device*.

13.2 Penerapan

13.2.1 Prosedur operasional harus didokumentasikan dan tersedia untuk semua pengguna yang membutuhkannya.

13.2.2 Perubahan terhadap proses bisnis, fasilitas pengolahan informasi dan sistem yang mempengaruhi keamanan informasi SPBE harus dikendalikan.

13.2.3 Penggunaan sumber daya harus dimonitor, dievaluasi dan diproyeksikan dari kebutuhan kapasitas di masa depan untuk memastikan kinerja sistem yang diperlukan.

13.2.4 Pengembangan, pengujian, dan operasional lingkungan harus dipisahkan untuk mengurangi risiko akses yang tidak sah atau perubahan lingkungan operasional.

13.2.5 Pendeteksian, pencegahan dan pemulihan kontrol untuk perlindungan terhadap malware harus diterapkan.

13.2.6 Pembaruan terhadap sistem informasi dan aplikasi yang digunakan dilakukan dan dilaporkan secara berkala.

13.2.7 Salinan *back-up* dari informasi, perangkat lunak dan hasil *image* dari sistem harus disimpan dan diuji secara teratur sesuai dengan aturan *back-up* yang telah disepakati.

13.2.8 *Log* kejadian yang berfungsi untuk merekam kegiatan pengguna dan kejadian keamanan informasi SPBE pada perangkat TI harus diterapkan, disimpan dan di kaji secara berkala.

13.2.9 Fasilitas *Logging* dan informasi *log* harus dilindungi terhadap gangguan dan akses yang tidak sah.

13.2.10 Kegiatan dari operator dan administrator sistem harus tercatat (*logged*) dan catatan (*log*) tersebut harus dilindungi dan dikaji secara berkala.

13.2.11 Jam (waktu) dari semua sistem pengolahan informasi yang relevan harus disinkronisasikan sesuai referensi sumber waktu tunggal.

13.2.12 Peraturan harus ditetapkan untuk mengendalikan instalasi perangkat lunak pada sistem operasional dan instalasi yang dilakukan oleh pengguna.

13.2.13 Informasi tentang kerentanan teknis terhadap sistem informasi yang digunakan harus diperoleh secara tepat waktu, paparan untuk kerentanan tersebut perlu dievaluasi dan langkah yang tepat harus diambil untuk mengatasi risiko yang terkait.

13.2.14 Audit yang dilakukan terhadap sistem informasi harus direncanakan dengan hati-hati dan disetujui untuk meminimalkan gangguan terhadap proses bisnis.

13.2.15 Sebuah aturan harus ditetapkan untuk mengelola risiko yang diperkenalkan oleh penggunaan *mobile device*.

13.2.16 Sebuah aturan harus ditetapkan untuk melindungi informasi yang diakses, diproses atau disimpan pada perangkat *teleworking*.

13.3 Dokumen Terkait

13.3.1 Laporan pengujian *backup* dan *restore*.
13.3.2 Peraturan *mobile device* dan *teleworking*.
13.3.3 Daftar/Ceklis pelaksanaan keamanan informasi dan klasifikasinya.
13.3.4 Prosedur pemantauan sumber daya TIK.

14. Keamanan Komunikasi

14.1 Tujuan

14.1.1 Untuk memastikan adanya perlindungan terhadap informasi di dalam jaringan dan dukungan terhadap perangkat pemrosesan informasi pada jaringan.

14.1.2 Untuk menjaga keamanan terhadap informasi yang dipertukarkan di lingkungan Pemerintah Kota Batam maupun yang dipertukarkan di luar lingkungan Pemerintah Kota Batam.

14.2 Penerapan

14.2.1 Jaringan harus dikelola dan dikendalikan untuk melindungi informasi yang berada dalam sistem dan aplikasi.

14.2.2 Mekanisme keamanan, tingkat layanan dan persyaratan manajemen dari seluruh layanan jaringan harus diidentifikasi dan dimasukkan dalam perjanjian layanan jaringan, terlepas apakah layanan ini disediakan sendiri atau menggunakan jasa pihak ketiga.

14.2.3 Grup dari layanan informasi, pengguna dan sistem informasi di dalam jaringan harus dipisahkan.

14.2.4 Aturan terkait pengalihan informasi harus ditetapkan untuk melindungi pengalihan informasi melalui penggunaan semua jenis fasilitas komunikasi.

14.2.5 Perjanjian harus membahas tentang pengalihan yang aman terhadap informasi bisnis antara Pemerintah Kota Batam dan pihak luar.

14.2.6 Informasi yang terlibat dalam pesan elektronik harus dilindungi secara tepat.

14.2.7 Persyaratan untuk kerahasiaan atau perjanjian kerahasiaan (*non-disclosure agreement*) yang mencerminkan kebutuhan internal Pemerintah Kota Batam untuk perlindungan informasi harus diidentifikasi, dikaji secara berkala dan didokumentasikan.

14.3 Dokumen Terkait

14.3.1 Topologi Jaringan.
14.3.2 SLA (*Service Level Agreement)*.
14.3.3 NDA dengan Pihak Ketiga.

15. Akuisisi, Pengembangan dan Pemeliharaan Sistem

15.1 Tujuan

15.1.1 Untuk memastikan bahwa keamanan informasi SPBE adalah bagian yang tidak terpisahkan dari siklus hidup sistem informasi. Hal ini juga mencakup kebutuhan sistem informasi yang menyediakan layanan melalui jaringan publik.

15.1.2 Untuk memastikan bahwa keamanan informasi SPBE dibuat dan diterapkan dalam siklus pengembangan sistem informasi.

15.1.3 Untuk memastikan perlindungan terhadap data yang digunakan untuk pengujian (*testing*).

15.2 Penerapan

15.2.1 Kebutuhan terkait keamanan informasi SPBE harus dimasukkan dalam persyaratan untuk perancangan sistem informasi yang baru atau ditambahkan pada sistem informasi yang sedang berjalan.

15.2.2 Informasi yang terlibat dalam layanan aplikasi yang melewati jaringan publik harus dilindungi dari kegiatan kecurangan, pengungkapan yang tidak sah serta kegiatan modifikasi.

15.2.3 Informasi yang terlibat dalam transaksi layanan aplikasi harus dilindungi untuk mencegah transmisi data yang tidak lengkap, mis-routing, perubahan pesan yang tidak sah, pengungkapan yang tidak sah, duplikasi pesan yang tidak sah.

15.2.4 Peraturan untuk pengembangan sistem dan perangkat lunak yang aman (*Secure* SDLC) harus ditetapkan dan diterapkan untuk proses pengembangan di dalam institusi.

15.2.5 Perubahan terhadap sistem dalam siklus pengembangan harus dikendalikan dengan menggunakan prosedur pengendalian perubahan yang formal.

15.2.6 Ketika terjadi perubahan platform/sistem operasi, aplikasi bisnis yang penting harus ditinjau dan diuji untuk memastikan bahwa tidak ada dampak buruk dari perubahan tersebut terhadap keamanan informasi SPBE.

15.2.7 Melakukan modifikasi terhadap paket perangkat lunak (*software package*) harus diminimalkan, hanya terbatas pada perubahan yang diperlukan dan semua perubahan harus dikendalikan secara ketat.

15.2.8 Prinsip untuk rekayasa sistem yang aman harus ditetapkan, didokumentasikan, dipelihara dan diterapkan untuk setiap upaya implementasi sistem informasi.

15.2.9 Dinas Komunikasi dan Informatika harus menetapkan dan melindungi lingkungan pengembangan yang aman untuk proses pengembangan

dan integrasi sistem yang menjangkau seluruh siklus hidup pengembangan sistem.

15.2.10 Dinas Komunikasi dan Informatika harus mengawasi dan memantau aktivitas pengembangan sistem yang dialihdayakan (*outsourced*).

15.2.11 Pengujian fungsi keamanan harus dilakukan selama proses pengembangan.

15.2.12 Program pengujian penerimaan (*acceptance testing*) dan kriteria terkait harus ditetapkan untuk sistem informasi yang baru, yang di-upgrade dan menggunakan versi baru.

15.2.13 Data Pengujian harus dipilih dengan hati-hati, dilindungi dan dikendalikan.

15.3 Dokumen Terkait

15.3.1 -

16. Pengendalian Aspek Keamanan Informasi dalam Rencana Bisnis Berkelanjutan atau *Business Continuity Plan* (BCP)

16.1 Tujuan

16.1.1 Kesinambungan keamanan informasi SPBE harus tertanam dalam *Business Continuity Plan* (BCP) pada Pemerintah Kota Batam.

16.1.2 Untuk memastikan ketersediaan terhadap perangkat pengolahan informasi.

16.2 Penerapan

16.2.1 Pemerintah Kota Batam harus menetapkan persyaratan untuk keamanan informasi SPBE dan kesinambungan terhadap pengelolaan keamanan informasi SPBE dalam situasi yang merugikan, misalnya selama krisis atau bencana.

16.2.2 Pemerintah Kota Batam harus menetapkan, mendokumentasikan, menerapkan dan memelihara proses, prosedur dan kontrol untuk memastikan tingkatan yang diperlukan oleh kesinambungan terhadap keamanan informasi SPBE selama situasi yang merugikan.

16.2.3 Pemerintah Kota Batam harus memverifikasi pelaksanaan dan menetapkan pengendalian terhadap kesinambungan keamanan informasi SPBE secara berkala untuk memastikan bahwa proses tersebut valid dan efektif dalam situasi yang merugikan.

16.2.4 Pemerintah Kota Batam secara berkala membuat laporan evaluasi terhadap pelaksanaan pengendalian aspek keamanan informasi SPBE dalam pengelolaan kesinambungan bisnis atau *Business Continuity Plan* (BCP).

16.2.5 Fasilitas pengolahan informasi harus diimplementasikan dengan redundansi yang cukup untuk memenuhi persyaratan ketersediaan.

16.3 Dokumen Terkait

16.3.1 Laporan uji coba *backup* dan *restore*.
16.3.2 Laporan Berkala Evaluasi *Business Continuity Plan* (BCP).
16.3.3 Prosedur *backup* dan *restore*.

17. Rencana Pemulihan Bencana atau *Disaster Recovery Plan* (DRP)

17.1 Tujuan

17.1.1 Melindungi organisasi dari kegagalan sistem utama setelah terjadi bencana.

17.1.2 Meminimalisasi risiko organisasi terhadap penundaan (*delay*) dalam penyediaan layanan setelah terjadi bencana.

17.1.3 Menjamin kehandalan dari sistem yang tersedia melalui pengetesan dan simulasi.

17.1.4 Meminimalisasi proses pengambilan keputusan oleh personal/manusia setelah terjadi bencana.

17.2 Penerapan

17.2.1 Pemerintah Kota Batam harus menetapkan persyaratan untuk keamanan informasi SPBE terhadap pengelolaan keamanan informasi SPBE setelah terjadi bencana.

17.2.2 Pemerintah Kota Batam harus menetapkan, mendokumentasikan, menerapkan dan memelihara proses, prosedur dan kontrol untuk memastikan tingkatan yang diperlukan terhadap keamanan informasi SPBE setelah terjadi bencana.

17.2.3 Pemerintah Kota Batam harus memverifikasi pelaksanaan dan menetapkan pengendalian terhadap pemulihan keamanan informasi SPBE secara berkala untuk memastikan bahwa proses tersebut valid dan efektif setelah terjadi bencana.

17.2.4 Pemerintah Kota Batam secara berkala membuat laporan evaluasi terhadap pelaksanaan pengendalian aspek keamanan informasi SPBE dalam rangka pemulihan SPBE setelah terjadi bencana.

17.2.5 Fasilitas pengolahan informasi harus diimplementasikan dengan redundansi yang cukup untuk memenuhi persyaratan ketersediaan setelah terjadi bencana.

17.3 Dokumen Terkait

17.3.1 Laporan uji coba *backup* dan *restore*.

17.3.2 Laporan Berkala Evaluasi Rencana Pemulihan Bencana atau *Disaster Recovery Plan* (DRP).

17.3.3 Prosedur *backup* dan *restore*.

18. Pengendalian Pihak Ketiga (Vendor/Pemasok)

18.1 Tujuan

18.1.1 Untuk memastikan terlindunginya aset-aset milik Pemerintah Kota Batam yang dapat diakses oleh pihak ketiga.

18.1.2 Untuk mempertahankan tingkat keamanan informasi SPBE dan pelayanan yang telah disepakati dengan pihak ketiga.

18.2 Penerapan

18.2.1 Melakukan kesepakatan dengan pemasok terhadap persyaratan keamanan informasi SPBE untuk mengurangi risiko yang terkait dengan akses pemasok ke dalam aset Pemerintah Kota Batam.

18.2.2 Semua persyaratan keamanan informasi SPBE yang relevan harus ditetapkan dan disetujui oleh setiap pemasok yang dapat mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur TI untuk informasi Pemerintah Kota Batam.

18.2.3 Perjanjian dengan pemasok harus meliputi persyaratan untuk mengatasi risiko keamanan informasi SPBE yang terkait dengan teknologi informasi dan komunikasi layanan serta rantai suplai produk.

18.2.4 Pemerintah Kota Batam harus secara teratur memonitor, mereviu dan melakukan audit terhadap pelayanan dari pemasok.

18.2.5 Perubahan terhadap penyediaan layanan oleh pemasok harus dikelola, dengan mempertimbangkan kritikalitas dari informasi bisnis, sistem dan proses yang terlibat serta kajian risiko.

18.2.6 Perjanjian dengan pihak ketiga mencakup pelaksanaan peraturan dan perundang-undangan terkait dengan Hak Kekayaan Intelektual (HAKI).

18.3 Dokumen Terkait

18.3.1 Perjanjian dengan Pihak Ketiga.
18.3.2 Penilaian Layanan Pihak Ketiga.
18.3.3 Prosedur penggunaan perangkat informasi milik Pihak Ketiga.
18.3.4 Prosedur pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan Pihak Ketiga.

19. Pengelolaan Insiden Keamanan informasi SPBE

19.1 Tujuan

19.1.1 Untuk memastikan sebuah pendekatan yang efektif dan konsisten terhadap pengelolaan insiden keamanan informasi SPBE dan mencakup komunikasi pada kejadian (*event*) dan kelemahan (*weakness*) terkait keamanan informasi SPBE.

19.1.2 Untuk memastikan agar peristiwa dan kelemahan keamanan informasi SPBE yang berhubungan dengan sistem informasi dikomunikasikan secepat mungkin agar dapat di ambil tindakan perbaikan yang tepat.

19.2 Penerapan

19.2.1 Tanggung jawab dan prosedur pengelolaan insiden harus ditetapkan untuk memastikan respon yang cepat, efektif dan teratur terhadap insiden keamanan informasi SPBE.

19.2.2 Kejadian (*event*) keamanan informasi SPBE harus dilaporkan secepat mungkin sesuai mekanisme yang berlaku.

19.2.3 Pegawai yang menggunakan sistem dan layanan informasi harus mencatat dan melaporkan setiap kelemahan keamanan informasi SPBE yang diamati atau dicurigai dalam suatu sistem atau layanan.

19.2.4 Peristiwa keamanan informasi SPBE harus dinilai dan harus diputuskan apakah akan diklasifikasikan sebagai insiden keamanan informasi SPBE.

19.2.5 Insiden keamanan informasi SPBE harus ditanggapi sesuai dengan prosedur yang terdokumentasi.

19.2.6 Pengetahuan yang diperoleh dari proses analisa dan penyelesaian masalah insiden keamanan informasi SPBE harus digunakan untuk mengurangi kemungkinan atau dampak dari insiden di masa depan

19.2.7 Pemerintah Kota Batam harus menentukan dan menerapkan mekanisme untuk melakukan identifikasi, pengumpulan, akuisisi dan pelestarian informasi, yang dapat berfungsi sebagai bukti.

19.3 Dokumen Terkait

19.3.1 Manajemen Insiden dan Permintaan.

19.3.2 Prosedur Investigasi Insiden Keamanan Informasi.

19.3.3 Keputusan Wali Kota tentang Tim Tanggap Insiden Siber Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Batam.

20. Audit Internal

20.1 Tujuan

20.1.1 Tujuan audit internal mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi.

18.1.2 Ruang lingkup audit internal mencakup pemeriksaan terhadap latar belakang SDM

20.2 Penerapan

20.2.1 Audit internal dilakukan pada selang waktu terencana untuk memberikan informasi apakah Keamanan informasi SPBE diimplementasikan dan dipelihara secara efektif serta sesuai dengan peraturan dan ketentuan yang berlaku.

20.2.2 Audit internal mencakup perencanaan, penetapan, penerapan dan pemeliharaan program audit, termasuk frekuensi, metode, tanggung jawab, persyaratan perencanaan dan pelaporan. Program audit harus mempertimbangkan pentingnya proses yang bersangkutan dan hasil audit sebelumnya.

20.2.3 Audit internal harus menentukan kriteria audit dan ruang lingkup untuk setiap audit.

20.2.4 Audit internal harus memilih auditor dan melakukan audit yang menjamin objektivitas dan ketidakberpihakan proses audit.

20.2.5 Audit internal harus memastikan bahwa hasil audit tersebut dilaporkan kepada Koordinator dan Pelaksana Teknis Keamanan Informasi SPBE.

20.2.6 Audit internal harus menyimpan informasi terdokumentasi sebagai alat bukti dari program audit dan hasil audit.

20.2.7 Hasil audit internal dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi.

20.3 Dokumen Terkait

20.3.1 Self Assesment Indeks Keamanan Informasi.

21. Kepatuhan

21.1 Tujuan

21.1.1 Untuk menghindari pelanggaran terhadap kewajiban hukum, undang-undang, peraturan atau kontrak yang terkait dengan keamanan informasi SPBE dan persyaratan keamanan.

21.1.2 Untuk memastikan bahwa keamanan informasi SPBE diimplementasikan dan dijalankan sesuai dengan peraturan Pemerintah Kota Batam.

21.2 Penerapan

21.2.1 Seluruh undang-undang, peraturan, persyaratan kontrak dan pendekatan legislatif yang terkait serta pendekatan Pemerintah Kota Batam untuk memenuhi persyaratan tersebut harus secara eksplisit diidentifikasi, didokumentasikan dan selalu *up-to-date* untuk setiap sistem informasi dan Pemerintah Kota Batam.

21.2.2 Peraturan harus diterapkan untuk memastikan kepatuhan dengan persyaratan legislatif, peraturan dan kontrak yang terkait dengan hak kekayaan intelektual dan penggunaan kepemilikan produk perangkat lunak.

21.2.3 Rekaman harus dilindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah dan rilis yang tidak sah, sesuai dengan legislasi, peraturan, persyaratan kontrak dan bisnis.

21.2.4 Memastikan bahwa penyimpanan rekaman dikategorikan secara rinci termasuk jangka waktu dan media penyimpanan.

21.2.5 Menetapkan pedoman penyimpanan dan penanganan media rekaman yang sesuai dengan rekomendasi pabrik. Apabila akan menyimpan rekaman dalam jangka waktu yang lama perlu mempertimbangkan penggunaan media-media khusus.

21.2.6 Perlindungan terhadap privasi dan informasi pribadi harus sesuai dengan undang-undang dan peraturan yang berlaku.

21.2.7 Perlindungan terhadap HAKI yang sesuai dengan undang-undang atau peraturan yang berlaku.

21.2.8 Pengendalian terhadap kriptografi harus digunakan sesuai dengan semua perjanjian, undang-undang dan peraturan yang berlaku.

21.2.9 Pendekatan Pemerintah Kota Batam dalam mengelola keamanan informasi SPBE serta pelaksanaannya (misalnya sasaran pengendalian, kebijakan, proses dan prosedur untuk keamanan informasi SPBE) harus dikaji secara independen pada interval yang direncanakan atau ketika terjadi perubahan yang signifikan.

21.2.10 Pelaksana Teknis Keamanan Informasi SPBE harus secara teratur meninjau, menguji dan melaporkan kepatuhan terhadap proses

pengolahan informasi dan prosedur dalam area tanggung jawab mereka, sesuai dengan kebijakan keamanan, standar dan persyaratan keamanan yang berlaku pada Pemerintah Kota Batam.

21.2.11 Sistem informasi harus dikaji secara berkala untuk kepatuhan terhadap kebijakan dan standar keamanan informasi SPBE yang berlaku pada Pemerintah Kota Batam.

21.3 Dokumen Terkait

21.3.1 Daftar Peraturan perundang-undangan yang terkait keamanan informasi.

21.3.2 Laporan peninjauan kepatuhan terhadap keamanan informasi.

22. Sanksi

22.1 Tujuan

22.1.1 Mencegah dan mengendalikan risiko yang timbul karena kesalahan pegawai, pihak ketiga dan masyarakat umum dalam menggunakan dan memanfaatkan sistem dan layanan yang diberikan Pemerintah Kota Batam.

22.1.2 Memberikan kepastian hukum terhadap insiden keamanan informasi SPBE.

22.2 Penerapan

22.2.1 Pegawai yang melakukan pelanggaran yang mengakibatkan terjadinya insiden keamanan informasi SPBE di Lingkungan Pemerintah Kota Batam akan ditindaklanjuti sesuai dengan kebijakan dan peraturan di Pemerintah Kota Batam.

22.2.2 Pihak ketiga yang bekerjasama dengan unit-unit organisasi di Pemerintah Kota Batam yang melakukan pelanggaran yang mengakibatkan terjadinya insiden keamanan informasi SPBE di Lingkungan Pemerintah Kota Batam akan ditindaklanjuti sesuai dengan kebijakan dan peraturan di Pemerintah Kota Batam serta ditindaklanjuti sesuai dengan peraturan perundang-undangan yang berlaku.

22.2.3 Masyarakat umum yang melakukan pelanggaran yang mengakibatkan terjadinya insiden keamanan informasi SPBE di Lingkungan Pemerintah Kota Batam akan ditindaklanjuti sesuai dengan peraturan perundang-undangan yang berlaku.

22.3 Dokumen Terkait

22.3.1 Daftar Peraturan perundang-undangan yang terkait kepegawaian.

22.3.2 Daftar Peraturan perundang-undangan yang terkait perjanjian kerjasama dengan Pemerintah.

22.3.3 Daftar Peraturan perundang-undangan yang terkait keamanan informasi.

23. Evaluasi Kebijakan

23.1 Tujuan

Menjamin terjaganya kesesuaian, kecukupan dan efektivitas dari SMKI di SKPD/Unit Kerja.

23.2 Penerapan

23.2.1 Tinjauan manajemen SMKI harus dihadiri oleh:

a. manajemen puncak dari SMKI di SKPD/Unit Kerja;
b. koordinator SMKI di SKPD/Unit Kerja;
c. koordinator atau petugas fungsional SMKI.

23.2.2 Apabila dibutuhkan, tinjauan manajemen SMKI dapat dihadiri oleh:

a. pemangku kepentingan yang relevan dari SMKI di unit kerja yang membidangi teknologi informatika;
b. *subject matter expert* yang memadai.

23.2.3 Tinjauan manajemen SMKI harus mencakup masukan sebagai berikut:

a. status dari tindakan yang diputuskan pada tinjauan manajemen terdahulu;
b. perubahan baik internal maupun eksternal yang terkait dengan SMKI;
c. masukan terkait kinerja keamanan informasi yang mencakup *trend* pada:
    1) ketidaksesuaian dan tindakan korektif;
    2) hasil pemantauan dan pengukuran;
    3) hasil audit, baik internal maupun eksternal; dan
    4) pemenuhan dari sasaran keamanan informasi.
d. masukan dari pihak terkait;
e. hasil dari *assessment* risiko dan status rencana penanganan risiko;
f. peluang untuk peningkatan secara berkesinambungan.

23.2.4 Berdasarkan dari masukan tersebut, tinjauan manajemen SMKI harus menghasilkan keluaran sebagai berikut:

a. keputusan terkait peningkatan SMKI secara berkesinambungan; dan
b. peluang dan kebutuhan untuk perubahan SMKI.

23.2.5 Setiap keluaran dari tinjauan manajemen SMKI harus digunakan sebagai dasar bagi peningkatan dan perencanaan tahunan SMKI.

23.3 Dokumen Terkait

23.3.1 -

Ditetapkan di Batam
Pada tanggal 4 Agustus 2022

KEPALA DINAS
KOMUNIKASI DAN INFORMATIKA
KOTA BATAM

PEMERINTAH DAERAH KOTA BATAM
DINAS KOMUNIKASI DAN INFORMATIKA

AZRIL APRIANSYAH, S.T., M.T.
Pembina Tingkat I
NIP. 19730408 200212 1 005