GUBERNUR LAMPUNG

KEPUTUSAN GUBERNUR LAMPUNG
NOMOR : G/768 /V.14/HK/2023

TENTANG

KEBIJAKAN TEKNIS DAN PEMBENTUKAN TIM PELAKSANA MANAJEMEN KEAMANAN INFORMASI PEMERINTAH PROVINSI LAMPUNG

GUBERNUR LAMPUNG,

Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Provinsi Lampung, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;

b. bahwa berdasarkan ketentuan Pasal 25A ayat (1) huruf b Peraturan Gubernur Lampung Nomor 8 Tahun 2022 tentang Perubahan Atas Peraturan Gubernur Lampung Nomor 51 Tahun 2020 tentang Tata Kelola Sistem Pemerintahan Berbasis Elektronik Pemerintah Provinsi Lampung, disebutkan bahwa Pemerintah Provinsi Lampung melaksanakan Manajemen Sistem Pemerintahan Berbasis Elektronik meliputi manajemen keamanan informasi;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b tersebut di atas, perlu menetapkan Keputusan Gubernur Lampung tentang Kebijakan Teknis dan Pembentukan Tim Pelaksana Manajemen Keamanan Informasi di Lingkungan Pemerintah Provinsi Lampung;

Mengingat : 1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016;

2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;

3. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang;

4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;

5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;

6. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital;
7. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik;
8. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
9. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah;
10. 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;
11. Peraturan Daerah Provinsi Lampung Nomor 4 Tahun 2019 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Lampung;
12. Peraturan Gubernur Lampung Nomor 30 Tahun 2021 tentang Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Provinsi Lampung;
13. Peraturan Gubernur Lampung Nomor 8 Tahun 2022 tentang Perubahan atas Peraturan Gubernur Lampung Nomor 51 Tahun 2020 tentang Tata Kelola Sistem Pemerintahan Berbasis Elektronik Pemerintah Provinsi Lampung;

MEMUTUSKAN:

Menetapkan : **KEPUTUSAN GUBERNUR TENTANG KEBIJAKAN TEKNIS DAN PEMBENTUKAN TIM PELAKSANA MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH PROVINSI LAMPUNG.**

KESATU : Menetapkan Kebijakan Teknis dan Pembentukan Tim Pelaksana Manajemen Keamanan Informasi Pemerintah Provinsi Lampung sebagaimana tercantum dalam Lampiran I dan Lampiran II yang merupakan bagian tidak terpisahkan dari Keputusan ini.

KEDUA : Tim Pelaksana Sistem Manajemen Keamanan Informasi Pemerintah Provinsi Lampung sebagaimana dimaksud pada Diktum Kesatu mempunyai uraian tugas sebagai berikut:

1. Manajemen Puncak

   Mempunyai kewenangan dalam memutuskan untuk alokasi terkait sumber daya memberikan peningkatan yang diperlukan dalam sistem manajemen dan tindakan masukan yang diperlukan dalam berkelanjutan sistem manajemen keamanan informasi.

Tugas dan tanggung jawab Manajemen Puncak yaitu:

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

2. Wakil Manajemen

Mempunyai kewenangan dalam mengkoordinasikan dan mengambil keputusan terkait dengan seluruh aktivitas penerapan sistem manajemen keamanan informasi di Lingkungan Pemerintah Provinsi Lampung.

Tugas dan tanggung jawab Wakil Manajemen yaitu:

a) menyusun, mengkoordinasikan, serta memantau pelaksanaan seluruh aktivitas dan proses sistem manajemen dalam rangka pemenuhan prasyarat sistem manajemen keamanan informasi;
b) mengkoordinasikan pelaksanaan proses dan aktivitas sistem manajemen serta pengamanan informasi di organisasi;
c) mengkoordinasikan proses peninjauan secara berkala terhadap implementasi sistem manajemen keamanan informasi di organisasi; dan
d) memberikan laporan secara berkala terkait kondisi sistem manajemen dan keamanan informasi organisasi kepada Tim Koordinator Sistem Pemerintahan Berbasis Elektronik Pemerintah Provinsi Lampung.

3. *Lead Auditor* Internal

   Mempunyai pemantauan pelaksanaan kewenangan dalam mengkoordinasikan aktivitas dan tindak lanjut implementasi terkait pengelolaan audit internal sistem manajemen keamanan informasi.

   Tugas dan tanggung jawab *Lead Auditor* Internal yaitu:

   a) menyusun dan memantau program dan jadwal audit internal maupun eksternal;
   b) mengkoordinasikan pelaksanaan proses audit internal;
   c) merangkum dan melaporkan hasil audit internal sistem manajemen keamanan informasi kepada Manajemen Puncak dan Wakil Manajemen; dan
   d) mengkoordinasikan proses verifikasi tindakan perbaikan dan pencegahan terhadap ketidaksesuaian yang ditemukan dalam proses audit internal maupun eksternal.

4. Auditor Internal

   Mempunyai kewenangan dalam melaksanakan aktivitas proses audit internal sistem manajemen keamanan informasi.

   Tugas dan tanggung jawab Auditor Internal yaitu:

   a) melakukan proses audit internal sistem keamanan informasi di organisasi berdasarkan jadwal yang ditentukan;
   b) menyusun laporan hasil audit internal; dan
   c) melakukan verifikasi tindakan perbaikan dan pencegahan terhadap ketidaksesuaian yang ditemukan dalam proses audit internal maupun eksternal.

5. Koordinator Manajemen Resiko

   Mempunyai kewenangan mengkoordinasikan pelaksanaan proses identifikasi dan penilaian resiko serta perumusan dan penetapan rencana penanganan resiko untuk resiko-resiko yang perlu dimitigasi.

   Tugas dan tanggung jawab Koordinator Manajemen Resiko yaitu:

   a) memantau proses dan status pelaksanaan rencana penanganan resiko yang telah ditetapkan;
   b) mengkoordinasikan pelaksanaan peninjauan secara berkala terhadap daftar resiko dan peniliaan resiko bersama dengan para pemilik proses;
   c) mengelola proses pendokumentasian terkait proses penilaian dan pengelolaan resiko.

6. Koordinator Standar dan Kepatuhan

   Mempunyai kewenangan dalam mengkoordinasikan aktivitas pemantauan dan tindak lanjut implementasi terkait kesesuaian dengan standar dan kepatuhan terhadap kebijakan/prosedur.

Tugas dan tanggung jawab Koordinator Standar dan Kepatuhan yaitu:

a) menyusun dokumentasi kebijakan dan prosedur yang diperlukan dalam rangka penerapan sistem manajemen keamanan informasi di Pemerintah Provinsi Lampung;
b) mengidentifikasi dan mendokumentasikan peraturan perundang-undangan dan kewajiban kontrak yang relevan dengan sistem manajemen keamanan informasi di Pemerintah Provinsi Lampung;
c) memantau dan memastikan bahwa pelaksanaan aktivitas dan penerapan kontrol keamanan informasi telah sesuai dengan ketentuan kebijakan dan prosedur yang telah ditetapkan, serta peraturan perundang-undangan dan kewajiban kontrak yang relevan;
d) menyusun dan mengkoordinasikan pelaksanaan program *awareness* keamanan informasi untuk seluruh pegawai Pemerintah Provinsi Lampung; dan
e) menyusun matriks pengukuran sasaran sistem manajemen keamanan informasi serta melakukan pemantauan dan perunjauan atas proses pelaksanaan dan hasil pengukuran tersebut.

7. Koordinator Pengelolaan Sumber Daya Manusia

Mempunyai kewenangan dalam mengkoordinasikan aktivitas pengelolaan sumber daya manusia dalam penerapan implementasi sistem manajemen keamanan informasi.

Tugas dan tanggung jawab Koordinator Pengelolaan Sumber Daya Manusia yaitu:

a) mengkoordinasikan pelaksanaan pengamanan sumber daya manusia berdasarkan panduan dari kebijakan dan prosedur terkait pengamanan sumber daya manusia di perusahaan;
b) memberikan pengenalan terkait sistem manajemen keamanan informasi yang dijalankan di perusahaan kepada pegawai dan personil pihak ketiga;
c) memastikan kegiatan dalam rangka peningkatan pengetahuan dan *awareness* pegawai perusahaan; dan
d) memastikan setiap pegawai perusahaan telah menandatangani *non-disclosure agreement* (NDA).

8. Koordinator Tim Penanggulangan dan Pemulihan Insiden

Mempunyai kewenangan dalam aktivitas pengelolaan insiden terkait keamanan informasi.

Tugas dan tanggung jawab Tim Penanggulangan dan Pemulihan Insiden yaitu:

a) mengkoordinasikan dan memantau pengelolaan insiden keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi;

b) menerima serta mengelola laporan terkait kejadian, kelemahan, dan insiden keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi organisasi; dan

c) mendokumentasikan proses pengelolaan insiden keamanan informasi di organisasi.

KETIGA : Hal-hal yang belum diatur dalam Keputusan ini mengenai teknis pelaksanaannya diatur lebih lanjut oleh Kepala Dinas Komunikasi Informatika dan Statistik Provinsi Lampung dengan berpedoman kepada ketentuan peraturan perundang-undangan.

KEEMPAT : Keputusan ini mulai berlaku pada tanggal ditetapkan dengan ketentuan apabila dikemudian hari terdapat kekeliruan dalam Keputusan ini akan diadakan pembetulan sebagaimana mestinya.

Ditetapkan di Telukbetung
pada tanggal 8 – 12 – 2023

GUBERNUR LAMPUNG,

ARINAL DJUNAIDI

Tembusan:
1. Kepala Badan Siber dan Sandi Negara di Jakarta;
2. Ketua DPRD Provinsi Lampung di Telukbetung;
3. Inspektur Provinsi Lampung di Bandar Lampung;
4. Kepala Badan Pengelolaan Keuangan dan Aset Daerah Provinsi Lampung di Telukbetung;
5. Kepala Biro Hukum Setda Provinsi Lampung di Telukbetung;
6. Masing-masing Anggota Tim yang bersangkutan.

LAMPIRAN I : KEPUTUSAN GUBERNUR LAMPUNG
NOMOR : G/ 768 /2023
TANGGAL : 8 - 12 - 2023

KEBIJAKAN TEKNIS MANAJEMEN KEAMANAN INFORMASI PEMERINTAH PROVINSI LAMPUNG

BAB I
PENDAHULUAN

A. PENDAHULUAN

Informasi adalah aset yang sangat penting bagi Pemerintah Provinsi Lampung, baik yang terkait dengan kepegawaian, keuangan, laporan, maupun informasi lainnya. Kebocoran, kerusakan, ketidakakuratan, ketidaktersediaan atau gangguan lain terhadap informasi tersebut dapat menimbulkan dampak yang merugikan baik secara finansial maupun non finansial bagi layanan Pemerintah Provinsi Lampung. Mengingat pentingnya informasi, maka informasi harus dilindungi atau diamankan oleh seluruh pegawai Pemerintah Provinsi Lampung.

Keamanan Informasi adalah suatu kondisi untuk melindungi aset yang dimiliki organisasi dari berbagai ancaman pihak internal maupun eksternal untuk menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, serta terjaganya aspek kerahasiaan, keutuhan dan ketersediaan dari informasi. Keamanan Informasi sangat bergantung pada pengamanan semua aspek dan komponen aset TIK terkait, seperti data, perangkat lunak, perangkat keras, jaringan, peralatan pendukung, dan sumber daya manusia.

Sehubungan dengan hal tersebut, dalam rangka menjaga keamanan informasi di lingkungan Pemerintah Provinsi Lampung, perlu menyusun sebuah standar tentang manajemen keamanan informasi, yang mengatur bagaimana informasi menjadi aman agar kerahasiaan, integritas, dan ketersediaan informasi tetap terjaga.

B. TUJUAN

Sistem Manajemen Keamanan Informasi (SMKI) ini digunakan sebagai pedoman atau standar dalam rangka melindungi aset informasi Pemerintah Provinsi Lampung dari berbagai bentuk ancaman baik dari dalam maupun luar lingkungan Pemerintah Provinsi Lampung, dengan tujuan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.

C. RUANG LINGKUP

Standar ini berlaku untuk pengelolaan pengamanan seluruh informasi Pemerintah Provinsi Lampung yang dilaksanakan oleh seluruh Perangkat Daerah Pemerintah Provinsi Lampung dan pihak ketiga baik sebagai pengelola dan/atau pengguna Teknologi Informasi dan Komunikasi (TIK).

D. PENGERTIAN UMUM

1. Aset Pemerintah Provinsi Lampung adalah sumber daya yang memiliki nilai bagi Pemerintah Provinsi Lampung.
2. Aset informasi adalah meliputi data/dokumen yang mencakup: kepegawaian, keuangan, laporan, kebijakan, maupun informasi lainnya.
3. Aset berwujud (*tangible*) meliputi: sumber daya manusia, gedung dan bangunan, perangkat komputer, perangkat jaringan dan komunikasi, removable media dan perangkat pendukung lainya.
4. Aset tak berwujud (*intangible*) meliputi: pengetahuan, pengalaman, keahlian, citra, reputasi.
5. Dokumen adalah data atau informasi yang tertulis atau tercetak yang dapat dipergunakan sebagai bukti atau keterangan. Dokumen dapat berbentuk *file* elektronik (*softcopy*) atau cetakan (*hardcopy*).
6. Hak Akses adalah kewenangan terkait penggunaan suatu aset informasi yang jenis dan tingkatannya disesuaikan dengan kebutuhan kerja dan risiko keamanan informasi. Hak ini, tergantung dari jenis asetnya secara formal diberikan atau disahkan oleh pemilik aset atau atasan langsung.
7. Hak akses khusus adalah izin atau hak istimewa yang diberikan kepada pengguna, program atau *workstation* untuk membuat, mengubah, menghapus atau melihat data dan file dalam sebuah sistem.
8. Informasi adalah sekumpulan data atau fakta yang dikelola menjadi sesuatu yang bermanfaat atau memiliki nilai bagi pemilik atau penerimanya.
9. Insiden keamanan informasi adalah peristiwa yang mengakibatkan tidak tercapainya aspek kerahasiaan, integritas atau ketersediaan aset milik Pemerintah Provinsi Lampung dan mengakibatkan dampak gangguan terhadap proses kerja Pemerintah Provinsi Lampung.
10. Kajian Risiko adalah keseluruhan proses analisa dan evaluasi risiko.
11. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi. Catatan: Sifat-sifat informasi yang lain seperti keaslian (*authenticity*), akuntabilitas (*accountability*), *non-repudiation* dan keandalan (*reliability*) dapat juga dimasukkan sebagai keamanan informasi.
12. Kebijakan Sistem Manajemen Keamanan Informasi adalah serangkaian aturan terkait keamanan infromasi di lingkungan Pemerintah Provinsi Lampung dalam rangka melindungi aset informasi milik Pemerintah Provinsi Lampung, meliputi kebijakan SMKI, pedoman pelaksanaan SMKI, dan kebijakan dasar (*baseline*) konfigurasi keamanan sistem dan perangkat TIK di lingkungan Pemerintah Provinsi Lampung.
13. Kelemahan keamanan informasi adalah kondisi yang berpotensi mengakibatkan tercapainya aspek kerahasiaan, integritas, atau ketersediaan aset milik Pemerintah Provinsi Lampung.
14. Koordinator SMKI adalah personil setingkat eselon III atau eselon II yang ditunjuk oleh Kepala Unit kerja atau setingkat eselon II di Pemerintah Provinsi Lampung untuk melaksanakan kegiatan penerapan kebijakan dan prosedur keamanan informasi di lingkungan Pemerintah Provinsi Lampung tempat dia ditugaskan. Petugas Keamanan Informasi bekerja dibawah pengawasan dan pengarahan Koordinator SMKI.

15. Manajemen Puncak SMKI adalah pejabat setingkat Eselon II yang ditunjuk oleh Gubernur Provinsi Lampung untuk mengkoordinasikan dan mengarahkan kegiatan penerapan kebijakan dan prosedur keamanan informasi di lingkungan Pemerintah Provinsi Lampung.
16. *Mobile Computing* adalah penggunaan perangkat komputasi jinjing (*portabel*), seperti *notebook*/laptop dan *smartphone*, untuk melakukan akses/konektivitas, pengolahan data dan penyimpanan data.
17. Panduan adalah rekomendasi tindakan yang dianjurkan dapat dilakukan untuk mencapai suatu sasaran.
18. Pedoman adalah kumpulan ketentuan yang menjadi dasar, pegangan, acuan atau petunjuk dan memberi arah bagaimana sesuatu harus dilakukan.
19. Pemilik Aset Informasi adalah pihak yang secara hukum ditunjuk sebagai penanggung jawab aset informasi atau proses kerja di Pemerintah Provinsi Lampung/pimpinan unit organisasi dimana data/informasi itu dibuat.
20. Penasehat adalah pejabat yang memberikan arahan terhadap masukan proyek TI dan penanganan masalah atau risiko-risiko yang signifikan dan berdampak pada kegiatan operasional Pemerintah Provinsi Lampung.
21. Pengguna adalah pihak atau personil yang dapat mengakses sistem informasi berdasarkan hak akses yang telah diberikan.
22. Pengguna adalah pihak atau personil yang menggunakan sistem informasi dan diberikan hak akses berdasarkan level tertentu.
23. Pemasok adalah penyedia yang menyalurkan layanan (barang dan/atau jasa) kepada entitas bisnis di lingkungan Pemerintah Provinsi Lampung.
24. Perangkat jaringan adalah peralatan jaringan komunikasi data, yang mencakup antara lain namun tidak terbatas pada: modem, hub, *router*, *switch*, *firewall*, *repeater*, *bridge*, server.
25. Perangkat lunak meliputi: perangkat lunak aplikasi, perangkat lunak sistem operasi, perangkat lunak pemrograman dan perangkat lunak tambahan/program bantu.
26. Perangkat pengolah informasi adalah perangkat yang digunakan untuk memproses informasi, seperti misalnya: komputer, laptop, telepon dan fax, printer, mesin fotokopi.
27. Perangkat pendukung adalah peralatan yang berfungsi untuk menjamin beroperasinya perangkat pengolah informasi serta melindunginya dari kerusakan, seperti misalnya *Uninterruptible Power Supply* (UPS), genset, *fire extinguisher*, *access door electronic*, HVAC, A/C, CCTV, sensor suhu, sensor temperatur, sensor air.
28. Pihak ketiga adalah seluruh pihak yang terkait dan berkepentingan atau memiliki hubungan dengan proses bisnis di Pemerintah Provinsi Lampung yang berada di luar struktur organisasi Pemerintah Provinsi Lampung.
29. Prosedur adalah serangkaian kegiatan, tindakan yang harus dijalankan dengan cara yang baku agar selalu memperoleh hasil yang sama dari keadaan yang sama.
30. Rekaman adalah dokumen yang menyatakan hasil yang dicapai atau memberi bukti suatu aktivitas dilakukan.
31. Sistem informasi adalah serangkaian perangkat keras, perangkat lunak, sumber daya manusia, serta prosedur dan/atau aturan yang diorganisasikan secara terpadu untuk mengolah data menjadi informasi yang memiliki manfaat untuk mencapai suatu tujuan.

32. Sistem Manajemen Keamanan Informasi (SMKI) adalah kerangka kerja manajemen pengamanan informasi yang menggunakan pendekatan berbasis risiko dalam menyusun, menerapkan, melaksanakan, mengawasi, mengkaji, memelihara dan meningkatkan kinerja keamanan informasi.
33. *Teleworking* adalah aktivitas dengan perjanjian kerja untuk melaksanakan pekerjaan secara jarak jauh (*remote*) untuk mengakses informasi atau sistem informasi di sistem atau jaringan internal Pemerintah Provinsi Lampung melalui jaringan eksternal atau publik.
34. Unit kerja adalah organisasi di lingkungan Pemerintah Provinsi Lampung setingkat eselon II, termasuk Unit Pelaksana Teknis.
35. Unit kerja pengelola TIK Pemerintah Provinsi Lampung adalah organisasi yang menyelenggarakan tata kelola, pengelolaan dan pemanfaatan TIK di lingkungan Pemerintah Provinsi Lampung.

BAB II
KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI

A. KETENTUAN UMUM SISTEM MANAJEMEN KEAMANAN INFORMASI

Pimpinan unit kerja harus memastikan tanggung jawab dalam penerapan sistem manajemen keamanan melalui:

1. Unit kerja harus menerapkan kebijakan keamanan informasi sebagaimana diatur dalam Keputusan Gubernur Provinsi Lampung ini di lingkungan Unit Kerja masing-masing.
2. Unit kerja menetapkan ruang lingkup, sasaran dan pernyataan komitmen penerapan SMKI serta penerapan pengendalian SMKI yang dibutuhkan oleh masing-masing unit kerja dengan berbasis risiko.
3. Unit kerja menerapkan dan mengembangkan manajemen risiko dengan mengikuti ketentuan mengenai manajemen risiko yang berlaku di lingkungan Pemerintah Provinsi Lampung. Pertimbangan lain dalam pengelolaan risiko di unit kerja harus memperhatikan:
   a. Kajian risiko yang dilakukan secara periodik minimal 1 (satu) tahun sekali terhadap aset-aset informasi untuk menemukan ancaman (*threat*) dan kelemahan (*vulnerability*) keamanannya serta dampak risiko yang mungkin ditimbulkannya. Tingkat kedalaman kajian risiko akan disesuaikan berdasarkan tingkat kerahasian dan tingkat kerawanan informasi.
   b. Setiap risiko yang perlu dimitigasi berdasarkan hasil kajian risiko perlu dilakukan proses pengendalian risiko dengan memilih opsi penanganan risiko dengan dapat memperhatikan kontrol keamanan informasi berdasarkan standar keamanan atau kontrol lainnya pada peraturan perundang-undangan yang berlaku.
4. Unit kerja harus secara kontinu melakukan sosialisasi dan pelatihan mengenai Keamanan Informasi kepada seluruh pegawai. Sosialisasi dan pelatihan harus mempertimbangkan penerapan kontrol keamanan yang dijalankan pada setiap fungsi yang terdapat di unit kerja di Pemerintah Provinsi Lampung.

5. Unit kerja mengendalikan dan mengkoordinasikan komunikasi, baik internal ataupun eksternal, yang relevan dengan Keamanan Informasi yang bertujuan untuk memastikan adanya informasi terkait Keamanan Informasi kepada pihak-pihak yang berkepentingan.
6. Unit kerja mengelola dokumentasi terkait pengelolaan keamanan informasi dalam suatu prosedur yang bertujuan untuk menjaga kemutakhiran dokumen dan ketersediaannya, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan dan mencegah akses oleh pihak yang tidak berwenang. Pengendalian dokumen juga mengatur mekanisme:
   a. Pengendalian catatan penerapan dan pelaksanaan keamanan informasi dilakukan untuk menjamin agar catatan tersebut dapat tersedia, terpelihara dan terkendali.
   b. Identifikasi dan pendokumentasian informasi terkait dengan keamanan informasi yang berasal dari sumber eksternal untuk memastikan kesesuaian dan kepatuhannya dan dikomunikasikan kepada pihak yang relevan dalam SMKI organisasi.
   c. Semua dokumentasi SMKI harus ditinjau paling sedikit satu kali dalam satu tahun atau apabila terdapat perubahan dalam SMKI dan/atau organisasi untuk menjamin kesesuaian dan kecukupannya.
7. Unit kerja melaksanakan pengendalian SMKI untuk memastikan implementasi dan operasional sistem manajemen keamanan informasi melalui:
   a. Pengelolaan ketersediaan dari sumber daya yang dibutuhkan dalam rangka implementasi keamanan informasi.
   b. Memastikan koordinasi implementasi kontrol keamanan informasi terhadap data dan informasi yang dikelola telah dilakukan secara berkala.
   c. Peningkatan yang berkesinambungan yang dijabarkan dalam program aktivitas Sistem Manajemen Keamanan Informasi.
   d. Tanggung jawab atas terlaksananya kontrol keamanan informasi untuk memastikan perlindungan terhadap data dan informasi yang dikelola.
8. Unit kerja melakukan evaluasi secara berkala untuk menjamin efektivitas dan meningkatkan keamanan informasi, mencakup proses pengukuran efektivitas penerapan SMKI atau pencapaian sasaran, audit internal dan tinjauan manajemen. Mekanisme evaluasi tersebut harus diatur dalam suatu prosedur sendiri. Hasil evaluasi harus didokumentasikan secara jelas dan ditindaklanjuti.
9. Audit internal SMKI dilaksanakan oleh fungsi kepatuhan internal di masing-masing unit kerja atau oleh unit yang mengkoordinasikan fungsi pengawasan internal di Pemerintah Provinsi Lampung. Pelaksanaan audit internal SMKI harus dipastikan telah memiliki kompetensi yang memadai serta memiliki objektivitas dan independen terhadap proses audit.
10. Unit Kerja harus memastikan bahwa setiap ketidaksesuaian telah ditindaklanjuti secara memadai dan memastikan upaya berkelanjutan untuk meningkatkan kinerja dan efektivitas penerapan SMKI.
11. Inisiatif peningkatan harus secara formal diidentifikasi, direncanakan, diimplementasikan dan ditinjau.

B. KETENTUAN PENGENDALIAN PENGAMANAN INFORMASI

Pengendalian pengamanan informasi pada unit kerja diterapkan sesuai dengan ruang lingkup pelaksanaan SMKI di masing-masing unit kerja, mencakup 13 (tiga belas) domain pengendalian sebagai berikut:

1. Kebijakan Keamanan Informasi
   a. Unit kerja menerapkan kebijakan keamanan informasi sebagaimana diatur dalam Keputusan Gubernur ini.
   b. Unit kerja mengkomunikasikan dan mensosialisasikan kebijakan keamanan informasi kepada seluruh pegawai dan pihak terkait di lingkungan masing-masing unit kerja.
   c. Unit kerja melakukan evaluasi dan peninjauan (review) secara berkala atas penerapan kebijakan keamanan informasi di masingmasing unit kerja.
   d. Peninjauan (*review*) berkala atas kebijakan keamanan informasi dikoordinasikan oleh unit pengelola TIK.
2. Organisasi Keamanan Informasi
   a. Organisasi Internal
      i. Pemerintah Provinsi Lampung membentuk Tim Pelaksana Manajemen Keamanan Informasi untuk memastikan penerapan kontrol keamanan informasi yang mencakup namun tidak terbatas pada peran sebagai berikut:
         1) Manajemen Puncak SMKI;
         2) Koordinator SMKI; dan
         3) Tim Keamanan Informasi, yang mencakup fungsi peran setidaknya sebagai berikut:
            a) Pengelolaan standar dan kepatuhan.
            b) Pengelolaan risiko.
            c) Pengendalian dokumen.
            d) Pengelolaan insiden keamanan informasi.
      ii. Peran dan tanggung jawab Tim Pelaksana Manajemen Keamanan Informasi dijabarkan pada lampiran terpisah.
   b. Perangkat Bergerak (*Mobile Device*) dan *Teleworking*
      i. Unit kerja pengelola TIK membangun kepedulian terhadap penggunaan *mobile device* dan *teleworking* terkait risiko keamanan perangkat dan resiko keamanan informasi dari masing-masing penggunaannya.
      ii. Pengguna *mobile device* dan *teleworking* harus mengikuti ketentuan yang berlaku terkait penggunaan *mobile device* dan *teleworking* untuk menjaga keamanan perangkat dan informasi di dalamnya.

3. Keamanan Sumber Daya Manusia
   a. Sebelum Bekerja
      i. Unit kerja, berkoordinasi dengan unit pengelola kepegawaian di Pemerintah Provinsi Lampung, harus melaksanakan pemeriksaan latar belakang calon pegawai dan pihak ketiga yang akan bekerja di unit kerja dengan memperhatikan privasi, perlindungan data pribadi dan/atau pekerjaan, berdasarkan ketentuan peraturan dan perundangan yang berlaku.

ii. Peran dan tanggung jawab pegawai, mitra kerja dan pihak ketiga lainnya terhadap keamanan informasi harus didefinisikan, didokumentasikan dan dikomunikasikan kepada yang bersangkutan sebelum penugasan.

iii. Peran dan tanggung jawab pegawai, mitra kerja dan pihak ketiga lainnya terhadap keamanan informasi harus menjadi bagian dari penjabaran tugas pokok dan fungsi, khususnya bagi mereka yang memiliki akses terhadap aset informasi yang bersifat rahasia, berharga (mempunyai nilai nominal tertentu dan merupakan hasil dari pembelanjaan APBN/APBD) dan rawan (mempunyai aspek nilai intangible atau terkait risiko keamanan terhadap aset informasi lainnya).

b. Selama Bekerja

i. Seluruh pegawai unit kerja serta mitra dan pihak ketiga lainnya harus mematuhi ketentuan terkait keamanan informasi yang berlaku di Pemerintah Provinsi Lampung serta bersedia dikenakan sanksi sesuai ketentuan yang berlaku jika terjadi pelanggaran.

ii. Seluruh pegawai yang bekerja di unit kerja harus mendapatkan pendidikan, pelatihan dan sosialisasi terkait keamanan informasi secara berkala sesuai tingkat tanggung jawabnya.

iii. Mitra dan pihak ketiga lainnya, jika diperlukan, mendapatkan sosialisasi untuk meningkatkan kepedulian terhadap keamanan informasi melalui proses induksi atau metode lain yang tepat.

iv. Terdapat pemberian sanksi yang formal dan dikomunikasikan untuk mengambil tindakan terhadap pegawai yang melakukan pelanggaran keamanan informasi, sesuai dengan kebijakan dan prosedur yang berlaku di institusi.

c. Ketika Terdapat Perubahan Atas Status Kepegawaian

i. Unit kerja harus melakukan peninjauan dan penyesuaian terhadap aset dan hak akses setiap kali terdapat perubahan atas status kepegawaian, baik untuk pegawai maupun mitra atau pihak ketiga.

ii. Setiap pengguna harus mengembalikan sumber daya informasi milik Pemerintah Provinsi Lampung yang digunakannya segera setelah penugasannya berakhir atau sumber daya informasi tersebut tidak lagi digunakan untuk bekerja di unit kerja.

iii. Hak akses pengguna dihapus atau dinonaktifkan segera setelah pengguna berubah tugas dan/atau fungsinya, setelah penugasan berakhir atau mutasi.

iv. Sebelum penghentian, pemutusan hubungan kerja atau mutasi efektif berlaku, unit kerja wajib mengingatkan hak dan kewajiban pegawai, mitra kerja dan pihak ketiga untuk tetap mematuhi kebijakan dan aturan keamanan informasi yang berlaku di Pemerintah Provinsi Lampung terutama yang terkait dengan kewajiban menjaga kerahasiaan.

4. Pengelolaan Aset

a. Tanggung Jawab Terkait Aset

i. Unit kerja melaksanakan identifikasi aset dan mendokumentasikannya dalam daftar inventarisasi aset masing-masing unit kerja.

ii. Aset yang diinventaris adalah aset dalam bentuk:
   1) 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*, perangkat jaringan komunikasi yang terdapat di area kerja.
   2) Perangkat lunak, meliputi perangkat lunak yang digunakan untuk mengolah informasi dalam bentuk elektronik, yang mencakup namun tidak terbatas pada sistem operasi, aplikasi, pemrograman dan program bantu (*utility*).
   3) Informasi, meliputi data-data yang telah diolah dan dilakukan pemrosesan informasi yang mencakup namun tidak terbatas pada database, laporan, catatan atau informasi yang bersifat *hardcopy* maupun *softcopy*.
   4) Perangkat pendukung meliputi perangkat digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan informasi yang mencakup namun tidak terbatas pada UPS, AC dan lemari penyimpanan informasi.
   5) Sumber daya manusia meliputi personil baik internal maupun eksternal yang terlibat dalam pengolahan dan penyimpanan informasi.
   6) 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*.

iii. Pemilik aset bertanggung jawab terhadap perlindungan keamanan seluruh aset informasi yang berada dibawah pengawasannya.

iv. Ketentuan penggunaan aset mengacu pada Pedoman Penggunaan Aset TI yang berlaku di Pemerintah Provinsi Lampung. Seluruh pengguna aset, tanpa kecuali, wajib mematuhi kebijakan dan aturan yang telah ditetapkan.

b. Klasifikasi Informasi

i. Seluruh informasi yang dikelola unit kerja harus diklasifikasikan sesuai tingkat kerahasiaan, nilai, ketentuan/kebutuhan kegiatan yang menggunakannya, tingkat kerahasiaan, tingkat kritikalitas serta aspek hukumnya dan dinyatakan secara jelas pada daftar aset informasi.

ii. Pemerintah Provinsi Lampung menetapkan 3 (tiga) golongan aset informasi sebagai berikut:
   1) Rahasia
      Merupakan informasi yang sangat peka dan berisiko tinggi. Hilangnya informasi ini akan menyebabkan kerugian finansial dan/atau gangguan operasional yang sangat besar. Pihak ketiga dapat mengakses informasi ini secara terbatas karena kewajiban dan kebutuhan Pemerintah Provinsi Lampung melalui serah terima resmi dengan syarat pihak ketiga dan pegawai pihak ketiga menandatangani Kesepakatan Kewajiban Menjaga Rahasia/*Non-Disclosure Agreement*. Contoh: Topologi Jaringan, IP *address*, *password* komputer, bahan/materi pelatihan, rencana anggaran atau pengadaan, data gaji dan penilaian kinerja pegawai, hasil *penetration test*, dan *log system administrator*.

2) Terbatas

Merupakan aset informasi yang telah terdistribusi secara luas di lingkungan internal Pemerintah Provinsi Lampung yang penyebarannya secara internal tidak lagi memerlukan izin dari Pemilik Aset Informasi dan risiko penyebarannya oleh pihak yang tidak berwenang tidak menimbulkan kerugian yang berarti. Informasi ini dapat diberikan kepada pihak ketiga oleh pemiliknya untuk kepentingan dinas melalui prosedur serah terima resmi. Contoh: kebijakan Pemerintah Provinsi Lampung, panduan kerja, prosedur kerja, instruksi kerja, memo/publikasi internal, informasi yang disediakan dalam intranet, dokumen kontrak dan data operasional TI lainnya.

3) Publik

Merupakan aset informasi yang secara sengaja disediakan Pemerintah Provinsi Lampung untuk dapat diketahui publik/masyarakat umum. Contoh: brosur, situs publik Pemerintah Provinsi Lampung dan siaran pers (*press release*).

iii. Pemberian label klarifikasi informasi harus dilakukan secara konsisten terhadap seluruh asset informasi. Ketentuan tata cara pemberian label klarifikasi informasi dan penanganannya ditetapkan oleh masing-masing unit kerja.

iv. Penanganan terhadap aset informasi harus mempertimbangkan tingkat klasifikasi yang telah ditetapkan oleh unit kerja. Penanganan informasi rahasia perlu mempertimbangkan proses siklus informasi mulai dari pembuatan, penggunaan, penyimpanan, distribusi, peminjaman, hingga pemusnahan. Tingkat perlindungan dan pembatasan akses harus diterapkan.

v. Untuk informasi yang bersifat terbatas dan publik tidak terdapat perlakuan khusus dan penanganan terhadap informasi tersebut ditentukan oleh unit kerja pemilik informasi.

c. Penanganan Media

i. Penggunaan media penyimpan yang bergerak harus diperhatikan terkait penanganan dari data/informasi sesuai dengan tingkat kritikalitas dari informasi.

ii. Informasi yang terkandung dalam media penyimpan informasi yang bisa dipakai ulang dan digunakan sebagai media transit (media yang bergerak) harus dihapus jika tidak lagi diperlukan dan harus dipastikan bahwa salinan asli informasi tersebut masih tersedia.

iii. Seluruh media penyimpanan informasi mudah jinjing (*removable*) harus diformat ulang dengan teknit tertentu sehingga data tidak bisa dikembalikan. Tetapi jika hal tersebut tidak bisa dilakukan, media tersebut harus dihancurkan.

iv. Media kertas (termasuk *carbon copies*, cetakan printer) yang mengandung informasi RAHASIA dihancurkan dengan menggunakan alat penghancur kertas atau dibakar.

v. Media lain, seperti disket, tape, CS, DVD, USB *flash disk* dan lain-lain harus dirusak secara fisik sehingga isinya tidak bisa diakses oleh pihak yang berwenang.

vi. Pertukaran informasi antara Pemerintah Provinsi Lampung dengan pihak lain melalui media fisik hanya akan dilakukan atas persetujuan tertulis kedua belah pihak. Pengamanan media fisik harus diperhatikan sesuai dengan informasi yang tersimpan berdasarkan tingkat kritikalitas informasi agar keamanan data terjamin saat proses pertukaran tersebut.

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

5. Pengendalian Akses

a. Unit kerja menyusun, mendokumentasikan dan mengkaji ketentuan akses terhadap aset berdasarkan kebutuhan organisasi persyaratan keamanan informasi. Ketentuan hak akses harus didokumentasikan dalam bentuk matriks hak akses.

b. Hak penggunaan/akses terhadap aset-aset informasi diberikan sesuai dengan kebutuhan fungsi dan tugas pengguna dan diberikan berdasarkan prinsip minimum/seperlunya, yaitu cukup untuk memenuhi kebutuhan *user* dalam menjalankan tugasnya.

c. Persyaratan untuk pengendalian hak akses mencakup:

i. 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; dan
4) Didasarkan atas prinsip *need to know* dan *need to use*, yaitu disesuaikan dengan kebutuhan pekerjaan dan operasional dalam lingkungan Pemerintah Provinsi Lampung.

ii. Pemisahan peran pengendalian akses, seperti administrasi akses dan otorisasi akses.

1) Unit kerja pengelola TIK mengatur dan membatasi akses pengguna dalam mengakses jaringan internal Pemerintah Provinsi Lampung sesuai peruntukannya.
2) Unit kerja pemilik sistem informasi harus mengembangkan mekanisme pemberian hak akses pengguna dan hak akses khusus yang dikelola secara formal pada seluruh siklusnya, mulai dari proses pendaftaran, penyediaan, peninjauan (*review*), penghapusan/penonaktifan dan penyesuaian, serta dilaksanakan oleh para pihak terkait sesuai jenjang kewenangannya.
3) Setiap permintaan registrasi dari pengguna harus disertai surat permohonan dan harus disetujui oleh pimpinan dari pemilik sistem informasi.
4) Hak akses khusus (*privileged access rights*) harus sangat dibatasi kepada personil yang terotorisasi dan terlatih. Hak akses khusus harus disetujui dan didokumentasikan secara formal. Pertimbangan dalam pembuatan hak akses khusus mencakup:
   a) Hak akses khusus untuk pihak ketiga hanya diberikan sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu.

b) Hak akses khusus tidak boleh diberikan sebelum proses otorisasi dilakukan oleh pimpinan pemilik sistem informasi.
c) Apabila memungkinkan, hak akses khusus harus dialokasikan secara individual dan tidak di-*share*. Hal ini dilakukan untuk menjamin akuntabilitas dari pengguna khusus.
d) Pencabutan hak akses khusus harus dilakukan setelah penggunaan hak akses tersebut telah selesai dan alokasi dari hak akses khusus harus ditinjau secara berkala dan setiap terdapat perubahan dalam status penggunaan akses tersebut.

5) Unit kerja memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya.
6) Setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan menyesuaikan atau menghapus hak akses khusus yang menyimpang.
7) Pengelola sistem informasi mengatur akses pengguna dalam mengakses informasi pada sistem informasi sesuai peruntukannya. Pengelola sistem informasi menjamin bahwa akses terhadap informasi hanya diberikan bagi mereka yang memerlukan akses dalam menjalankan pekerjaannya.
8) Pemilik Aset Informasi harus memastikan bahwa sistem dan aplikasi dibawah pengelolaannya memiliki fasilitas manajemen hak akses pengguna, manajemen password yang baik serta mekanisme otentikasi pengguna yang aman.
9) Ketentuan *password* yang ditetapkan di Pemerintah Provinsi Lampung adalah:
   a) Minimum terdiri dari 8 (delapan) karakter.
   b) Tidak boleh menggunakan password yang mudah ditebak dan tidak terdiri dari informasi pribadi seperti ulang tahun pengguna, nama perusahaan, atau nama pengguna.
10) Unit kerja pengelola TIK bertanggung jawab untuk membatasi dan mengendalikan penggunaan system utilities pada sistem informasi. 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.
11) Unit kerja pengelola sistem informasi harus memastikan bahwa source code dikelola dan disimpan secara memadai baik yang dikembangkan oleh internal Unit kerja maupun yang dikembangkan oleh penyedia jasa aplikasi.
12) Untuk sistem aplikasi yang dikembangkan oleh penyedia jasa/pihak ketiga, *source code* dan akses terkaitnya harus diserahkan kepada Pemerintah Provinsi Lampung. Penyedia jasa/pihak ketiga harus menjaga kerahasiaan informasi dan tidak menyebarluaskan kepada pihak yang tidak berwenang.

6. Kriptografi
   a. Unit kerja pengelola TIK menerapkan kriptografi yang tepat dan efektif untuk melindungi kerahasiaan, keabsahan dan integritas dari informasi.

b. Sistem kriptografi harus digunakan untuk melindungi aset informasi yang memiliki klasifikasi RAHASIA.

7. Pengelolaan Keamanan Fisik dan Lingkungan
   a. Pengamanan Area
      i. Unit kerja harus menerapkan perimeter keamanan fisik untuk melindungi daerah-daerah yang berisi informasi dan fasilitas pengolahan informasi.
      ii. Pemerintah Provinsi Lampung menetapkan pengelompokan area wilayah/fisik di lingkungan Pemerintah Provinsi Lampung ke dalam 3 (tiga) kategori sebagai berikut:
         1) Area Publik Area Publik merupakan wilayah area yang dapat dimasuki oleh seluruh pihak. Area publik meliputi: area *lobby*, area penerimaan tamu/resepsionis.
         2) Area Terbatas Area Terbatas merupakan wilayah area yang hanya dapat dimasuki oleh seluruh pegawai dan unit kerja serta tamu yang telah diberikan izin akses. Area Terbatas meliputi: area kerja dari unit kerja.
         3) Area Tertutup Area Tertutup merupakan wilayah area dimana terdapat proses dan/atau perangkat yang bersifat kritikal/sensitif dan hanya diperbolehkan diakses oleh kalangan pegawai tertentu dari unit kerja serta tamu yang telah memperoleh izin atau otorisasi khusus. Area Tertutup meliputi antara lain: ruang Data *Center* dan DRC, ruang perangkat jaringan, ruang arsip, ruang keuangan.
      iii. Unit kerja harus menetapkan ketentuan aturan pembatasan atau prosedur untuk bekerja di area terbatas dan tertutup. Mekanisme pembatasan ini dapat dilakukan dengan aturan penerimaan tamu yang diterapkan berdasarkan kritikalitas area tersebut.
      iv. Untuk area data *center*, *disaster recovery center*, ruang jaringan dan ruang arsip harus dilindungi dengan menerapkan pengamanan fisik pada perimeter area tersebut dengan kriteria:
         1) Konstruksi dinding, atap dan lantai yang kuat.
         2) Pintu akses menuju area harus dilengkapi dengan mekanisme kontrol akses, seperti: *access door lock*.
         3) Pintu dan jendela harus senantiasa dalam kondisi terkunci, khususnya pada saat tanpa penjagaan.
         4) Perangkat CCTV perlu terpasang pada sisi eksterior dan interior area.
         5) Tidak diperbolehkan menyimpan bahan-bahan berbahaya yang mudah terbakar.
      v. Pengendalian akses masuk fisik
         1) 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.
         2) Kunjungan ke dalam area tersebut harus disetujui secara formal oleh pengelolaan area tersebut.
         3) Selama kunjungan di dalam area tersebut, pengunjung harus senantiasa didampingi oleh personil unit kerja.

vi. Seluruh area yang terdapat perangkat pemrosesan informasi harus terlindungi dari terjadinya pencurian dan akses oleh pihak yang tidak berwenang.

vii. Setiap area harus dipastikan terdapat alat pemadam kebakaran kebakaran ringan (APAR) dan diusahakan terdapat sistem pendeteksi asap (*smoke detector*) dan/atau sistem pemercik api otomatis (*sprinkler system*). Sistem pemadam kebakaran harus dipelihara secara berkala melalui pengujian rutin.

viii. Aktivitas pada area-area kritikal harus disertai dengan fasilitas CCTV dan dimonitor secara berkala.

ix. Unit Kerja menjaga, mengawasi, dan mengendalikan area keluar masuk barang untuk menghindari risiko akses yang tidak terotorisasi ke informasi dan ke perangkat pengolah informasi.

b. Pengamanan Perangkat

i. Seluruh perangkat harus ditempatkan di lokasi yang aman dan diposisikan sedemikian rupa untuk mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang serta ancaman lingkungan/eksternal seperti: kebakaran, air, debu.

ii. Perangkat pendukung harus dipasang/tersedia untuk menjamin beroperasinya perangkat pengolah informasi dan secara berkala harus diperiksa dan diuji ulang kinerjanya.

iii. Perangkat pengolah informasi (termasuk mesin faksimili, printer, komputer) yang digunakan untuk memproses informasi RAHASIA harus ditempatkan di lokasi yang aman untuk mencegah penyingkapan informasi tersebut ke pihak yang tidak berwenang.

iv. Penempatan kabel data dan sumber daya listrik harus dilindungi dari kerusakan.

v. Pasokan listrik yang digunakan untuk mengoperasikan perangkat pengolah informasi Pemerintah Provinsi Lampung harus mempunyai sumber alternatif dengan daya dan jangka waktu ketersediaan (jangka waktu pengoperasian) yang cukup.

vi. Unit Kerja harus melaksanakan pemeliharaan (*maintenance*) perangkat secara berkala serta melindungi perangkat dan fasilitas pengelolaan informasi dari gangguan, ancaman, dan bencana dalam rangka memastikan ketersediaan, keutuhan, dan fungsinya berjalan dengan baik. Proses pemeliharaan tersebut mencakup aktivitas sebagai berikut:

1) Seluruh perangkat pengolah informasi penting dan peralatan pendukung harus diperiksa dan diujicoba efektivitasnya secara teratur/berkala, dirawat dan dibersihkan sesuai dengan spesifikasi pabrikannya.

2) Perawatan dan perbaikan perangkat pengolah informasi hanya dilakukan oleh personil yang berwenang dan mempunyai kompetensi teknis yang sesuai.

3) Bagi pemeliharaan yang tidak dapat dilakukan di lokasi kantor Unit Kerja, maka informasi rahasia dan kritikal yang tersimpan dalam peralatan tersebut harus dipindahkan terlebih dahulu dan harus mendapatkan persetujuan dari pejabat yang berwenang.

vii. Perangkat pengolah informasi penyimpan data yang tidak lagi digunakan harus disanitasi sebelum digunakan kembali atau dihapuskan/dimusnahkan. Perangkat pengolah informasi dimusnahkan menggunakan metode dan prosedur pemusnahan yang mempertimbangkan aspek keamanan informasi agar tidak bisa dibaca dan digunakan lagi oleh pihak yang tidak berwenang.

viii. Penggunaan perangkat keras yang dibawa ke luar area kerja diperbolehkan tetapi harus disetujui oleh pejabat yang berwenang

ix. Pengguna harus memastikan aset yang tidak berada dalam pengawasan secara langsung atau yang digunakan diluar area kerja, telah diberikan perlindungan keamanan yang memadai.

x. Pengguna harus memastikan bahwa tidak terdapat atau tertampilkan informasi rahasia pada perangkat atau media yang digunakan ketika meninggalkan area kerja

8. Keamanan Operasional

a. Prosedur Operasional dan Tanggung Jawab

i. Unit kerja harus mendokumentasikan, memelihara dan menyediakan prosedur operasional terkait dengan penggunaan perangkat pengolah informasi bagi pengguna sesuai peruntukannya.

ii. Unit kerja harus mengendalikan setiap perubahan terkait organisasi, proses bisnis dan fasilitas pengolah informasi, yang berdampak pada keamanan informasi. Proses pengendalian terhadap perubahan setidaknya mencakup proses permohonan, analisa dan evaluasi serta persetujuan. Seluruh proses terkait pengelolaan perubahan harus didokumentasikan.

iii. Unit kerja harus memantau penggunaan atau utilisasi kapasitas sumber daya yang dimiliki serta membuat proyeksi kebutuhan ke depan untuk menjamin ketersediaan aset yang diperlukan. Pemantauan kapasitas tersebut dengan mempertimbangkan batas ambang kapasitas yang ditetapkan.

iv. Unit kerja pengelola TIK harus melakukan pemilahan lingkungan pengembangan, pengujian dan operasional sistem informasi untuk mengurangi risiko perubahan dan/atau akses oleh pihak yang tidak berwenang terhadap sistem informasi.

b. Perlindungan Terhadap Ancaman Program Yang Membahayakan (*Malware*)

i. Unit kerja harus menerapkan sistem yang mampu melakukan pendeteksian, pencegahan dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan (*malware*).

ii. Sistem sebagaimana disebutkan pada butir i harus senantiasa dipantau dan dimutakhirkan untuk memastikan kesesuaiannya dengan kondisi terkini.

iii. Unit kerja pengelola TIK harus memantau dan mengevaluasi jaringan dari ancaman virus dan dapat menutup akses ke website yang dapat menimbulkan ancaman kepada sistem informasi.

iv. Setiap insiden terkait dengan malware harus dilaporkan kepada Tim Penanggulangan Insiden (CSIRT) dan dikategorikan sebagai insiden keamanan informasi.

c. Pengelolaan Pencadangan (*Backup*) Informasi
   i. Unit kerja mengidentifikasi informasi penting dan/atau kritikal yang dimiliki atau dikelola untuk kemudian menetapkan perencanaan pencadangan (*backup*) informasi yang mencakup setidaknya: jenis/nama informasi, metode dan/atau media *backup* serta periode/frekuensi pelaksanaan *backup*.
   ii. Unit kerja melaksanakan proses *backup* secara berkala sesuai dengan perencanaan yang telah ditetapkan untuk menjamin keutuhan dan ketersediaannya saat diperlukan.
   iii. Data *backup* harus diuji secara berkala untuk memastikan keutuhannya

d. Pengelolaan dan Pemantauan Data Aktivitas (*Log*)
   i. Unit kerja pemilik sistem informasi harus memastikan bahwa pencatatan aktivitas (*log*) pada sistem, yang mencakup: aktivitas pengguna, *exceptions*, *fault*, kejadian (*event*) keamanan informasi serta aktivitas administrator dan operator sistem; telah dapat tercatat/terekam, tersimpan secara aman, dan ditinjau (*review*) secara berkala untuk membantu pengendalian akses dan investigasi dimasa mendatang.
   ii. Fasilitas pencatatan *log* dan informasi *log* yang dicatat harus dilindungi dari penghapusan dan akses oleh pihak yang tidak berwenang.
   iii. Unit kerja pemilik sistem informasi harus memastikan bahwa seluruh perangkat pengolah informasi yang dikelolanya telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.
   iv. Data aktifitas (*log*) yang sudah tidak terpakai dapat dihapuskan sesuai prosedur yang berlaku.

e. Pengendalian Perangkat Lunak
   i. Proses untuk mengendalikan instalasi perangkat lunak pada sistem operasional harus ditetapkan dan diimplementasikan untuk memastikan terjaganya kerahasiaan, integritas dan ketersediaan informasi.
   ii. Ketentuan terkait instalasi perangkat lunak pada sistem operasional dan pada perangkat pengolah informasi di pengguna ditetapkan oleh unit kerja pengelola TIK di Pemerintah Provinsi Lampung.
   iii. Instalasi perangkat lunak hanya diperbolehkan untuk dilakukan oleh personil yang telah ditunjuk atau fungsi yang berwenang sesuai tugas dan tanggung jawabnya.
   iv. Perangkat lunak yang diinstal harus perangkat yang berlisensi atau *opensource* serta dapat diketahui asalnya usulnya.

f. Pengelolaan Kerentanan Teknis
   i. Unit kerja pengelola TIK harus melaksanakan evaluasi dan penilaian terkait kerentanan teknis pada sistem dan teknologi informasi di Pemerintah Provinsi Lampung serta menerapkan pengendalian dan penanganan yang memadai terhadap kerentanan yang ditemukan.
   ii. Pelaksanaan aktivitas terkait evaluasi kerentanan teknis dan audit sistem informasi harus direncanakan secara seksama agar tidak menimbulkan gangguan terhadap operasional sistem informasi di Pemerintah Provinsi Lampung.

9. Keamanan Komunikasi
   a. Pengelolaa Keamanan Jaringan
      i. Unit kerja pengelola TIK bertanggung jawab atas pengelolaan dan pengendalian keamanan jaringan termasuk memisahkan jaringan untuk pengguna, sistem informasi dan layanan informasi.
      ii. Pengelolaan keamanan jaringan meliputi:
         1) Pemantauan dan evaluasi kegiatan pengelolaan jaringan;
         2) Pengendalian dan pengaturan tentang penyambungan atau perluasan jaringan internal atau eksternal Pemerintah Provinsi Lampung ;
         3) Pengendalian dan pengaturan akses ke sistem jaringan internal atau eksternal Pemerintah Provinsi Lampung;
         4) Pencatatan informasi pihak ketiga yang diizinkan mengakses ke jaringan Pemerintah Provinsi Lampung dan menerapkan pemantauan serta pencatatan kegiatan selama menggunakan jaringan;
         5) Pemutusan layanan jaringan jika terjadi gangguan keamanan informasi; dan
         6) Perlindungan jaringan dari akses yang tidak berwenang.
      iii. Unit kerja pengelola TIK harus menerapkan fitur keamanan layanan dan memberikan jaminan layanan jaringan yang tertuang dalam kesepakatan penyediaan layanan, termasuk layanan yang disediakan oleh Pihak Ketiga.
   b. Keamanan dalam Perpindahan (*Transfer*) Informasi
      i. Penyediaan informasi internal Pemerintah Provinsi Lampung bagi masyarakat umum harus disetujui oleh pemilik informasi dan dilindungi keutuhannya dari modifikasi oleh pihak yang tidak berwenang.
      ii. Pertukaran informasi penting dan/atau rahasia, hanya dilakukan jika telah terdapat pengendalian pengamanan yang memadai serta penetapan ketentuan-ketentuan keamanan informasi dalam perjanjian pertukaran informasi antara pihak yang terkait.
      iii. Pertukaran informasi melalui sarana surat elektronik harus memperhatikan prinsip perlindungan data dan informasi baik dari aspek penggunaan oleh pegawai maupun dari teknologi yang diterapkan.
      iv. Akses ke informasi dan sistem informasi baik oleh pegawai maupun pihak ketiga hanya diberikan untuk pelaksanaan kegiatan di Pemerintah Provinsi Lampung dan setelah perjanjian kesepakatan Kewajiban Menjaga Rahasia (*Non-Disclosure Agreement*/NDA) disetujui oleh kedua belah pihak.

10. Akusisi, Pengembangan dan Pemeliharaan Sistem
    a. Persyaratan Keamanan Pada Sistem Informasi
       i. Pengembangan sistem informasi dalam hal ini mencakup proses atau aktivitas pembangunan sistem informasi baru, peningkatan (*enhancement*) dan/atau penambahan fungsi/fitur baru serta perbaikan kode program (*bugs fixing*).

ii. Pemilik sistem informasi harus mengidentifikasi, menetapkan dan mendokumentasikan secara jelas persyaratan-persyaratan keamanan informasi yang relevan sebelum pelaksanaan pengembangan sistem informasi, pada dokumen persyaratan dan spesifikasi perangkat lunak.

iii. Persyaratan dan spesifikasi sebagaimana tercantum pada butir i harus disetujui dan disepakati bersama antara pemilik aset informasi yang terlibat serta pihak pengembang sistem sebelum kegiatan pengembangan sistem informasi dimulai.

iv. Unit kerja pengelola TIK harus melindungi informasi dalam layanan aplikasi yang melewati jaringan publik dari kemungkinan aktivitas penipuan (*fraud*), perselisihan kontrak (*contract dispute*) dan pengungkapan informasi yang tidak sah.

v. Unit kerja pengelola TIK harus melindungi informasi dalam transaksi pada layanan aplikasi untuk mencegah transmisi yang tidak lengkap, kesalahan routing dan perubahan serta pengungkapan dan duplikasi pesan yang tidak sah.

b. Keamanan Dalam Proses Pengembangan dan Pendukung

i. Unit kerja pengelola TIK harus menetapkan ketentuan pengembangan sistem informasi yang aman.

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

iii. Unit kerja yang melakukan pengembangan sistem informasi harus mengawasi dan memantau pengembangan sistem informasi yang dilakukan oleh pihak ketiga untuk memastikan bahwa proses pengembangannya memenuhi syarat-syarat keamanan informasi yang ditetapkan dalam kontrak.

iv. Aturan untuk pengembangan sistem harus ditetapkan dan diimplementasikan untuk proses pengembangan sistem di Pemerintah Provinsi Lampung, mencakup setidaknya:
   1) Panduan *secure coding*;
   2) Pengendalian versi aplikasi;
   3) Pengelolaan penyimpanan *source code*;
   4) Metode pengujian untuk mengidentifikasi dan memperbaiki kerentanan.

v. Pengendalian perubahan pada proses pengembangan sistem informasi harus dikendalikan untuk memastikan keakuratan sistem informasi yang sedang dikembangkan.

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

vii. Apabila *platform* operasional, misalnya sistem operasi, database dan/atau *middleware*, dari sistem informasi Pemerintah Provinsi Lampung mengalami perubahan, harus dilakukan peninjauan dan pengujian terhadap sistem informasi/aplikasi kritikal Pemerintah Provinsi Lampung untuk memastikan tidak ada dampak buruk terhadap operasional dan keamanan organisasi.

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

ix. Unit kerja yang melakukan pengembangan sistem informasi harus melakukan perlindungan terhadap lingkungan pengembangan sepanjang siklus pelaksanaan pengembangan sistem/*System Development Life Cylce* (SDLC) dan melakukan pengawasan dalam hal pengembangan dilakukan oleh pihak eksternal/pihak ketiga.

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

xi. Unit kerja pemilik sistem informasi harus mengawasi aktivitas pengembangan sistem yang dialihdayakan (*outsourced*). Hal ini mencakup setidaknya:
   1) Perjanjian terkait lisensi dan kepemilikan sistem.
   2) Pengujian penerimaan sistem untuk menguji kualitas dan akurasi dari system
   3) Prasyarat dokumentasi untuk sistem.

xii. Unit kerja yang melakukan pengembangan sistem informasi bertanggung jawab untuk membuat perencanaan, melaksanakan pengujian aplikasi yang mencakup pendekatan/metode, alur dan parameter pengujian. Proses pengujian sistem informasi mencakup beberapa hal sebagai berikut:
   1) Menetapkan kriteria dan jadwal untuk pengujian penerimaan system, baik untuk pengembangan sistem informasi baru serta peningkatan (*enhancement*) dan versi baru dari sistem informasi.
   2) Pengujian terhadap suatu aplikasi, dapat dilakukan secara bertingkat mulai dari unit testing, *System Integration Testing* (SIT), sampai dengan *User Acceptance Testing* (UAT).
   3) Unit testing dipersiapkan dan dilakukan oleh masing-masing pengembang (*developer*) pada lingkungan pengembangan dengan mengacu kepada standar pengujian yang telah ditentukan.
   4) *System Integration Testing* (SIT) dilakukan di lingkungan pengembangan/pengujian, oleh pengembang bersama dengan unit kerja pengelola TIK dan unit pemilik sistem informasi.
   5) *User Acceptance Testing* (UAT) dilakukan di lingkungan pengujian di infrastruktur milik Pemerintah Provinsi Lampung, oleh unit pemilik sistem informasi bersama dengan pengguna (user) terkait dan unit kerja pengelola TIK.

c. Data Pengujian

i. Data yang digunakan dalam pengujian sistem (*system test data*) harus dilindungi dari kemungkinan rusak, hilang atau perubahan yang dilakukan tanpa ijin.

ii. Pengamanan terhadap data hasil pengujian perlu memperhatikan hal-hal sebagai berikut:
   1) Data untuk pengujian sistem harus dipilih secara hati-hati. Hal ini untuk menghindari pengungkapan atau perubahan informasi sensitif oleh pihak yang tidak berhak serta melindung dari kemungkinan kerusakan dan kehilangan informasi.

2) *Masking* data harus dilakukan apabila data operasional yang sensitif digunakan untuk keperluan pengujian.
3) Data operasional (*production*) yang digunakan untuk keperluan pengujian harus dihapus dari lingkungan/server pengujian segera setelah proses pengujian telah selesai dilaksanakan.

11. Pengelolaan Gangguan Keamanan Informasi (Pengelolaan Insiden Keamanan Informasi)
    a. Unit kerja pengelola TIK menyusun dan menetapkan ketentuan terkait dengan pengelolaan gangguan keamanan informasi.
    b. Unit kerja memastikan bahwa setiap kelemahan keamanan informasi dan kejadian keamanan informasi dalam sistem atau layanan TIK harus dilaporkan dan ditindaklanjuti secepat mungkin sesuai mekanisme yang berlaku dan terdokumentasi.
    c. Unit kerja harus memastikan pengelolaan dan penanganan gangguan keamanan informasi dilakukan sesuai dengan prosedur.
    d. Tindakan untuk memulihkan keamanan dari pelanggaran dan perbaikan kegagalan sistem harus dikendalikan secara hati-hati dan formal.
    e. Unit kerja pengelola TIK atau unit/fungsi terkait dengan pengelolaan gangguan keamanan informasi mendokumentasikan seluruh gangguan keamanan informasi yang terjadi beserta tindakan perbaikannya untuk digunakan sebagai basis pengetahuan agar dapat mengurangi peluang atau dampak gangguan dimasa mendatang.
    f. Seluruh gangguan keamanan informasi yang terjadi dan tindakan mengatasinya harus dicatat/didokumentasikan dalam pelaporan gangguan keamanan informasi, dan akan menjadi masukan pada proses peningkatan penanganan gangguan keamanan informasi.
    g. Pengetahuan yang diperoleh dari proses analisa dan penyelesaian masalah insiden keamanan informasi digunakan untuk mengurangi kemungkinan atau dampak dari insiden di masa depan.

12. Pengendalian Pengelolaan Kelangsungan Kegiatan Dari Sisi Keamanannya
    Keamanan informasi dalam pengelolaan kelangsungan kegiatan bertujuan untuk melindungi sistem informasi, memastikan berlangsungnya kegiatan dan layanan pada saat keadaan darurat serta memastikan pemulihan yang tepat.
    a. Perencanaan Kelangsungan Keamanan Informasi
        i. Pemerintah Provinsi Lampung mengembangkan suatu Kebijakan Pengelolaan Kelangsungan Kegiatan sistem informasi Pemerintah Provinsi Lampung untuk mengurangi dampak kegagalan sistem informasi atau bencana yang menyebabkan terganggunya kegiatan Pemerintah Provinsi Lampung.
        ii. Kebijakan Pengelolaan Kelangsungan Layanan TIK dilakukan dengan mempertimbangkan:
            1) Identifikasi aset-aset informasi vital dan sensitif, khususnya yang berklasifikasi RAHASIA.
            2) Identifikasi kejadian-kejadian yang menyebabkan gangguan tehadap proses kegiatan penting.

iii. Unit kerja harus menetapkan Prasyarat untuk keberlanjutan keamanan informasi dan diintegrasikan dengan prasyarat keberlanjutan bisnis organisasi untuk menjamin keberlanjutan dari keamanan informasi di Pemerintah Provinsi Lampung, pada saat dan setelah terjadinya gangguan besar atau bencana.

iv. Prasyarat keamanan informasi dapat diintegrasikan pada siklus proces *business continuity management* yang mencakup:
   1) Memahami kebutuhan organisasi.
   2) Menentukan strategi BCM.
   3) Mengembangkan dan mengimplementasikan rencana penanggulangan/keberlanjutan bisnis.
   4) Pengujian, pemeliharaan dan peninjauan rencana penanggulangan/keberlanjutan bisnis.

v. Tim Pengelola Keamanan Informasi Pemerintah Provinsi Lampung mengelola DRP dan salinannya serta informasi lain yang diperlukan dalam penanganan disaster di lokasi yang aman dan mudah dijangkau.

vi. Pelaksanaan Rencana Keberlangsunan Keamanan Informasi
   1) Pengelolaan Kelangsungan sistem Pemerintah Provinsi Lampung harus dilaksanakan untuk menjamin tetap beroperasinya Pemerintah Provinsi Lampung pada keadaan darurat sesuai dengan kebutuhan dan jangka waktu yang ditetapkan.
   2) Penanggulangan keadaan darurat secara langsung ditangani oleh Tim Pengelola Keamanan Informasi yang keanggotaannya disesuaikan setiap satu tahun sekali.
   3) Unit kerja yang dalam pelaksanaan tugas dan fungsinya mengandalkan layanan Data *Center* Pemerintah Provinsi Lampung harus mempersiapkan prosedur kerja alternatif sesuai dengan ketentuan yang berlaku untuk mengurangi gangguan operasional pada saat terjadi keadaan darurat.
   4) Tim Pengelolaan BCP Keamanan Informasi Pemerintah Provinsi Lampung memastikan kesiapan dan keahlian pegawai serta pihak terkait lainnya dalam menghadapi keadaan darurat dengan melaksanakan pelatihan secara berkala.

vii. Verifikasi, Reviu dan Evaluasi Keberlangsunan Keamanan Informasi
   1) Tim Pengelola BCP harus merencanakan dan mengkoordinasikan kegiatan uji coba secara berkala terhadap proses, prosedur, petunjuk pelaksanaan, sarana dan perangkat, untuk memastikan apakah berfungsi sebagaimana mestinya pada saat diperlukan
   2) Pemerintah Provinsi Lampung menerapkan dua metode uji coba yaitu:
      a) Uji fungsi (*functional testing*) untuk memastikan bagianbagian dari *Disaster Recovery Plan* berfungsi sebagaimana mestinya. Uji fungsi dilaksanakan secara periodik.
      b) Uji coba keseluruhan (*full scale testing*) untuk memastikan seluruh bagian dari *Disaster Recovery Plan* berfungsi sebagaimana mestinya. Uji coba keseluruhan dilaksanakan secara periodik.

c) Uji coba keseluruhan harus dapat mensimulasikan kondisi darurat yang paling mendekati keadaan nyata dengan menggunakan skenario terburuk.

3) Pelaksanaan uji coba harus memperhatikan hal-hal berikut:
   a) Kesesuaian dengan kebutuhan.
   b) Kemungkinan timbulnya dampak negatif.
   c) Waktu dan lama pelaksanaan.
   d) Kebutuhan sumberdaya dan biaya.
   e) Kesiapan pelaksanaan.
   f) Ketergantungan dengan pihak ketiga.
4) Hasil uji coba (uji fungsi dan uji coba keseluruhan) harus dievaluasi dan dijadikan sebagai masukan untuk perbaikan *Disaster Recovery Plan*, termasuk didalamnya perbaikan profil risiko, rencana mitigasi, materi pelatihan dan *awareness*.
5) Seluruh proses, prosedur dan petunjuk pelaksanaan Pengelolaan Kelangsungan sistem Pemerintah Provinsi Lampung dan *Disaster Recovery Plan* harus terdokumentasi dengan baik dan senantiasa diperbaharui sesuai dengan kebutuhan.
6) Tim Pengelola BCP harus melakukan reviu terhadap akurasi proses, prosedur dan petunjuk pelaksanaan secara berkala minimal 1 kali dalam 1 tahun.

13. Kepatuhan

a. Kepatuhan Terhadap Persyaratan Hukum dan Kontrak

i. Unit kerja pengelola TIK, berkoordinasi dengan unit/fungsi terkait hukum/legal, harus mengidentifikasi, mendokumentasikan dan memelihara kemutakhiran seluruh persyaratan peraturan perundang-undangan dan kontrak terkait dengan keamanan informasi.

ii. Seluruh pengguna, baik internal Pemerintah Provinsi Lampung maupun pihak ketiga, harus memastikan pemenuhan kepatuhan terhadap peraturan perundang-undangan dan persyaratan kontrak terkait dengan hak atas kekayaan intelektual dan penggunaan materi berlisensi.

iii. Unit kerja pengelola TIK bertanggung jawab atas pengendalian terhadap penggunaan kriptografi dalam rangka kepatuhan terhadap perjanjian dan peraturan perundang-undangan.

iv. Rekaman milik Pemerintah Provinsi Lampung harus dilindungi dari kehilangan, kerusakan, pemalsuan, akses yang tidak sah, dan rilis yang tidak sah.

v. Privasi dan perlindungan terhadap informasi identitas pribadi harus dipastikan sebagaimana dipersyaratkan dalam peraturan perundang-undangan yang berlaku. Kepemilikan dan kerahasiaan data pribadi yang terdapat pada sistem informasi harus dijaga dan dilindungi secara memadai, data pribadi hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan dan ketentuan perundang-undangan.

b. Peninjauan Keamanan Informasi

i. Penerapan dan pengelolaan keamanan informasi di Pemerintah Provinsi Lampung harus ditinjau (review) secara mandiri atau oleh pihak independen dalam selang waktu yang direncanakan dan/atau ketika terdapat perubahan yang signifikan.

ii. Unit kerja pengelola TIK bertanggung jawab terkait proses peninjauan terhadap sistem dan teknologi informasi terkait kepatuhan teknis secara berkala.

BAB III
PENUTUP

Dengan disusunnya Kebijakan Teknis Keamanan Informasi Pemerintah Provinsi Lampung diharapkan dapat meningkatkan kesadaran seluruh pegawai di lingkungan Pemerintah Provinsi Lampung bahwa aset data dan informasi sangat penting serta menjadi acuan dalam pengamanan data dan informasi.

GUBERNUR LAMPUNG,

ARINAL DJUNAIDI

LAMPIRAN II : KEPUTUSAN GUBERNUR LAMPUNG
NOMOR : G/ 768 /2023
TANGGAL : 07 - 12 - 2023

SUSUNAN PERSONALIA TIM PELAKSANA MANAJEMEN KEAMANAN INFORMASI PEMERINTAH PROVINSI LAMPUNG

I.	Manajemen Puncak	:	Kepala Dinas Komunikasi Informatika dan Statistik Provinsi Lampung
II.	Wakil Manajemen	:	Sekretaris Dinas Komunikasi Informatika dan Statistik Provinsi Lampung
III.	Koordinator Audit Internal	:	Liswardy, S.H (Sandiman Ahli Madya pada Dinas Komunikasi Informatika dan Statistik Provinsi Lampung)
	Auditor Internal	:	1. Apri Triansah, S.Kom (Pranata Komputer Ahli Pertama Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung) 2. Arif Andi Susanto, S.Kom (Pranata Komputer Ahli Pertama Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung) 3. Iswarawati, S.Komp (Sandiman Ahli Pertama Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung)
IV.	Koordinator Manajemen Resiko	:	Kepala Bidang Teknologi Informasi dan Komunikasi Dinas Komunikasi Informatika dan Statistik Provinsi Lampung
	Tim Manajemen Resiko	:	1. Anny Sri Wahyuniati, S.Sos (Pranata Komputer Ahli Muda Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung) 2. Erny Mariati, S.E, MM (Pranata Komputer Ahli Muda Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung) 3. Martian Ariandi, S.Kom (Pranata Komputer Ahli Muda Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung)
V.	Koordinator Standar dan Kepatuhan	:	Kepala Bidang Tata Kelola Pemerintahan Berbasis Elektronik Dinas Komunikasi Informatika dan Statistik Provinsi Lampung
	Tim Standar dan Kepatuhan	:	1. Yulia, S.Kom, MM (Pranata Komputer Ahli Muda Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung) 2. Eka Yuni Harti, S.E., M.M (Pranata Komputer Ahli Muda Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung)

VI.	Koordinator Pengelolaan Sumber Daya Manusia	:	Kasubbag Umum dan Kepegawaian Dinas Komunikasi Informatika dan Statistik Provinsi Lampung
	Tim Pengelolaan Sumber Daya Manusia	:	1. Yurna Jasmita, S.E., M.M. (Analis Kepegawaian Madya Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung) 2. Yuli Fitriana, S.IP (Perencana Ahli Muda Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung)
VII.	Koordinator Tim Penanggulangan dan Pemulihan Insiden	:	Kepala Bidang Persandian dan Statistik Dinas Komunikasi Informatika dan Statistik Provinsi Lampung
	Tim Penanggulangan dan Pemulihan Insiden	:	1. Arie Korneliyya S.T., M.M., M.T (Sandiman Ahli Muda Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung) 2. Yuli Mandari, S.S.T (Sandiman Ahli Pertama Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung)

GUBERNUR LAMPUNG,

ARINAL DJUNAIDI