MENTERI PERHUBUNGAN
REPUBLIK INDONESIA

KEPUTUSAN MENTERI PERHUBUNGAN REPUBLIK INDONESIA
NOMOR KP 64 TAHUN 2017
TENTANG
KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN KEMENTERIAN PERHUBUNGAN

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI PERHUBUNGAN REPUBLIK INDONESIA,

Menimbang :

a. bahwa dalam rangka mendukung pengelolaan Teknologi Informasi dan Komunikasi (TIK) yang ditetapkan dalam Keputusan Menteri Perhubungan Nomor KP 784 Tahun 2016 tentang Tata Kelola Teknologi Informasi dan Komunikasi (TIK) di Lingkungan Kementerian Perhubungan, perlu adanya kebijakan dan standar keamanan informasi di lingkungan Kementerian Perhubungan;
b. bahwa dalam rangka melindungi kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) aset informasi Kementerian Perhubungan dari berbagai bentuk ancaman keamanan informasi baik dari dalam maupun luar lingkungan Kementerian Perhubungan, perlu melakukan pengaturan pengelolaan keamanan informasi di lingkungan Kementerian Perhubungan;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Menteri Perhubungan tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Perhubungan;

Mengingat : 1. Keputusan Presiden Republik Indonesia Nomor 83/P Tahun 2016 tentang Penggantian Beberapa Menteri Negara Kabinet Kerja Periode 2014-2019;

2. Peraturan Menteri Komunikasi dan Informatika Nomor: 41/PER/MEN.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi Dan Komunikasi Nasional;

3. Peraturan Menteri Perhubungan Nomor PM 189 Tahun 2015 tentang Organisasi dan Tata Kerja Kementerian Perhubungan (Berita Negara Republik Indonesia Tahun 2015 Nomor 1844), sebagaimana telah diubah dengan Peraturan Menteri Perhubungan Nomor PM 86 Tahun 2016 tentang Perubahan atas Peraturan Menteri Perhubungan Nomor 189 Tahun 2015 (Berita Negara Republik Indonesia Tahun 2016 Nomor 1012);

4. Peraturan Menteri Komunikasi dan Informatika Nomor PM 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);

5. Peraturan Menteri Perhubungan Nomor KP 39 Tahun 2009 tentang Rencana Induk Pemanfaatan Teknologi Informasi dan Komunikasi (TIK) di Lingkungan Departemen Perhubungan;

6. Keputusan Menteri Perhubungan Republik Indonesia Nomor 738 Tahun 2014 tentang Kebijakan dan Standar Siklus Pengembangan Sistem Informasi di Lingkungan Kementerian Perhubungan;

7. Keputusan Menteri Perhubungan Republik Indonesia Nomor KP 374 Tahun 2015 tentang Kebijakan Pengelolaan Teknologi Informasi dan Komunikasi di Lingkungan Kementerian Perhubungan;

8. Keputusan Menteri Perhubungan Republik Indonesia Nomor KP 784 Tahun 2016 tentang Tata Kelola Teknologi Informasi dan Komunikasi (TIK) di Lingkungan Kementerian Perhubungan;

Memperhatikan: 1. ISO / IEC 270001:2013 *(Information Technology – Security Techniques – Information Security Management System – Requirements);*
2. ISO / IEC 27002:2013 *(Information technology – Security techniques – Code of practice for information security controls).*

MEMUTUSKAN:

Menetapkan : KEPUTUSAN MENTERI PERHUBUNGAN REPUBLIK INDONESIA TENTANG KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN KEMENTERIAN PERHUBUNGAN

PERTAMA : Menetapkan Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Perhubungan, yang selanjutnya disebut Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan sebagaimana tercantum dalam lampiran yang merupakan bagian tidak terpisahkan dari Keputusan Menteri Perhubungan ini.

KEDUA : Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan sebagaimana dimaksud dalam Diktum PERTAMA digunakan sebagai pedoman dalam melindungi keamanan aset informasi milik Kementerian Perhubungan yang terdiri dari 11 (sebelas) sasaran pengendalian yaitu:

1. Umum;
2. Organisasi Keamanan Informasi;
3. Pengelolaan Aset Informasi;
4. Keamanan Sumber Daya Manusia;
5. Keamanan Fisik dan Lingkungan;
6. Pengelolaan Komunikasi dan Operasional;
7. Akses;
8. Keamanan Informasi dalam Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi;
9. Pengelolaan Gangguan Keamanan Informasi;

10. Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan; dan
11. Kepatuhan.

KETIGA : Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan dikoordinasikan oleh *Chief Information Officer (CIO)* Kementerian Perhubungan, yang sekaligus berperan sebagai *Chief Information Security Officer (CISO)* Kementerian Perhubungan.

KEEMPAT : Dalam melaksanakan tugasnya, CISO Kementerian Perhubungan membentuk Tim Keamanan Informasi Kementerian Perhubungan yang diketuai oleh CISO Kementerian Perhubungan dan beranggotakan para CISO Unit Eselon I, Koordinator Keamanan Informasi Kementerian Perhubungan serta Petugas Keamanan Informasi Kementerian Perhubungan.

KELIMA : *Chief Information Security Officer (CISO)* Unit Eselon I dilaksanakan oleh Sekretaris Inspektorat Jenderal/Para Sekretaris Direktorat Jenderal dan Badan di lingkungan Kementerian Perhubungan.

KEENAM : Dalam melaksanakan tugasnya, CISO Unit Eselon I membentuk Tim Keamanan Informasi Unit Eselon I di lingkungan Unit Eselon I masing-masing.

KETUJUH : Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan dikaji ulang secara berkala untuk menjamin efektivitas pelaksanaannya.

KEDELAPAN : Ketentuan lebih lanjut mengenai Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan ditetapkan oleh:

1. CISO Kementerian Perhubungan untuk tingkat Kementerian Perhubungan;
2. CISO Unit Eselon I untuk tingkat Unit Eselon I.

KESEMBILAN : Ketentuan pelaksanaan yang berkaitan dengan keamanan informasi yang sudah berlaku di Unit Eselon I, sepanjang tidak bertentangan dengan Keputusan Menteri Perhubungan ini dinyatakan tetap berlaku.

KESEPULUH : Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan sebagaimana dimaksud dalam Diktum PERTAMA dilaksanakan secara bertahap dalam jangka waktu paling lama 3 (tiga) tahun sejak ditetapkannya Keputusan Menteri Perhubungan ini.

KESEBELAS : Keputusan Menteri Perhubungan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 11 Januari 2017

MENTERI PERHUBUNGAN
REPUBLIK INDONESIA,

ttd

BUDI KARYA SUMADI

Salinan Keputusan Menteri Perhubungan ini disampaikan kepada:

1. Sekretaris Jenderal, Inspektur Jenderal, para Direktur Jenderal dan Kepala Badan di Lingkungan Kementerian Perhubungan;
2. Staf Ahli Menteri bidang Teknologi, Energi, dan Lingkungan Perhubungan;
3. Para Kepala Biro/Pusat di Lingkungan Sekretaris Jenderal Kementerian Perhubungan;
4. Sekretaris Inspektorat Jenderal/ParaSekretaris Direktorat Jenderal dan Badan di lingkungan Kementerian Perhubungan;
5. Pejabat Unit TIK Eselon I di lingkungan Kementerian Perhubungan.

Salinan sesuai dengan aslinya

KEPALA BIRO HUKUM

SRI LESTARI RAHAYU
Pembina Utama Muda (IV/c)
NIP. 19620620 198903 2 001

LAMPIRAN
KEPUTUSAN MENTERI PERHUBUNGAN
NOMOR
TENTANG KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN KEMENTERIAN PERHUBUNGAN

KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN KEMENTERIAN PERHUBUNGAN

I. PENGERTIAN

Dalam Keputusan ini yang dimaksud dengan :

1. Akun adalah identifikasi pengguna yang diberikan oleh unit TIK, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem TIK.
2. Akun khusus adalah akun yang diberikan oleh unit TIK sesuai kebutuhan tetapi tidak terbatas pada pengelola TIK sesuai kebutuhan tetapi tidak terbatas pada pengelolaan TIK (baik berupa aplikasi atau sistem), dan kelompok kerja (baik berupa acara kedinasan, tim atau unit kerja).
3. Aset fisik adalah jenis aset yang dimiliki wujud fisik, misalnya perangkat komputer, perangkat jaringan dan komunikasi, removable media dan perangkat pendukung lainnya.
4. Aset tak berwujud adalah jenis aset yang tidak memiliki wujud fisik, misalnya pengetahuan, pengalahan, keahlian, citra dan reputasi. Aset ini mempunyai umur lebih dari satu tahun (aset tidak lancar) dan dapat diamortisasi selama periode pemanfaatannya, yang biasanya tidak lebih dari empat puluh tahun.
5. Conduit adalah sebuah tabung atau saluran untuk melindungi kabel yang biasanya terbuat dari baja.
6. Daftar inventaris aset informasi adalah kumpulan informasi yang memuat bentuk pemilik, lokasi, retensi dan hal-hal yang terkait dengan asset informasi.
7. Data adalah catatan atas kumpulan fakta yang mempunyai arti baik secara kualitatif maupun kuantitatif.

8. *Denial of Service* adalah suatu kondisi dimana sistem tidak dapat memberikan layanan secara normal, yang disebabkan oleh suatu proses yang tidak terkendali baik dari dalam maupun dari luar sistem.
9. Direktori adalah hirarki atau *tree structure.*
10. Dokumen SMKI Kementerian Perhubungan adalah dokumen terkait pelaksanaan SMKI yang meliputi antara lain dokumen kebijakan, standar, prosedur dan catatan penerapan SMKI.
11. Informasi adalah hasil pemrosesan, manipulasi dan pengorganisasian data yang dapat disajikan sebagai pengetahuan.
    Catatan: dalam penggunaannya data dapat berupa informasi yang menjadi data baru, sebaliknya informasi dapat berfungsi sebagai data untuk menghasilkan informasi baru.
12. *Fallback* adalah suatu tindakan pembalikan/ menarik diri dari posisi awal.
13. Fasilitas adalah sarana untuk melancarkan pelaksanaan fungsi atau mempermudah sesuatu.
14. Fasilitas utama adalah sarana utama gedung atau bangunan seperti pusat control listrik, CCTV.
15. *Fault logging* adalah pencatatan permasalahan sistem informasi.
16. Hak akses khusus adalah akses terhadap sistem informasi sensitif, termasuk didalamnya dan tidak terbatas pada sistem operasi, perangkat penyimpanan (*storage devices*), *file server*, dan aplikasi-aplikasi sensitif, hanya diberikan kepada pengguna yang membutuhkan dan pemakaiannya terbatas dan dikontrol.
17. *Hash totals* adalah nilai pemeriksaaan kesalahan yang diturunkan dari penambahan satu himpunan bilangan yang diambil dari data (tidak harus berupa data *numeric*) yang diproses atau dimanipulasi dengan cara tertentu.
18. Jejak audit (*audit trails*) adalah urutan kronologis catatan audit yang berkaitan dengan pelaksanaan suatu kegiatan.
19. Kata sandi adalah serangkaian kode yang dibuat Pengguna, bersifat rahasia dan pribadi yang digunakan bersamaan dengan Akun Pengguna.
20. Keamanan informasi adalah perlindungan asset informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan dan ketersediaan aset informasi.

21. Komunitas keamanan informasi adalah kelompok/ komunitas yang memiliki pengetahuan/ keahlian khusus dalam bidang keamanan informasi atau yang relevan dengan keamanan informasi, seperti : Indonesia *security Incident Response Team on Internet and Infrastructure*/ ID-SIRTIL Unit *Cybercrime* POLRI, ISC2 ISACA).
22. Koneksi eksternal (*remote access*) adalah suatu akses jaringan komunikasi dari luar organisasi kedalam organisasi.
23. Kriptografi adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal untuk meningkatkan keamanan informasi. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi.
24. *Malicious Code* adalah semua macam program yang membahayakan termasuk makro atau script yang dapat dieksekusi dan dibuat dengan tujuan untuk merusak sistem komputer.
25. Master disk adalah media yang digunakan sebagai sumber dalam melakukan instalasi perangkat lunak.
26. *Mobile Computing* adalah penggunaan perangkat komputasi yang dapat dipindah (portable) misalnya notebook, tablet dan smartphone untuk melakukan akses, pengolahan data dan penyimpanan.
27. Penanggung jawab pengendalian dokumen adalah pihak yang memiliki kewenangan dan bertanggung jawab dalam proses pengendalian dokumen SMKI.
28. Pengguna adalah pegawai Kementerian Perhubungan dan atau pihak ketiga serta tidak terbatas pada pengelola TIK dan kelompok kerja yang diberikan hak akses sistem TIK di Kementerian Perhubungan.
29. Pemilik aset informasi adalah unit kerja yang memiliki kewenangan terhadap aset informasi.
30. Pencatatan waktu (*timestamp*) adalah catatan waktu dalam tanggal dan/atau format waktu tertentu saat suatu aktivitas/transaksi terjadi. Format ini biasanya disajikan dalam bentuk format yang konsisten, yang memungkinkan untuk membandingkan dua aktivitas/transaksi yang berbeda berdasarkan waktu.
31. Perangkat jaringan adalah peralatan jaringan komunikasi data seperti modem, hub, *switch, router,* dan lain-lain.
32. Perangkat lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya.

33. Perangkat pendukung adalah peralatan pendukung untuk menjamin beroperasinya perangkat keras dan perangkat jaringan serta untuk melindungi dari kerusakan. Contoh: perangkat pendukung adalah *Uninterruptible Power Supply* (UPS), pembangkit tenaga listrik/generator, antena komunikasi, dan lain-lain.
34. Perangkat pengolah informasi adalah setiap sistem pengolahan informasi, layanan atau infrastruktur. Contoh perangkat pengolah informasi adalah komputer, faksimili, telepon, mesin fotocopy, *Scanner* dan lain-lain.
35. Penjamin escrow adalah perjanjian dengan pihak ketiga untuk memastikan apabila pihak ketiga tersebut bangkrut (mengalami *failure*), maka Kementerian Perhubungan berhak untuk mendapatkan kode program (*source code*).
36. Perjanjian kerahasiaan adalah perikatan antara para pihak yang mencantumkanbahan rahasia, pengetahuan atau informasi yang mana pihak-pihak ingin berbagi satu sama lain untuk tujuan tertentu tetapi ingin membatasi akses dengan pihak lain.
37. Petugas Pelaksana Pengelolaan Proses Kelangsungan kegiatan adalah pegawai yang ditunjuk oleh Pimpinan unit eselon I untuk mengelola proses kelangsungan pada saat keadaan darurat.
38. Pihak berwenang adalah pihak yang mempunyai kewenangan terkait suatu hal, seperti : Kepolisian, Instansi Pemadam Kebakaran, dan penyedia Jasa Telekomunikasi/ Internet.
39. Pihak ketiga adalah semua unsur diluar pengguna unit TIK Kementerian Perhubungan yang bukan bagian dari Kementerian Perhubungan, misal mitra kerja Kementerian Perhubungan seperti : Konsultan, penyedia jasa komunikasi, pemasok dan pemelihara perangkat pengolah informasi, dan Kementerian/ Lembaga lain.
40. Proses Pendukung (*support process*) adalah proses-proses penunjang yang mendukung suatu proses utama yang terkait. Contoh : proses pendukung dalam pengembangan (*development*) adalah proses pengujian perangkat lunak, proses perubahan perangkat lunak.
41. Rencana Kontijensi adalah suatu rencana ke depan pada keadaan yang tidak menentu dengan skenario, tujuan, teknik, manajemen, pelaksanaan serta sistem penanggulangannya telah ditentukan secara bersama untuk mencegah dan mengatasi keadaan darurat.

42. *Rollback* adalah sebuah mekanisme yang digunakan untuk mengembalikan sistem ke kondisi semula sebelum perubahan diimplementasikan. Mekanisme ini biasanya terdapat pada sistem basis data.
43. *Routing* adalah sebuah mekanisme yang digumakan untuk mengarahkan dan menentukan rute/ jalur yang akan dilewati paket dari satu perangkat ke perangkat yang berada di jaringan lain.
44. Sanitasi adalah proses penghilangan informasi yang disimpan secara permanen dengan menggunakan medan magnet atau perusahaan fisik.
45. Sistem Manajemen Keamanan Informasi (SMKI) adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penanggung jawab proses dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola dan meningkatkan keamanan informasi.
46. Sistem informasi adalah serangkaian perangkat keras, perangkat lunak, sumber daya manusia, serta prosedur dan atau aturan yang diorganisasi secara terpadu untuk mengolah data menjadi informasi yang berguna untuk mencapai suatu tujuan.
47. Sistem TIK adalah suatu sistem operasi, sistem surat elektronik,sistem aplikasi, sistem basis data, sistem jaringan intranet/ internet dan sebagainya.
48. Subnet (kependekatan dari sub network) adalah pengelompokan secara logis dari perangkat jaringan yang terhubung.
49. System administrator adalah akun khusus untuk mengelola sistem informasi.
50. System utilities adalah sebuah sistem perangkat lunak yang melakukan suatu tugas/fungsi yang sangat spesifik, biasanya disediakan oleh sistem operasi dan berkaitan dengan pengelolaan sumber daya sistem (system resources), seperti memory, disk, printer, dan sebagainya.
51. Teleworking adalah penggunaan teknologi telekomunikasi untuk memungkinkan pegawai bekerja di suatu lokasi yang berada diluar kantor untuk mengakses jaringan internal kantor.

II. PENGENDALIAN UMUM

A. TUJUAN

Kebijakan dan Standar Sistem Manajemen Keamanan Informasi (SMKI) ini digunakan sebagai pedoman dalam rangka melindungi aset informasi Kementerian Perhubungan dari berbagai bentuk ancaman baik dari dalam maupun luar lingkungan Kementerian perhubungan, yang dilakukan secara sengaja maupun tidak sengaja. Pengamanan dan perlindungan ini diberikan untuk menjamin kerahasiaan *(confidentiality)*, keutuhan *(integrity)*, dan ketersediaan *(availability)* aset informasi agar selalu terjaga dan terpelihara dengan baik.

B. RUANG LINGKUP

1. Catatan Penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan;
2. Penyusunan Dokumen Pendukung;
3. Pengendalian Dokumen.

C. KEBIJAKAN

1. Catatan Penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan.

   Kebijakan ini berlaku untuk pengelolaan pengamanan seluruh aset informasi Kementerian Perhubungan dan dilaksanakan oleh seluruh unit kerja, pegawai Kementerian Perhubungan baik sebagai pengguna maupun pengelola Teknologi Informasi dan Komunikasi (TIK), dan pihak ketiga di lingkungan Kementerian Perhubungan.
2. Penyusunan Dokumen Pendukung.

   Aset informasi Kementerian Perhubungan adalah asset dalam bentuk:

   a. Data / dokumen, meliputi : data transportasi, data kepegawaian, dokumen penawaran dan kontrak, dokumen perjanjian kerahasiaan, kebijakan Kementerian, hasil penelitian, bahan peneltian, prosedur operasional, rencana kelangsungan kegiatan (*business continuity plan),* dan hasil audit serta data informasi penting lainnya;
   b. Perangkat lunak, meliputi : perangkat lunak aplikasi, perangkat lunak sistem, dan perangkat bantu pengembangan sistem;

c. Aset fisik, meliputi: perangkat komputer, perangkat jaringan dan komunikasi, *removable* media, dan perangkat pendukung; dan
d. Aset tak berwujud (*intangible*), meliputi : pengetahuan, pengalaman, keahlian, citra dan reputasi.

3. Pengendalian Dokumen.
   a. Setiap pimpinan Unit eselon I bertanggung jawab mengatur penerapan Kebijakan dan Standar SMKI di lingkungan Kementerian Perhubungan yang ditetapkan dalam Keputusan Menteri Perhubungan ini di lingkungan unit eselon I masing-masing.
   b. Unit eselon I harus menerapkan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan yang ditetapkan dalam Keputusan Menteri Perhubungan ini di Lingkungan unit eselon I masing-masing.
   c. Pimpinan unit TIK Pusat dan setiap Pimpinan unitTIK eselon I bertanggung jawab mengatur pelaksanaan pengamanan dan perlindungan aset informasi di lingkungan unit eselon I masing-masing dengan mengacu pada Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan yang ditetapkan dalam Keputusan Menteri Perhubungan ini.
   d. Unit TIK pusat dan Unit TIK eselon I bertanggung jawab melaksanakan pengamanan aset informasi di lingkungan unit eselon I masing-masing dengan mengacu pada Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan yang ditetapkan dalam Keputusan Menteri Perhubungan ini.
   e. Unit TIK pusat dan Unit TIK eselon I bertanggung jawab meningkatkan pengetahuan, keterampilan dan kepedulian terhadap keamanan informasi pada seluruh pengguna di lingkungan unit eselon I masing-masing.
   f. Unit TIK pusat dan Unit TIK eselon I menerapkan dan mengembangan manajemen risiko dalam rangka pelaksanaan pengamanan dan perlindungan aset informasi dengan mengikuti ketentuan Penerapan Manajemen Risiko di Lingkungan Kementerian Perhubungan.
   g. Unit TIK pusat dan Unit TIK eselon I tidak bertanggung jawab atas kerugian atau kerusakan data maupun perangkat lunak

milik pihak ketiga yang diakibatkan dari upaya melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi.

h. Unit TIK pusat dan Unit TIK eselon I melakukan evaluasi terhadap pelaksanaan SMKI secara berkala untuk menjamin efektivitas dan meningkatkan keamanan informasi.

i. Inspektorat Jenderal Kementerian Perhubungan melakukan audit internal SMKI di lingkungan Kementerian Perhubungan untuk memastikan pengendalian, proses dan prosedur SMKI dilaksanakan secara efektif sesuai dengan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan dan dipelihara dengan baik.

j. Unit TIK pusat dan Unit TIK eselon I menggunakan laporan audit internal SMKI untuk meninjau efektivitas penerapan SMKI dan melakukan tindak lanjut terhadap temuan auditor.

D. STANDAR

1. Catatan Penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan.

   a. Unit TIK pusat dan Unit TIK eselon I harus menggunakan catatan penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan untuk mengukur kepatuhan dan efektivitas penerapan SMKI.

   b. Catatan penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan harus meliputi:

      1) Formulir-formulir sesuai prosedur operasional yang dijalankan;
      2) Catatan gangguan keamanan informasi;
      3) Catatan dari sistem;
      4) Catatan pengunjung di *secure areas*;
      5) Kontrak dan perjanjian layanan;
      6) Perjanjian kerahasiaan (*confidentiality agreements*); dan
      7) Laporan audit.

2. Penyusunan Dokumen Pendukung

   Penyusunan dokumen pendukung kebijakan keamanan informasi harus memuat:

   a. Tujuan dan ruang lingkup dokumen pendukung kebijakan keamanan informasi;

b. Kerangka kerja setiap tujuan / sasaran pengendalian keamanan informasi;
c. Metodologi penilaian risiko (*risk assessment);*
d. Penjelasan singkat mengenai standar, prosedur dan kepatuhan termasuk persyaratan peraturan yang harus dipenuhi, pengelolaan kelangsungan kegiatan, konsekuensi apabila terjadi pelanggaran;
e. Tanggung jawab dari setiap bagian terkait; dan
f. Dokumen referensi yang digunakan dalam menyusun dokumen pendukung kebijakan keamanan informasi.

3. Pengendalian Dokumen
   a. Unit TIK pusat dan Unit TIK eselon I harus mengendalikan dokumen SMKI Kementerian Perhubungan untuk menjaga kemutakhiran dokumen, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan, dan mencegah akses oleh pihak yang tidak berwenang.
   b. Unit TIK pusat dan Unit TIK eselon I harus menempatkan dokumen SMKI Kementerian Perhubungan di semua area operasional sehingga mudah diakses oleh pengguna di unit kerja masing-masing sesuai peruntukannya.

III. PENGENDALIAN ORGANISASI KEAMANAN INFORMASI

A. TUJUAN

Bab ini bertujuan memberikan pedoman dalam membentuk organisasi fungsional keamanan informasi yang bertanggung jawab untuk mengelola keamanan informasi dan perangkat pengolah informasi di lingkungan Kementerian Perhubungan termasuk hubungan dengan pihak luar.

B. RUANG LINGKUP

Kebijakan dan standar organisasi keamanan informasi meliputi:

1. Struktur Tim Keamanan Informasi di Kementerian Perhubungan dan unit eselon I;
2. Perjanjian kerahasiaan; dan
3. Hubungan dengan pihak berwenang, komunitas keamanan informasi, dan pihak ketiga.

C. KEBIJAKAN

1. Struktur Tim Keamanan Informasi Kementerian Perhubungan

   Struktur Tim Keamanan Informasi Kementerian Perhubungan berikut tanggung jawab dan wewenangnya diuraikan dalam standar organisasi keamanan informasi.

2. Struktur Tim Keamanan Informasi Unit Kerja Eselon I

   Struktur Tim Keamanan Informasi Unit Kerja Eselon I berikut tanggung jawab dan wewenangnya diuraikan dalam standar organisasi keamanan informasi.

3. Tanggung jawab dan wewenang Tim Keamanan Informasi Kementerian Perhubungan dapat dipetakan dalam jabatan struktural dan/atau diperankan oleh Pejabat struktural dan/atau Pejabat fungsional.

4. Perjanjian Kerahasiaan

   Unit kerja eselon I mengidentifikasi dan mengkaji secara berkala persyaratan untuk menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen perjanjian kerahasiaan.

5. Hubungan dengan Pihak Berwenang

   Unit kerja eselon I mengidentifikasi dan menjalin kerjasama dengan pihak-pihak berwenang di luar Kementerian Perhubungan yang terkait dengan keamanan informasi.

6. Hubungan dengan Komunitas Keamanan Informasi

   Unit TIK pusat dan Unit TIK eselon I menjalin kerjasama dengan komunitas keamanan informasi di luar Kementerian Perhubungan melalui pelatihan, seminar, atau forum lain yang relevan dengan keamanan informasi.

7. Hubungan dengan Pihak Ketiga

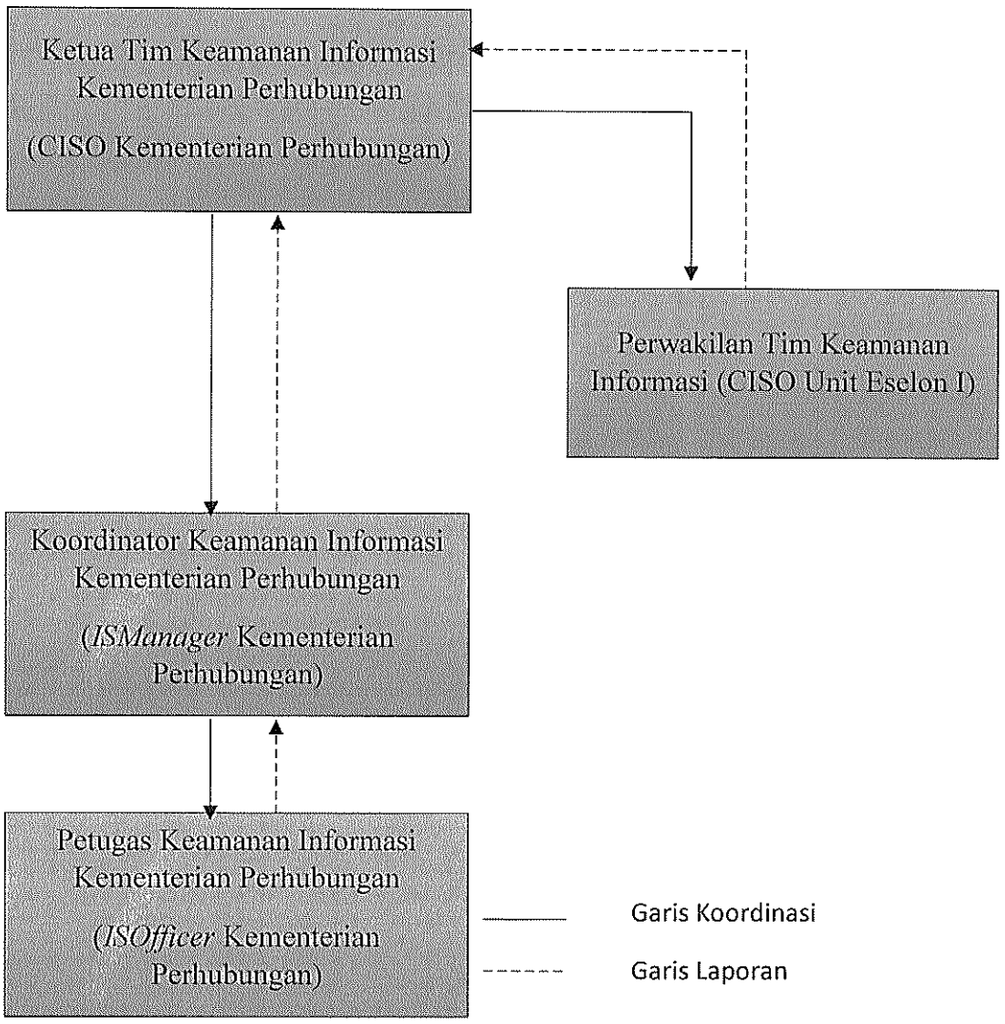
   Unit TIK pusat dan Unit TIK eselon I harus menerapkan pengendalian keamanan informasi berdasarkan hasil penilaian risiko untuk mencegah atau mengurangi dampak risiko terkait dengan pemberian akses kepada pihak ketiga

D. STANDAR

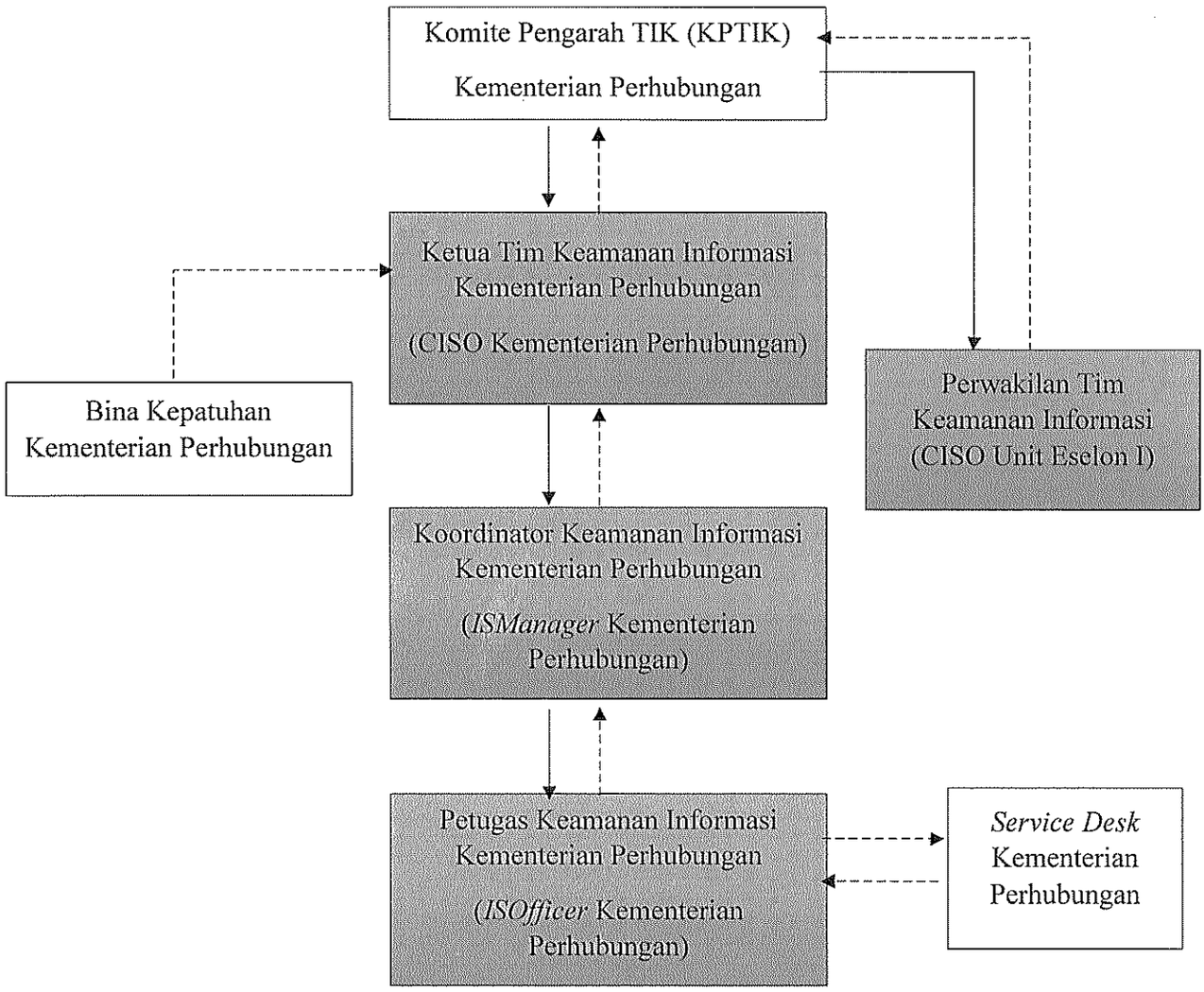
1. Tim Keamanan Informasi

a. Struktur Tim Keamanan Informasi Kementerian Perhubungan

Bagan 1. Struktur Tim Keamanan Informasi Kementerian Perhubungan

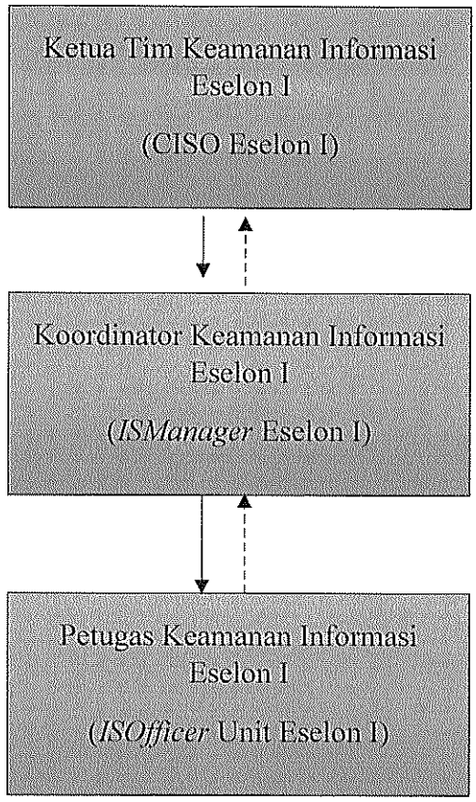


Bagan 2. Hubungan Kerja Tim Keamanan Informasi Kementerian Perhubungan dengan Unit Kerja Terkait

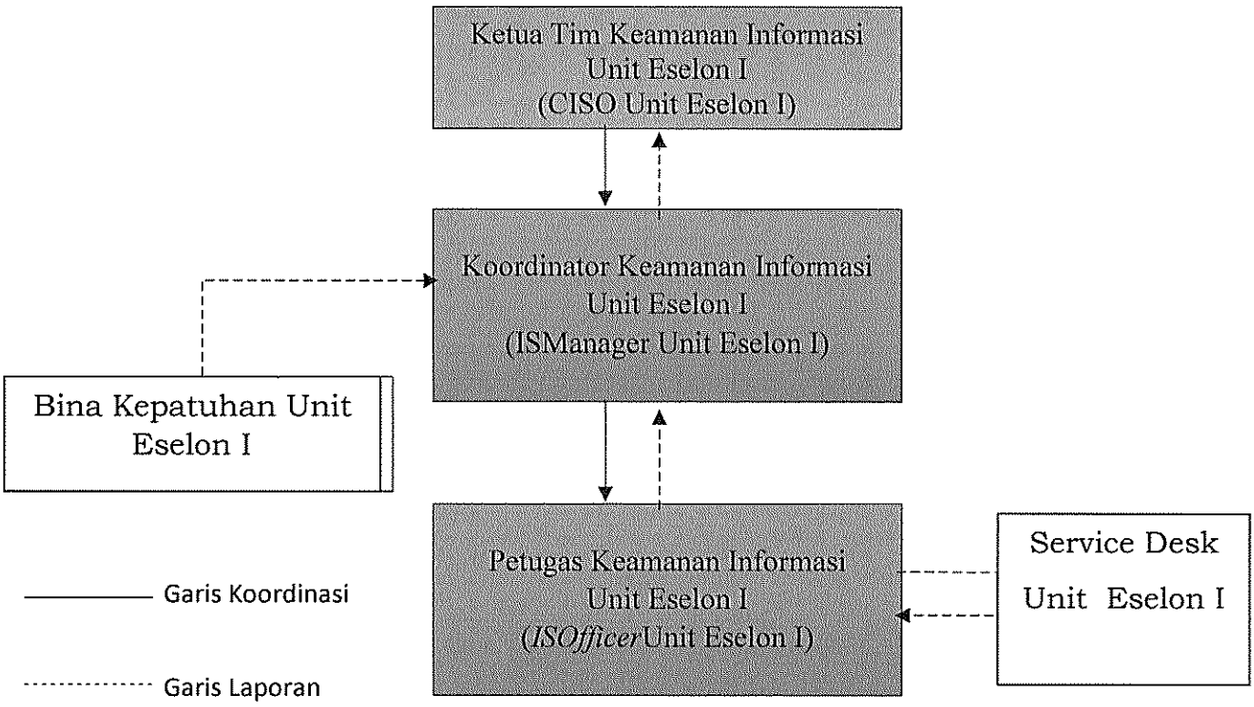


b. Struktur Tim Keamanan Informasi Unit Eselon I

Bagan 3. Struktur Tim Keamanan Informasi Unit Eselon I



Bagan 4. Hubungan Kerja Tim Keamanan Informasi Unit Eselon I dengan Unit Kerja Terkait



c. Tanggung Jawab Tim Keamanan Informasi Kementerian Perhubungan

1) Ketua Tim Keamanan Informasi Kementerian Perhubungan (*Chief Information Security Officer*/CISO Kementerian Perhubungan) bertanggung jawab untuk :

a) Mengkoordinasikan perumusan dan penyempurnaan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan;

b) Memelihara dan mengendalikan penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan di seluruh area yang menjadi tujuan/ sasaran pengendalian;

c) Menetapkan target keamanan informasi setiap tahunnya dan menyusun rencana kerja untuk Kementerian Perhubungan, masing-masing unit eselon I, maupun yang bersifat lintas unit;

d) Memastikan efektifitas dan konsistensi penerapan kebijakan dan standar SMKI di Lingkungan Kementerian Perhubungan dan mengukur kinerja keseluruhan; dan

e) Melaporkan kinerja penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan dan pencapaian target kepada Komite Pengarah TIK Kementerian Perhubungan (*ICT Steering Commitee*);

2) Koordinator Keamanan Informasi Kementerian Perhubungan (*Information Security Manager*/ISManager Kementerian Perhubungan) bertanggung jawab untuk :

a) Memastikan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan diterapkan secara efektif;

b) Memastikan langkah-langkah perbaikan sudah dilakukan berdasarkan saran dan rekomendasi yang diberikan dalam pelaksanaan evaluasi dan/atau audit penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan;

c) Memastikan peningkatan kesadaran, kepedualian dan kepatuhan seluruh pegawai terhadap Kebijakan dan Standar SMKI di Lingkungan Kementeiran Perhubungan;

d) Melaporkan kinerja penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan sesuai ruang lingkup tanggung jawabnya kepada Ketua Tim Keamanan Informasi Kementerian Perhubungan yang akan digunakan sebagai dasar peningkatan keamanan informasi;

e) Mengkoordinasikan penanganan gangguan keamanan informasi di tingkat Kementerian Perhubungan; dan

f) Memastikan terlaksananya audit internal terhadap penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan pada masing-masing unit eselon I di lingkungan Kementerian Perhubungan paling sedikit 1 (satu) kali dalam 3 (tiga) tahun.

3) Petugas Keamanan Informasi Kementerian Perhubungan (*Information Security Officer/ ISOfficer* Kementerian Perhubungan) bertanggung jawab untuk :

a) Melaksanakan dan mengawasi penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan;

b) Memberi masukan peningkatan terhadap Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan;
c) Mendefinisikan kebutuhan, merekomendasikan, dan mengupayakan penyelenggaraan pendidikan dan pelatihan keamanan informasi bagi pegawai;
d) Memantau, mencatat, dan menguraikan secara jelas gangguan keamanan informasi yang diketahui atau laporan yang diterima, dan menindaklanjuti laporan tersebut sesuai prosedur pelaporan gangguan keamanan informasi; dan
e) Memberi panduan dan/atau bantuan penyelesaian masalah-masalah keamanan informasi.

4) Perwakilan Tim Keamanan Informasi terdiri dari para Ketua Tim Keamanan Informasi Unit Eselon I (CISO Unit Eselon I), dan bertanggung jawab untuk :
a) Melakukan koordinasi penerapan Kebijakan dan Standar SMKI di lingkungan Kementerian Perhubungan; dan
b) Melakukan evaluasi dampak gangguan keamanan informasi untuk dilaporkan kepada Ketua Tim Keamanan Informasi Kementerian Perhubungan, dan menindaklanjutinya.

d. Tanggung jawab Tim Keamanan Informasi Unit Eselon I
1) Ketua Tim Keamanan Informasi Unit Eselon I (CISO Unit Eselon I) bertanggung jawab untuk :
a) Memelihara dan mengendalikan penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan di seluruh area yang menjadi tujuan/sasaran pengendalian pada unit eselon I masing-masing;
b) Menetapkan target keamanan informasi setiap tahunnya dan menyusun rencana kerja pada unit eselon I masing-masing;
c) Mengukur efektifitas dan konsistensi penerapan kebijakan dan standar SMKI di Lingkungan Kementerian Perhubungan pada unit eselon I masing-masing; dan
d) Memberi masukan untuk meningkatkan penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan.

b) Memberi masukan peningkatan terhadap Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan;
c) Mendefinisikan kebutuhan, merekomendasikan, dan mengupayakan penyelenggaraan pendidikan dan pelatihan keamanan informasi bagi pegawai;
d) Memantau, mencatat, dan menguraikan secara jelas gangguan keamanan informasi yang diketahui atau laporan yang diterima, dan menindaklanjuti laporan tersebut sesuai prosedur pelaporan gangguan keamanan informasi; dan
e) Memberi panduan dan/atau bantuan penyelesaian masalah-masalah keamanan informasi.

4) Perwakilan Tim Keamanan Informasi terdiri dari para Ketua Tim Keamanan Informasi Unit Eselon I (CISO Unit Eselon I), dan bertanggung jawab untuk :
a) Melakukan koordinasi penerapan Kebijakan dan Standar SMKI di lingkungan Kementerian Perhubungan; dan
b) Melakukan evaluasi dampak gangguan keamanan informasi untuk dilaporkan kepada Ketua Tim Keamanan Informasi Kementerian Perhubungan, dan menindaklanjutinya.

d. Tanggung jawab Tim Keamanan Informasi Unit Eselon I
1) Ketua Tim Keamanan Informasi Unit Eselon I (CISO Unit Eselon I) bertanggung jawab untuk :
a) Memelihara dan mengendalikan penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan di seluruh area yang menjadi tujuan/sasaran pengendalian pada unit eselon I masing-masing;
b) Menetapkan target keamanan informasi setiap tahunnya dan menyusun rencana kerja pada unit eselon I masing-masing;
c) Mengukur efektifitas dan konsistensi penerapan kebijakan dan standar SMKI di Lingkungan Kementerian Perhubungan pada unit eselon I masing-masing; dan
d) Memberi masukan untuk meningkatkan penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan.

2) Koordinator Keamanan Informasi Unit Eselon I bertanggung jawab untuk:
   a) Memastikan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubugan diterapkan secara efektif pada unit eselon I masing-masing;
   b) Memastikan langkah-langkah perbaikan sudah dilakukan berdasarkan saran dan reomendasi yang diberikan dalam pelaksanaan evaluasi dan/atau audit penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan pada unit eselon I masing-masing;
   c) Memastikan peningkatan kesadaran, kepedulian, dan kepatuhan seluruh pegawai terhadap Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan pada unit eselon I masing-masing;
   d) Melaporkan kinerja penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan pada unit eselon I masing-masing seuai ruang lingkup tanggung jawabnya kepada Ketua Tim Keamanan Informasi Unit Eselon I yang akan digunakan sebagai dasar peningkatan keamanan Informasi;
   e) Mengkoordinasikan penanganan gangguan keamanan informasi pada unit eselon I masing-masing;
   f) Memastikan evaluasi terhadap Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan pada unit eselon I masing-masing terlaksana secara efektif dan efisien; dan
   g) Memastikan terlaksananya evaluasi dan/atau audit internal terhadap penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan pada unit eselon I masing-masing paling sedikit 1 (satu) kali dalam 2 (dua) tahun.
3) Petugas Keamanan Informasi Unit Eselon I bertanggung jawab untuk :
   a) Melaksanakan dan mengawasi penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan pada unit eselon I masing-masing;

b) Memberi masukan untuk meningkatkan penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan pada unit eselon I masing-masing melalui Ketua Tim Keamanan Informasi Unit Eselon I;

c) Mendefinisikan kebutuhan, merekomendasikan, dan mengupayakan penyelenggaraan pendidikan dan pelatihan keamanan informasi bagi pegawai pada unit eselon I masing-masing;

d) Memantau, mencatat, menguraikan dan menindaklanjuti gangguan keamanan informasi yang diketahui dan dilaporkan sesuai prosedur pelaporan gangguan keamanan informasi pada unit eselon I masing-masing; dan

e) Memberikan panduan dan/atau bantuan penyelesaian masalah-masalah keamanan informasi pada unit eselon I masing-masing.

2. Perjanjian Kerahasiaan

Perjanjian kerahasiaan harus memuat unsur-unsur sebagai berikut :

a. Definisi dari informasi yang akan dilindungi;
b. Durasi yang diharapkan dari sebuah perjanjian kerahasiaan;
c. Tanggung jawab dan tidakan penanda-tangan untuk menghindari pengungkapan informasi secara tidak sah;
d. Perlindungan kepemilikan informasi, rahasia organisasi dan kekayaan intelektual;
e. Izin menggunakan informasi rahasia, dan hak-hak penanda-tangan untuk menggunakan informasi;
f. Hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia;
g. Proses untuk pemberitahuan dan pelaporan dari penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan informasi;
h. Tindakan yang diperlukan pada saat sebuah perjanjian kerahasiaan diakhiri;
i. Syarat-syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian; dan
j. Tindakan yang diambil apabila terjadi pelanggaran terhadap perjanjian ini.

IV. PENGENDALIAN PENGELOLAAN ASET INFORMASI

A. TUJUAN

Pengelolaan aset informasi bertujuan memberikan pedoman dalam mengelola aset informasi di lingkungan Kementerian Perhubungan untuk melindungi dan menjamin keamanan aset informasi.

B. RUANG LINGKUP

Kebijakan dan standar pengelolaan Aset Informasi ini meliputi :

1. Tanggung jawab setiap unit eselon 1 terhadap aset informasi; dan
2. Pengklasifikasian aset informasi

C. KEBIJAKAN

1. Tanggung Jawab terhadap Aset Informasi
   a. Unit TIK pusat dan unit TIK eselon I mengidentifikasi aset informasi dan mendokumentasikannya dalam daftar inventaris aset informasi. Daftar inventaris aset informasi dipelihara dan dikelola perubahannya oleh Penanggung Jawab Pengendalian Dokumen.
   b. Pimpinan Unit Eselon I menetapkan pemilik aset informasi di setiap unit eselon I.
   c. Pemimpin Unit Eselon I menetapkan pemilik aset informnasi yang terkait dengan perangkat pengolah informasi.
   d. Pemilik Aset Informasi menetapkan aturan penggunaan aset informasi.
2. Klasifikasi Aset Informasi
   a. Aset informasi diklasifikasikan sesuai tingkat kerahasiaan, nilai, tingkat kritikalitas, serta aspek hukumnya.
   b. Ketentuan rinci klasifikasi aset informasi diuraikan dalam standar pengelolaan aset informasi.
   c. Pemberiaan label klasifikasi aset informasi harus dilakukan secara konsisten terhadap seluruh aset informasi.

D. STANDAR

1. Tanggung Jawab Pengelolaan Aset Informasi
   a. Pemilik Aset Informasi menetapkan dan mengkaji secara berkala klasifikasi aset informasi dan jenis perlindungan keamanannya.

b. Pemilik Aset Informasi menetapkan pihak yang berwenang untuk mengakses aset informasi.

2. Dalam pengelolaan aset informasi Kementerian Perhubungan, aset informasi diklasifikasikan seperti pada tabel berikut:

KLASIFIKASI ASET	KETERANGAN
SANGAT RAHASIA *(STRICTLY CONFIDENTIAL)*	Aset informasi Kementerian Perhubungan yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menyebabkan kerugian yang berdampak pada ketahanan dan keutuhan nasional.
RAHASIA *(CONFIDENTIAL)*	Aset informasi Kementerian Perhubungan yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak Perhubungan atau menganggu citra dan reputasi Kementerian Perhubungan dan/atau yang menurut peraturan perundang-undangan dinyatakan rahasia.
TERBATAS *(INTERNAL USE ONLY)*	Aset informasi Kementerian Perhubungan yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menganggu kelancaran kegiatan Kementerian Perhubungan tetapi tidak akan mengganggu citra dan reputasi Kementerian Perhubungan.
PUBLIK	Aset informasi yang secara sengaja disediakan Kementerian Perhubungan untuk dapat diketahui masyarakat umum.

Tabel Klasifikasi Aset Informasi

V. PENGENDALIAN KEAMANAN SUMBER DAYA MANUSIA

A. TUJUAN

Kemananan sumber daya manusia bertujuan memastikan bahwa seluruh pegawai dan pihak ketiga di lingkungan Kementerian Perhubungan memahami tanggung jawabnya masing-masing, sadar atas ancaman keamanan informasi, serta mengetahui proses terkait keamanan informasi keamanan informasi sebelum, selama, dan setelah bertugas.

B. RUANG LINGKUP

Kebijakan dan standar ini mencakup peran dan tanggung jawab seluruh pegawai dan pihak ketiga di lingkungan Kementerian Perhubungan dalam hal keamanan sumber daya manusia yang harus dipahami dan dilaksanakan. Peran dan tanggung jawab pegawai juga mengacu pada peraturan perundang-undangan lainnya yang berlaku.

C. KEBIJAKAN

Keamanan Sumber Daya Manusia meliputi :

1. Seluruh pegawai bertanggung jawab untuk menjaga keamanan informasi Kementerian Perhubungan sesuai dengan tugas dan fungsinya.
2. Pihak ketiga harus menyetujui dan menandatangani syarat dan perjanjian untuk menjaga keamanan informasi Kementerian Perhubungan.
3. Peran dan tanggung jawab pegawai dan pihak ketiga terhadap keamanan informasi didefinisikan, didokumentasikan, dan dikomunikasikan kepada yang bersangkutan.
4. Unit eselon I akan melakukan pemeriksaan data pribadi yang diberikan oleh pegawai baru dan pihak ketiga sesuai dengan peraturan dan perundang-undangan yang berlaku.
5. Seluruh pegawai harus mendapatkan pendidikan, pelatihan dan sosialisasi keamanan informasi secara berkala sesuai tingkat tanggung jawabnya.
6. Pihak ketiga, jika diperlukan, mendapatkan sosialisasi untuk meningkatkan kepeduliaan terhadap keamanan informasi.

7. Seluruh pegawai dan pihak ketiga yang melanggar Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan akan dikenai sanksi atau tindakan disiplin sesuai ketentuan yang berlaku.
8. Kepatuhan pegawai terhadap Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan harus dievaluasi secara berkala oleh atasan masing-masing dan menjadi bagian dari penilaian kinerja pegawai.
9. Seluruh pegawai yang berhenti bekerja dan mutasi harus mengembalikan seluruh aset informasi yang dipergunakan selama bekerja sesuai dengan ketentuan yang berlaku.
10. Pihak ketiga yang habis masa kontrak kerjanya harus mengembalikan seluruh aset informasi yang dipergunakan selama bekerja di Kementerian Perhubungan.
11. Unit eselon I harus menghentikan hak penggunaan aset informasi bagi pegawai yang sedang menjalani pemeriksaan yang terkait dengan dugaan adanya pelanggaran Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan dan/atau yang sedang menjalani proses hukum.
12. Unit eselon I harus mencabut hak akses terhadap aset informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi bekerja di Kementerian Perhubungan.

D. STANDAR

Keamanan Sumber Daya Manusia meliputi :

1. Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menjadi bagian dari penjabaran tugas dan fungsi, khususnya bagi yang memeiliki akses terhadap aset informasi;
2. Pimpinan dari pegawai berkeahlian khusus atau yang berada di posisi kunci (*key person*) harus memastikan ketersediaan pengganti pegawai tersebut dengan kompetensi yang setara apabila pegawai yang bersangkutan mutasi/berhenti;
3. Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menyertakan persyaratan untuk :
   a. Melaksanakan dan bertindak sesuai dengan organisasi keamanan informasi;
   b. Melindungi aset dari akses yang tidak sah, penyingkapan, modifikasi, kerusakan atau gangguan;

c. Melaksanakan proses keamanan atau kegiatan keamanan informasi sesuai dengan peran dan tanggung jawabnya; dan
d. Melaporkan kejadian, potensi kejadian, atau risiko keamanan informasi sesuai dengan Kebijakan dan Standar SMKI di lingkungan Kementerian Perhubungan.

4. Pemeriksaan latar belakang calon pegawai dan pihak ketiga Kementerian Perhubungan harus memperhitungkan privasi, perlindungan data pribadi dan/atau pekerjaan berdasarkan undang-undang, meliputi:
   a. Ketersediaan referensi, dari referensi hubungan kerja dan referensi pribadi;
   b. Pemeriksaan kelengkapan dan ketepatan dari riwayat hidup pemohon;
   c. Konfirmasi kualifikasi akademik dan profesional yang diklaim;
   d. Pemeriksaan independen identitas (paspor atau dokumen yang sama); dan
   e. Pemeriksaan lebih rinci, seperti pemeriksaan kredit atau pemeriksaan dari catatan kriminal.

VI. PENGENDALIAN KEAMANAN FISIK DAN LINGKUNGAN

A. TUJUAN

Keamanan fisik dan lingkungan bertujuan untuk mencegah akses fisik oleh pihak yang tidak berwenang, menghindari terjadinya kerusakan pada perangkat pengolah informasi serta gangguan pada aktifitas organisasi.

B. RUANG LINGKUP

Kebijakan dan standar keamanan fisik dan lingkungan ini meliputi:

1. Pengamanan area; dan
2. Pengamanan perangkat.

C. KEBIJAKAN

1. Pengamanan Area
   a. Seluruh pegawai, pihak ketiga, dan tamu yang memasuki lingkungan Kementerian Perhubungan harus mematuhi aturan yang berlaku di Kementerian Perhubungan.

b. Ketentuan rinci tentang pengamanan area lingkungan kerja di Kementerian Perhubungan diuraikan dalam standar keamanan fisik dan lingkungan.

2. Pengamanan Perangkat

a. Penempatan dan perlindungan perangkat

Perangkat pengolah informasi dan perangkat pendukung harus ditempatkan di lokasi yang aman dan diposisikan sedemikian rupa untuk mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang.

b. Penyediaan perangkat pendukung

Perangkat pendukung harus dipasang untuk menjamin beroperasinya perangkat pegolah informasi dan secara berkala harus diperiksa dan diuji ulang kinerjanya.

c. Pengamanan Kabel

1) Kabel sumber daya listrik harus dilindungi dari kerusakan; dan

2) Kabel telekomunikasi yang mengalirkan informasi harus dilindungi dari kerusakan dan penyadapan.

d. Pemeliharaan Perangkat

Perangkat harus dipelihara secara berkala untuk menjamin ketersediaan, keutuhan (integrity) dan fungsinya.

e. Pengamanan perangkat di luar lingkungan Kementerian Perhubungan,

Penggunaan perangkat yang dibawa ke luar dari lingkungan Kementerian Perhubungan harus disetujui oleh Pejabat yang berwenang.

f. Pengamanan penggunaan kembali atau penghapusan/pemusnahan perangkat

1) Perangkat pengolah informasi penyimpan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dihapuskan/dimusnahkan; dan

2) Penanganan perangkat pengolah informasi penyimpan data di Kementerian Perhubungan sesuai dengan standar penanganan media penyimpan data yang ditetapkan dalam ketentuan tersendiri.

D. STANDAR

Pengamanan area dan pengamanan perangkat meliputi:

1. Perangkat harus dipelihara sesuai dengan petunjuk manualnya. Untuk pemeliharaan yang dilakukan oleh pihak ketiga, harus diadakan Perjanjian Tingkat Layanan (*Service Level Agreement/SLA*) yang mendefinisikan tingkat pemeliharaan yang disediakan dan tingkat kinerja yang harus dipenuhi pihak ketiga.
2. Pemeliharaan terhadap perangkat keras atau perangkat lunak dilakukan hanya oleh pegawai yang berwenang.
3. Dalam hal pemeliharaan perangkat tidak dapat dilakukan di tempat, maka pemindahan perangkat harus mendapatkan persetujuan Pejabat yang berwenang. Terhadap data yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA yang disimpan dalam perangkat tersebut harus dipindahkan terlebih dahulu.
4. Otorisasi penggunaan perangkat harus dilakukan secara tertulis dan data yang terkait dengan aset informasi yang digunakan, seperti nama pemakai aset, lokasi, dan tujuan penggunaan aset, harus dicatat dan disimpan.
5. Pengamanan Area
   a. Unit TIK pusat dan unit TIK eselon I menyimpan perangkat pengolah informasi di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai antara lain pintu elektronik, sistem pemadam kebakaran, alarm bahaya dan perangkat pemutus aliran listrik;
   b. Akses ke ruang server, pusat data, dan area kerja yang berisikan aset informasi yang memiliki kalsifikasi SANGAT RAHASIA dan RAHASIA harus dibatasi dan hanya diberikan kepada pegawai yang berwenang;
   c. Pihak ketiga yang memasuki ruang server, pusat data, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus didampingi pegawai unit TIK pusat dan/atau unit TIK eselon I sepanjang waktu kunjungan. Waktu masuk dan keluar serta maksud kedatangan harus dicatat dalam buku catatan kunjungan;
   d. Kantor, ruangan, dan perangkat yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus dilindungi secara memadai;

e. Pegawai dan pihak ketiga tidak diizinkan merokok, makan, minum di ruang server dan pusat data; dan
f. Area keluar masuk barang dan area publik harus selalu dijaga, diawasi dan dikendalikan, dan jika memungkinkan disterilkan dari perangkat pengolah informasi untuk menghindari akses oleh pihak yang tidak berwenang.

6. Pengamanan Kantor, Ruangan, dan Fasilitas

Pengamanan kantor, ruangan, dan fasilitas mencakup:

a. Pengamanan kantor, ruangan, dan fasilitas harus sesuai dengan peraturan dan standar keamanan dan keselamatan kerja yang berlaku;
b. Fasilitas utama harus ditempatkan khusus untuk menghindari akses publik;
c. Pembatasan pemberian identitas atau tanda-tanda keberadaan aktivitas pengolahan informasi; dan
d. Direktori dan buku telepon internal yang mengidentifikasi lokasi perangkat pengolah informasi tidak mudah diakses oleh publik.

7. Perlindungan terhadap Ancaman Eksternal dan Lingkungan

Perlindungan terhadap ancaman eksternal dan lingkungan harus mempertimbangkan:

a. Bahan-bahan berbahaya atau mudah terbakar harus disimpan pada jarak yang aman dari secure areas;
b. Perlengkapan umum seperti alat tulis tidak boleh disimpan di dalam *secure areas*;
c. Perangkat *fallback* dan media *backup* harus diletakkan pada jarak yang aman untuk menghindari kerusakan dari bencana yang mempengaruhi fasilitas utama; dan
d. Perangkat pemadam kebakaran harus disediakan dan diletakkan di tempat yang tepat.

8. Penempatan dan Perlindungan Perangkat

Penempatan dan perlindungan perangkat harus mencakup:

a. Perangkat harus diletakkan pada lokasi yang meminimalkan akses yang tidak perlu ke dalam area kerja;
b. Perangkat pengolah informasi yang menangani informasi sensitif harus diposisikan dan dibatasi arah sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak yang tidak berwenang selama digunakan, dan perangkat penyimpanan

diamankan untuk menghindari akses oleh pihak yang tidak berwenang;

c. Perangkat yang memerlukan perlindungan khusus seperti perangkat cetak khusus, perangkat jaringan di luar ruang server harus terisolasi untuk mengurangi tingkat perlindungan/perlakuan standar yang perlu dilakukan;
d. Langkah-langkah pengendalian dilakukan untuk meminimalkan risiko potensi ancaman fisik, seperti pencurian, api, bahan peledak, asap, air termasuk kegagalan penyediaan air, debu, getaran, efek kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetis, dan perusakan;
e. Kondisi lingkungan, seperti suhu dan kelembaban harus dimonitor untuk mencegah perubahan kondisi yang dapat mempengaruhi pengoperasian perangkat pengolah informasi;
f. Perlindungan petir harus diterapkan untuk semua bangunan dan filter perlindungan petir harus dipasang untuk semua jalur komunikasi dan listrik; dan
g. Perangkat pengolah informasi sensitif harus dilindungi untuk meminimalkan risiko kebocoran informasi.

9. Pengamanan Kabel

Perlindungan keamanan kabel mencakup:

a. Pemasangan kabel sumber daya listrik dan kabel telekomunikasi ke perangkat pengolah informasi selama memungkinkan harus terletak di bawah tanah, atau menerapkan alternatif perlindungan lain yang memadai;
b. Pemasangan kabel jaringan harus dilindungi dari penyusupan yang tidak sah atau kerusakan, misalnya dengan menggunakan conduit atau menghindari rute melalui area publik;
c. Pemisahan antara kabel sumber daya listrik dengan kabel telekomunikasi untuk mencegah interferensi;
d. Penandaan/penamaan kabel dan perangkat harus diterapkan secara jelas untuk memudahkan penanganan kesalahan;
e. Penggunaan dokumentasi daftar panel patch diperlukan untuk mengurangi kesalahan; dan
f. Pengendalian untuk sistem informasi yang sensitif harus mempertimbangkan
   1) Penggunaan conduit;

2) Penggunaan ruangan terkunci pada tempat inspeksi dan titik pemutusan kabel;
3) Penggunaan rute alternatif dan/ atau media transmisi yang menyediakan keamanan yang sesuai;
4) Penggunaan kabel fiber optik;
5) Penggunaan lapisan elektromagnet untuk melindungi kabel;
6) Inisiasi penghapusan teknikal *(technical sweeps)* dan pemeriksaan secara fisik untuk peralatan yang tidak diotorisasi saat akan disambungkan ke kabel; dan
7) Penerapan akses kontrol ke panel patch dan ruangan kabel;

VII. PENGENDALIAN PENGELOLAAN KOMUNIKASI DAN OPERASIONAL

A. TUJUAN

Pengelolaan komunikasi dan operasional bertujuan untuk memastikan operasional yang aman dan benar pada perangkat pengolah informasi, mengimplementasikan dan memelihara keamanan informasi, mengelola layanan yang diberikan pihak ketiga, meminimalkan risiko kegagalan, melindungi keutuhan dan ketersediaan informasi dan perangkat lunak, memastikan keamanan pertukaran informasi dan pemantauan terhadap proses operasional.

B. RUANG LINGKUP

Kebijakan dan standar pengelolaan komunikasi dan operasional ini meliputi:

1. Prosedur operasional dan tanggung jawab;
2. Pengelolaan layanan oleh pihak ketiga;
3. Perencanaan dan penerimaan sistem;
4. Perlindungan terhadap ancaman program yang membahayakan *(malicious code)*;
5. *Backup*;
6. Pengelolaan keamanan jaringan;
7. Penanganan media penyimpan data;
8. Pertukaran informasi; dan
9. Pemantauan.

C. KEBIJAKAN

1. Prosedur Operasional dan Tanggung Jawab
   a. Dokumentasi prosedur operasional

      Unit TIK pusat dan unit TIK eselon I harus mendokumentasikan, memelihara, dan menyediakan seluruh prosedur operasional yang terkait dengan penggunaan perangkat pengolah informasi bagi pengguna sesuai dengan peruntukannya.
   b. Pengelolaan perubahan layanan TIK

      Unit TIK pusat dan unit TIK eselon I harus mengendalikan perubahan terhadap perangkat pengolah informasi. Pengelolaan perubahan layanan TIK di Kementerian Perhubungan yang ditetapkan dalamketentuan tersendiri.
   c. Pemisahan tugas

      Unit eselon I harus melakukan pemisahan tugas untuk proses yang melibatkan informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA untuk menghindari adanya pegawai yang memiliki pengendalian eksklusif terhadap seluruh aset informasi dan perangkat pengolahnya.
   d. Pemisahan perangkat pengembangan dan operasional

      Unit TIK pusat dan unit TIK eselon I harus melakukan pemisahan perangkat. pengembangan, pengujian, dan operasional untuk mengurangi risiko perubahan atau akses oleh pihak yang tidak berwenang terhadap sistem operasional.
2. Pengelolaan Layanan oleh Pihak Ketiga
   a. Penyediaan layanan

      Unit eselon I harus memastikan bahwa pengendalian keamanan informasi, definisi layanan, dan tingkat layanan yang tercantum dalam kesepakatan penyediaan layanan telah diterapkan, dioperasikan, dan dipelihara oleh pihak ketiga.
   b. Pemantauan dan kajian layanan pihak ketiga

      Unit eselon I harus melakukan pemantauan dan kajian terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh pihak ketiga secara berkala.
   c. Pengelolaan perubahan pada layanan pihak ketiga

      Unit eselon I harus memperhatikan kekritisan, proses yang terkait, dan hasil penilaian ulang risiko layanan apabila terjadi perubahan pada layanan yang disediakan pihak ketiga.

3. Perencanaan dan Penerimaan Sistem

   Kegiatan perencanaan dan penerimaan sistem meliputi:

   a. Pengelolaan kapasitas dalam rangka perencanaan sistem

      1) Unit TIK pusat dan unit TIK eselon I harus memantau penggunaan perangkat pengolah informasi dan membuat perkiraan pertumbuhan kebutuhan ke depan untukmemastikan ketersediaan kapasitas; dan

      2) Pengelolaan kapasitas di Kementerian Perhubungan ditetapkan dalam ketentuan tersendiri.

   b. Penerimaan Sistem

      1) Unit TIK pusat dan unit TIK eselon I harus menetapkan kriteria penerimaan (*acceptance criteria*) untuk sistem informasi baru, pemutakhiran (*upgrade*) dan versi baru serta melakukan pengujian sebelum penerimaan; dan

      2) Penerimaan sistem di Kementerian Perhubungan ditetapkan dalam ketentuan tersendiri.

4. Perlindungan terhadap Ancaman Program yang Membahayakan (*Malicious Code*)

   a. Unit TIK pusat dan unit TIK eselon I harus menerapkan sistem yang dapat melakukan pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan (*malicious code*).

   b. Perlindungan terhadap ancaman program yang membahayakan (*malicious code*) di Kementerian Perhubungan ditetapkan dalam ketentuan tersendiri.

5. Backup

   a. Unit TIK pusat dan unit TIK eselon I harus melakukan backup informasi dan perangkat lunak yang berada di Pusat Data secara berkala.

   b. Proses backup di Kementerian Perhubungan sesuai dengan standar backup data yang ditetapkan dalam ketentuan tersendiri.

6. Pengelolaan Keamanan Jaringan

   a. Pengendalian jaringan

      1) Unit TIK pusat dan unit TIK eselon I harus mengelola dan melindungi jaringan dari berbagai bentuk ancaman; dan

2) Ketentuan rinci pengendalian jaringan di Kementerian Perhubungan diuraikan dalam standar pengelolaan komunikasi dan operasional.

b. Keamanan layanan jaringan

Unit TIK pusat dan unit TIK eselon I harus mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan serta mencantumkannya dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh pihak ketiga.

7. Penanganan Media Penyimpan Data

a. Unit eselon I harus mempunyai prosedur yang mengatur penanganan media penyimpan data untuk melindungi aset informasi.

b. Penanganan media penyimpanan data di Kementerian Perhubungan sesuai dengan standar penanganan media penyimpan data yang ditetapkan dalam ketentuan tersendiri.

8. Pertukaran Informasi

a. Pertukaran informasi dan perangkat lunak antara Kementerian Perhubungan dengan pihak ketiga hanya akan dilakukan atas kesepakatan tertulis kedua belah pihak.

b. Unit eselon I harus melakukan penilaian risiko yang memadai sebelum melaksanakan pertukaran informasi.

c. Unit eselon I harus menerapkan pengendalian keamanan informasi untuk pengiriman informasi melalui surat elektronik atau pengiriman informasi melalui jasa layanan pengiriman dalam rangka menghindari akses pihak yang tidak berwenang.

d. Ketentuan rinci pertukaran informasi di Kementerian Perhubungan diuraikan dalam standar pengelolaan komunikasi dan operasional.

9. Pemantauan

a. Audit logging

Unit eselon I harus menerapkan *audit logging* yang mencatat aktivitas pengguna, pengecualian, dan kejadian keamanan informasi dalam kurun waktu tertentu untuk membantu pengendalian akses dan investigasi di masa mendatang.

b. Memantau penggunaan sistem

Unit TIK pusat dan unit TIK eselon I harus memantau penggunaan sistem dan mengkaji secara berkala hasil kegiatan pemantauan.

c. Perlindungan data catatan

Unit eselon I harus melindungi fasilitas pencatatan dan data yang dicatat dari kerusakan dan akses oleh pihak yang tidak berwenang.

d. Pencatatan kegiatan *system administrator* dan *system operator*

Unit TIK pusat dan unit TIK eselon I harus menerapkan pencatatan kegiatan *system administrator* dan *system operator.*

e. Pencatatan kesalahan (*fault logging*)

Unit eselon I harus menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindakan penanganan yang tepat.

f. Sinkronisasi waktu

Unit TIK pusat dan unit TIK eselon I harus memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.

D. STANDAR

1. Dokumentasi Prosedur Operasional

Prosedur operasional harus mencakup:

a. Tata cara pengolahan dan penanganan informasi;
b. Tata cara menangani kesalahan-kesalahan atau kondisi khusus yang terjadi beserta pihak yang harus dihubungi bila mengalami kesulitan teknis;
c. Cara memfungsikan kembali perangkat dan cara mengembalikan perangkat ke keadaan awal saat terjadi kegagalan sistem;
d. Tata cara *backup* dan *restore*; dan
e. Tata cara pengelolaan jejak audit (*audit trails*) pengguna dan catatan kejadian/kegiatan sistem.

2. Pemisahan Perangkat Pengembangan dan Operasional

Pemisahan perangkat pengembangan dan operasional harus mempertimbangkan:

a. Pengembangan dan operasional perangkat lunak harus dioperasikan di sistem atau prosesor komputer dan domain atau direktori yang berbeda;

b. Instruksi Kerja (*working instruction*) rilis dari pengembangan perangkat lunak ke operasional harus ditetapkan dan didokumentasikan;
c. *Compiler, editor*, dan alat bantu pengembangan lain tidak boleh diakses dari sistem operasional ketika tidak dibutuhkan;
d. Lingkungan sistem pengujian harus diusahakan sama dengan lingkungan sistem operasional;
e. Pengguna harus menggunakan profil pengguna yang berbeda untuk sistem pengujian dan sistem operasional, serta aplikasi harus menampilkan pesan identifikasi dari sistem untuk mengurangi risiko kesalahan; dan
f. Data yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA tidak boleh disalin ke dalam lingkungan pengujian sistem.

3. Pemantauan dan Pengkajian Layanan Pihak Ketiga

Pemantauan dan pengkajian layanan dari pihak ketiga, serta laporan dan catatan dari pihak ketiga mencakup proses sebagai berikut:

a. Pemantauan tingkat kinerja layanan untuk memastikan kesesuaian kepatuhan dengan perjanjian;
b. Pengkajian laporan layanan pihak ketiga dan pengaturan pertemuan berkala dalam rangka pembahasan perkembangan layanan sebagaimana diatur dalam perjanjian/ kesepakatan;
c. Pemberian informasi tentang gangguan keamanan informasi dan pengkajian informasi ini bersama pihak ketiga sebagaimana diatur dalam perjanjian/ kesepakatan;
d. Pemeriksaan jejak audit pihak ketiga dan pencatatan peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan; dan
e. Penyelesaian dan pengelolaan masalah yang teridentifikasi.

4. Pengelolaan Keamanan Jaringan

Pengelolaan keamanan jaringan mencakup:

a. Pemantauan kegiatan pengelolaan jaringan untuk menjamin bahwa perangkat jaringan digunakan secara efektif dan efisien;
b. Pengendalian dan pengaturan tentang penyambungan atau perluasan jaringan internal atau eksternal Kementerian Perhubungan;
c. Pengendalian dan pengaturan akses ke sistem jaringan internal atau eksternal Kementerian Perhubungan;

d. Pencatatan informasi pihak ketiga yang diizinkan mengakses ke jaringan Kementerian Perhubungan dan menerapkan pemantauan serta pencatatan kegiatan selama menggunakan jaringan.
e. Pemutusan layanan tanpa pemberitahuan sebelumnya jika terjadi gangguan keamanan informasi;
f. Perlindungan jaringan dari akses yang tidak berwenang mencakup:
   1) Penetapan untuk penanggung jawab pengelolaan jaringan dipisahkan dari pengelolaan perangkat pengolah informasi;
   2) Penerapan pengendalian khusus untuk melindungi keutuhan informasi yang melewati jaringan umum antara lain dengan penggunaan enkripsi dan tanda tangan elektronik (digital signature); dan
   3) Pendokumentasian arsitektur jaringan seluruh komponen perangkat keras jaringan dan perangkat lunak.
g. Penerapan fitur keamanan layanan jaringan mencakup:
   1) Teknologi keamanan seperti autentikasi, enkripsi, dan pengendalian sambungan jaringan;
   2) Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan keamanan dan aturan koneksi jaringan; dan
   3) Prosedur untuk penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau aplikasi.

5. Pertukaran Informasi
   a. Prosedur pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:
      1) Perlindungan pertukaran informasi dari pencegatan, penyalinan, modifikasi, miss-routing, dan perusakan;
      2) Pendeteksian dan perlindungan terhadap kode berbahaya yang dapat dikirim melalui penggunaan komunikasi elektronik;
      3) Perlindungan informasi elektronik dalam bentuk *attachment* yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA;
      4) Pertimbangan risiko terkait penggunaan perangkat komunikasi nirkabel;
   b. Pertukaran informasi yang tidak menggunakan perangkat komunikasi elektronik, mengacu pada ketentuan yang berlaku.

c. Pengendalian pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:
   1) Pencegahan terhadap penyalahgunaan wewenang pegawai dan pihak ketiga yang dapat membahayakan organisasi;
   2) Penggunaan teknik kriptografi;
   3) Penyelenggaraan penyimpanan dan penghapusan/pemusnahan untuk semua korespondensi kegiatan, termasuk pesan, yang sesuai dengan ketentuan yang berlaku;
   4) Larangan meninggalkan informasi sensitif pada perangkat pengolah informasi;
   5) Pembatasan penerusan informasi secara otornatis;
   6) Pembangunan kepedulian atas ancaman pencurian informasi, misalnya terhadap:
      a) Pengungkapan informasi sensitif untuk menghindari mencuri dengar saat melakukan panggilan telepon;
      b) Akses pesan diluar kewenangannya;
      c) Pemrograman mesin faksimili baik sengaja maupun tidak sengaja untuk mengirim pesan ke nomor tertentu; dan
      d) Pengiriman dokumen dan pesan ke tujuan yang salah.

d. Pembangunan kepedulian atas pendaftaran data demografis, seperti alamat surat elektronik atau informasi pribadi lainnya untuk menghindari pengumpulan informasi yang tidak sah; dan

e. Penyediaan informasi internal Kementerian Perhubungan bagi masyarakat umum harus disetujui oleh pemilik informasi dan sesuai dengan ketentuan yang berlaku.

6. Pemantauan

Prosedur pemantauan penggunaan sistem pengolah informasi ditetapkan untuk menjamin agar kegiatan akses yang tidak sah tidak perlu terjadi. Prosedur ini mencakup pemantauan:

a. Kegagalan akses (*access failures*);

b. Pola-pola *log-on* yang mengindikasikan penggunaan yang tidak wajar;

c. Alokasi dan penggunaan hak akses khusus (*privileged access capability*);

d. Penelusuran transaksi dan pengiriman file tertentu yang mencurigakan; dan

e. Penggunaan sumber daya sensitif.,

VIII. PENGENDALIAN AKSES

A. TUJUAN

Pengendalian akses bertujuan untuk memastikan otorisasi akses pengguna dan mencegah akses pihak yang tidak berwenang terhadap aset informasi khususnya perangkat pengolah informasi.

B. RUANG LINGKUP

Kebijakan dan standar pengendalian akses ini meliputi:

1. Persyaratan untuk pengendalian akses;
2. Pengelolaan akses pengguna;
3. Tanggung jawab pengguna;
4. Pengendalian akses jaringan;
5. Pengendalian akses ke sistem operasi;
6. Pengendalian akses ke aplikasi dan sistem informasi; dan
7. *Mobile Computing* dan *Teleworking.*

C. KEBIJAKAN

1. Persyaratan untuk Pengendalian Akses

   Unit eselon I harus menyusun, mendokumentasikan, dan mengkaji ketentuan akses ke aset informasi berdasarkan kebutuhan organisasi dan persyaratan keamanan.

2. Pengelolaan Akses Pengguna

   a. Pendaftaran pengguna

      Unit TIK pusat dan unit TIK eselon I harus menyusun prosedur pengelolaan hak akses pengguna sesuai dengan peruntukannya.

   b. Pengelolaan hak akses khusus

      Unit TIK pusat dan unit TIK eselon I harus membatasi dan mengendalikan penggunaan hak akses khusus.

   c. Pengelolaan kata sandi pengguna

      1) Unit TIK pusat dan unit TIK eselon I harus mengatur pengelolaan kata sandi pengguna;dan
      2) Pengelolaan kata sandi pengguna sesuai dengan standar yang ditetapkan dalam Kebijakan dan Standar Penggunaan Akun dan Kata Sandi, Surat Elektronik, dan Internet di Lingkungan Kementerian Perhubungan.

d. Kajian hak akses pengguna

Unit eselon I harus memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya.

3. Tanggung Jawab Pengguna

a. Pengguna harus mematuhi aturan pembuatan dan penggunaan kata sandi. Tanggung jawab pengguna terhadap kata sandi sesuai dengan standar tanggung jawab pengguna yang ditetapkan dalam ketentuan tersendiri.;

b. Pengguna harus memastikan perangkat pengolah informasi yang digunakan mendapatkan perlindungan terutama pada saat ditinggalkan; dan

c. Pengguna harus melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang.

4. Pengendalian Akses Jaringan

a. Penggunaan layanan jaringan

1) Unit TIK pusat dan unit TIK eselon I harus mengatur akses pengguna dalam mengakses jaringan Kementerian Perhubungan sesuai dengan peruntukannya;dan

2) Unit TIK pusat dan unit TIK eselon I harus mengatur akses pengguna dalam mengakses internet. Akses pengguna dalam mengakses internet sesuai dengan standar yang ditetapkan dalam ketentuan tersendiri.

b. Otorisasi pengguna untuk koneksi eksternal

Unit TIK pusat dan unit TIK eselon I harus menerapkan proses otorisasi pengguna untuk setiap akses ke dalam jaringan internal melalui koneksi eksternal (*remote access*).

c. Perlindungan terhadap diagnosa jarak jauh dan konfigurasi port

1) Akses ke perangkat keras dan perangkat lunak untuk diagnosa harus dikontrol berdasarkan prosedur dan hanya digunakan oleh pegawai yang berwenang untuk melakukan pengujian, pemecahan masalah, dan pengembangan sistem; dan

2) Port pada fasilitas jaringan yang tidak dibutuhkan dalam kegiatan atau fungsi layanan harus dinonaktifkan.

d. Pemisahan dalam jaringan

Unit TIK pusat dan unit TIK eselon I harus memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi.

e. Pengendalian koneksi jaringan

Unit TIK pusat dan unit TIK eselon I harus menerapkan mekanisme pengendalian akses pengguna sesuai dengan persyaratan pengendalian akses.

f. Pengendalian routing jaringan

Pengendalian routing jaringan internal Kementerian Perhubungan harus dilakukan sesuai pengendalian akses dan kebutuhan layanan informasi.

5. Pengendalian Akses ke Sistem Operasi

a. Prosedur akses yang aman

Akses ke sistem operasi harus dikontrol dengan menggunakan prosedur akses yang aman.

b. Identifikasi dan otorisasi pengguna

1) Setiap pengguna harus memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya; dan

2) Proses otorisasi pengguna harus menggunakan teknik autentikasi yang sesuai untuk memvalidasi identitas dari pengguna.

c. Sistem pengelolaan kata sandi

Sistem pengelolaan kata sandi harus mudah digunakan dan dapat memastikan kualitas kata sandi yang dibuat pengguna.

d. Penggunaan *system utilities*

Unit TIK pusat dan unit TIK eselon I harus membatasi dan mengendalikan penggunaan *system utilities*.

e. *Session time-out*

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

f. Pembatasan waktu koneksi

Unit TIK pusat dan unit TIK eselon I harus membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA.

6. Pengendalian Akses ke Aplikasi dan Sistem Informasi
   a. Unit TIK pusat dan unit TIK eselon I harus memastikan bahwa akses terhadap aplikasi dan sistem informasi hanya diberikan kepada pengguna sesuai peruntukannya.
   b. Aplikasi dan sistem informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus diletakkan pada lokasi terpisah untuk mengurangi kemungkinan diakses oleh pihak yang tidak berwenang.
7. *MobileComputing* dan *Teleworking*
   a. Unit TIK pusat dan unit TIK eselon I membangun kepedulian pengguna perangkat *mobile computing* dan *teleworking* akan risiko-risiko keamanan yang terus meningkat terhadap informasi yang tersimpan dalam perangkat *mobile computing*; dan
   b. Pengguna perangkat *mobile computing* dan *teleworking* harus mengikuti prosedur yang terkait penggunaan perangkat *mobile computing* dan *teleworking* untuk menjaga keamanan perangkat dan informasi di dalamnya.

D. STANDAR

1. Persyaratan untuk Pengendalian Akses

   Persyaratan untuk pengendalian akses mencakup:
   a. Penentuan kebutuhan keamanan dari pengolah aset informasi; dan
   b. Pemisahan peran pengendalian akses, seperti administrasi akses dan otorisasi akses.
2. Pengelolaan Akses Pengguna

   Prosedur pengelolaan akses pengguna harus mencakup:
   a. Penggunaan akun yang unik untuk mengaktifkan pengguna agar terhubung dengan sistem informasi atau layanan, dan pengguna dapat bertanggung jawab dalam penggunaan sistem informasi atau layanan tersebut. Penggunaan akun khusus hanya diperbolehkan sebatas yang diperlukan untuk kegiatan atau alasan operasional, dan harus disetujui Pejabat yang berwenang serta didokumentasikan;
   b. Pemeriksaan bahwa pengguna memiliki otorisasi dari pemilik sistem untuk menggunakan sistem informasi atau layanan, dan

jika diperlukan harus mendapat persetujuan yang terpisah dari Pejabat yang berwenang;

c. Pemeriksaan bahwa tingkat akses yang diberikan sesuai dengan tujuan kegiatan dan konsisten dengan Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan;
d. Pemberian pernyataan tertulis kepada pengguna tentang hak aksesnya dan meminta pengguna menandatangani pernyataan ketentuan akses tersebut;
e. Pemastian penyedia layanan tidak memberikan akses kepada pengguna sebelum prosedur otorisasi telah selesai;
f. Pemeliharaan catatan pengguna layanan yang terdaftar dalam menggunakan layanan;
g. Penghapusan atau penonaktifan akses pengguna yang telah berubah tugas dan/ atau fungsinya, setelah penugasan berakhir atau mutasi;
h. Pemeriksaan, penghapusan, serta penonaktifan akun secara berkala dan untuk pengguna yang memiliki lebih dari 1 (satu) akun; dan
i. Pemastian bahwa akun tidak digunakan oleh pengguna lain.

3. Pengelolaan Hak Akses Khusus (*privilege management*)

Pengelolaan hak akses khusus harus mempertimbangkan:

a. Hak akses khusus setiap sistem dari pabrikan perlu diidentifikasi untuk dialokasikan/ diberikan kepada pengguna yang terkait dengan produk, seperti sistem operasi, sistem pengelolaan basis data, aplikasi;
b. Hak akses khusus hanya diberikan kepada pengguna sesuai dengan peruntukkannya berdasarkan kebutuhan dan kegiatan tertentu;
c. Pengelolaan proses otorisasi dan catatan dari seluruh hak akses khusus yang dialokasikan/ diberikan kepada pengguna. Hak akses khusus tidak boleh diberikan sebelum proses otorisasi selesai;
d. Pengembangan dan penggunaan sistem rutin (misal *job scheduling*) harus diutamakan untuk menghindari kebutuhan dalam memberikan hak akses khusus secara terus menerus kepada pengguna;

e. Hak akses khusus harus diberikan secara terpisah dari akun yang digunakan untuk kegiatan umum, seperti akun *system administrator, database administrator,* dan *network administrator.*

4. Kajian Hak Akses Pengguna

   Kajian hak akses pengguna harus mempertimbangkan:

   a. Hak akses pengguna harus dikaji paling sedikit 6 (enam) bulan sekali atau setelah terjadi perubahan pada sistem, atau struktur organisasi;
   b. Hak akses khusus harus dikaji paling sedikit 6 (enam) bulan sekali dalam jangka waktu lebih sering dibanding jangka waktu pengkajian hak akses pengguna, atau apabila terjadi perubahan pada sistem, atau struktur organisasi;
   c. Pemeriksaan hak akses khusus harus dilakukan secara berkala, untuk memastikan pemberian hak akses khusus telah diotorisasi.

5. Pengendalian Akses Jaringan

   a. Menerapkan prosedur otorisasi untuk pemberian akses ke jaringan dan layanan jaringan;
   b. Menerapkan teknik autentikasi akses dari koneksi eksternal, seperti teknik kriptografi, *token hardware,* dan *dial-back*; dan
   c. Melakukan penghentian/ isolasi layanan jaringan pada area jaringan yang mengalami gangguan keamanan informasi.

6. Pemisahan dalam Jaringan

   Melakukan pemisahan dalam jaringan antara lain:

   a. Pemisahan berdasarkan kelompok layanan informasi, pengguna, dan aplikasi; dan
   b. Pemberian akses jaringan kepada tamu, hanya dapat diberikan akses terbatas misalnya internet dan/ atau surat elektronik tanpa bisa terhubung ke jaringan internal Kementerian Perhubungan.

7. *Mobile Computing* dan *Teleworking*

   a. Penggunaan perangkat *mobile computing* dan *teleworking* harus mempertimbangkan:
      1) Memenuhi keamanan informasi dalarn penentuan lokasi;
      2) Menjaga keamanan akses;
      3) Menggunakan anti malicious code;
      4) Memakai perangkat lunak berlisensi; dan
      5) Mendapat persetujuan Pejabat yang berwenang/ atasan langsung pegawai.

b. Pencabutan hak akses dan pengembalian fasilitas perangkat *teleworking* apabila kegiatan telah selesai.

IX. PENGENDALIAN KEAMANAN INFORMASI DALAM PENGADAAN, PENGEMBANGAN, DAN PEMELIHARAAN SISTEM INFORMASI

A. TUJUAN

Keamanan informasi dalam pengadaan, pengembangan, dan pemeliharaan sistem informasi bertujuan untuk memastikan bahwa keamanan informasi merupakan bagian yang terintegrasi dengan sistem informasi, mencegah terjadinya kesalahan, kehilangan, serta modifikasi oleh pihak yang tidak berwenang.

B. RUANG LINGKUP

Kebijakan dan standar keamanan informasi dalam pengadaan, pengembangan dan pemeliharaan sistem informasi ini meliputi:

1. Keamanan Sistem Informasi;
2. Pengolahan informasi pada aplikasi;
3. Pengendalian penggunaan kriptografi;
4. Keamanan file sistem (*system files*);
5. Keamanan dalam proses pengembangan dan pendukung (*support proceses*); dan
6. Pengelolaan kerentanan teknis.

C. KEBIJAKAN

Pengadaan, pengembangan dan pemeliharaan sistem informasi harus memenuhi persyaratan sebagai berikut:

1. Keamanan Sistem lnformasi

   Unit TIK pusat dan unit TIK eselon I menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi yang relevan sebelum pengadaan, pengembangan, atau pemeliharaan sistem informasi baru.

2. Pengolahan Informasi pada Aplikasi

   a. Validasi data yang masuk

      Data yang akan dimasukkan ke aplikasi harus diperiksa terlebih dahulu kebenaran dan kesesuaiannya.

b. Pengendalian proses internal

Pada setiap aplikasi harus disertakan proses validasi untuk mendeteksi bahwa informasi yang dihasilkan utuh dan sesuai dengan yang diharapkan.

c. Validasi data keluaran

Data keluaran aplikasi harus divalidasi untuk memastikan data yang dihasilkan adalah benar.

3. Pengendalian Penggunaan Kriptografi
   a. Unit TIK pusat dan unit TIK eselon I harus mengembangkan dan menerapkan sistem kriptografi untuk perlindungan informasi dan membuat rekomendasi yang tepat bagi penerapannya.
   b. Sistem kriptografi harus digunakan untuk melindungi aset informasi yang memiliki klasifikasi SANGAT RAHASIA, RAHASIA, dan TERBATAS.
4. Keamanan File Sistem
   a. Pengendalian operasional perangkat lunak

      Unit TIK pusat dan unit TIK eselon I harus mempunyai prosedur untuk pengendalian perangkat lunak pada sistem operasional.

   b. Perlindungan terhadap sistem pengujian data

      Unit TIK pusat dan unit TIK eselon I harus menentukan sistem pengujian data, melindunginya dari kemungkinan kerusakan, kehilangan atau perubahan oleh pihak yang tidak berwenang.

   c. Pengendalian akses ke kode program (*source code*)

      Unit TIK pusat dan unit TIK eselon I harus mengendalikan akses ke kode program (*source code*) secara ketat dan salinan versi terkini dari perangkat lunak disimpan di tempat yang aman.
5. Keamanan dalam Proses Pengembangan dan Pendukung (*Support Proceses*);
   a. Prosedur pengendalian perubahan sistem operasi

      Unit TIK pusat dan unit TIK eselon I harus mengendalikan perubahan pada sistem operasi dengan penggunaan prosedur pengendalian perubahan.

   b. Prosedur pengendalian perubahan pada perangkat lunak

      Unit TIK pusat dan unit TIK eselon I harus mengendalikan perubahan terhadap perangkat lunak, baik perangkat lunak yang dikembangkan sendiri maupun pihak ketiga.

c. Kajian teknis aplikasi setelah perubahan sistem operasi dan/ atau perangkat lunak

Unit TIK pusat dan unit TIK eselon I harus meninjau dan menguji sistem operasi dan/ atau perangkat lunak untuk memastikan tidak ada dampak merugikan pada proses operasional atau keamanan informasi Kementerian Perhubungan pada saat terjadi perubahan sistem operasi dan/ atau perangkat lunak, terutama pada perangkat lunak yang memproses informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA.

d. Kebocoran informasi

Unit TIK pusat dan unit TIK eselon I harus mencegah kemungkinan terjadinya kebocoran informasi.

e. Pengembangan perangkat lunak oleh pihak ketiga

Unit TIK pusat dan unit TIK eselon I harus melakukan supervisi dan memantau pengembangan perangkat lunak oleh pihak ketiga.

6. Pengelolaan Kerentanan Teknis

a. Unit TIK pusat dan unit TIK eselon I harus mengumpulkan informasi kerentanan teknis secara berkala dari seluruh sistem informasi yang digunakan maupun komponen pendukung sistem informasi.

b. Unit TIK pusat dan unit TIK eselon I harus melakukan evaluasi dan penilaian risiko terhadap kerentanan teknis yang ditemukan dalam sistem informasi serta menetapkan pengendalian yang tepat terhadap risiko terkait.

D. STANDAR

1. Spesifikasi kebutuhan perangkat pengolah informasi yang dikembangkan baik oleh internal atau pihak ketiga harus didokumentasikan secara formal.
2. Pengolahan Data pada Aplikasi

a. Pemeriksaan data masukan harus mempertimbangkan:

1) Penerapan masukan rangkap (*dual input*) atau mekanisme pengecekan masukan lainnya untuk mendeteksi kesalahan berikut:

a) Di luar rentang/batas nilai-nilai yang diperbolehkan;

b) Karakter tidak valid dalam field data;

c) Data hilang atau tidak lengkap;

d) Melebihi batas atas dan bawah volume data; dan
e) Data yang tidak diotorisasi dan tidak konsisten.

2) Pengkajian secara berkala terhadap isi field kunci (*key field*) atau file data untuk mengkonfirmasi keabsahan dan integritas data;
3) Memeriksa dokumen *hard copy* untuk memastikan tidak adanya perubahan data masukan yang tidak melalui otorisasi;
4) Menampilkan pesan yang sesuai dalam menanggapi kesalahan validasi;
5) Prosedur untuk menguji kewajaran dari data masukan;
6) Menguraikan tanggung jawab dari seluruh pegawai yang terkait dalam proses perekaman data; dan
7) Sistem mampu membuat dari mengeluarkan catatan aktivitas terkait proses perekaman data.

b. Menyusun daftar pemeriksaan (*check list*) yang sesuai, mendokumentasikan proses pemeriksaan, dan menyimpan hasilnya secara aman. Proses pemeriksaan mencakup:
1) Pengendalian *session* atau *batch*, untuk mencocokkan data setelah perubahan transaksi;
2) Pengendalian balancing untuk memeriksa data sebelum dan sesudah transaksi;
3) Validasi data masukan yang dihasilkan sistem;
4) Keutuhan dan keaslian data yang diunduh/ diunggah (*download/upload*);
5) *Hash totals* dari *record* dan *file*;
6) Aplikasi berjalan sesuai dengan rencana dan waktu yang ditentukan;
7) Program dijalankan dalam urutan yang benar dan menghentikan sementara jika terjadi kegagalan sampai masalah diatasi; dan
8) Sistem mampu membuat dan mengeluarkan catatan aktivitas pengelolaan internal.

c. Pemeriksaan data keluaran harus mempertimbangkan:
1) Kewajaran dari data keluaran yang dihasilkan;
2) Pengendalian rekonsiliasi data untuk memastikan kebenaran pengolahan data;

3) Menyediakan informasi yang cukup untuk pengguna atau sistem pengolahan informasi untuk menentukan akurasi, kelengkapan, ketepatan, dan klasifikasi informasi;
4) Prosedur untuk menindaklanjuti validasi data keluaran;
5) Menguraikan tanggung jawab dari seluruh pegawai yang terkait proses data keluaran; dan
6) Sistem mampu membuat dan mengeluarkan catatan aktivitas dalam proses validasi data keluaran.

3. Pengendalian dan Penggunaan Kriptografi

Pengembangan dan penerapan sistem kriptografi untuk perlindungan informasi harus mempertimbangkan:

a. Kondisi dari suatu kegiatan yang menentukan bahwa informasi harus dilindungi, seperti risiko kegiatan, media pengiriman informasi, tingkat perlindungan yang dibutuhkan;
b. Tingkat perlindungan yang dibutuhkan harus diidentifikasi berdasarkan penilaian risiko, antara lain jenis, kekuatan, dan kualitas dari algoritma enkripsi yang akan digunakan;
c. Keperluan enkripsi untuk perlindungan informasi SANGAT RAHASIA, RAHASIA dan TERBATAS yang melalui perangkat *mobile computing*, *removable media*, atau jalur komunikasi;
d. Pengelolaan kunci kriptografi, seperti perlindungan kunci kriptografi, pemulihan informasi terenkripsi dalam hal kehilangan atau kerusakan kunci kriptografi; dan
e. Dampak penggunaan informasi terenkripsi, seperti pengendalian terkait pemeriksaan suatu konten, kecepatan pemrosesan pada sistem.

4. Keamanan File Sistem

a. Pengembangan prosedur pengendalian perangkat lunak pada sistem operasional harus mempertimbangkan:
   1) Proses pemutakhiran perangkat lunak operasional, aplikasi, *library program* hanya boleh dilakukan oleh *system administrator* terlatih setelah melalui proses otorisasi;
   2) Sistem operasional hanya berisi program aplikasi *executable* yang telah diotorisasi, tidak boleh berisi kode program (*source code*) atau *compiler*;

3) Aplikasi dan perangkat lunak sistem operasi hanya dapat diimplementasikan setelah melewat proses pengujian yang ekstensif;
4) Sistem pengendalian konfigurasi harus digunakan untuk mengendalikan seluruh perangkat lunak yang telah diimplementasikan beserta dokumentasi sistem;
5) Strategi *rollback* harus tersedia sebelum suatu perubahan diimplementasikan;
6) Catatan audit harus dipelihara untuk menjaga kemutakhiran *library program operasional*;
7) Versi terdahulu dari suatu aplikasi harus tetap disimpan untuk keperluan kontijensi; dan
8) Versi lama dari suatu perangkat lunak harus diarsip, bersama dengan informasi terkait dan prosedur, parameter, konfigurasi rinci, dan perangkat lunak pendukung.

b. Perlindungan terhadap sistem pengujian data harus mempertimbangkan:
1) Prosedur pengendalian akses, yang berlaku pada sistem aplikasi operasional, harus berlaku juga pada sistem aplikasi pengujian;
2) Proses otorisasi setiap kali informasi/ data operasional digunakan pada sistem pengujian;
3) Penghapusan informasi/ data operasional yang digunakan pada sistem pengujian segera setelah proses pengujian selesai; dan
4) Pencatatan jejak audit penggunaan informasi/ data operasional.

c. Pengendalian akses ke kode program (*source code*) harus mempertimbangkan:
1) Kode program (*source code*) tidak boleh disimpan pada sistem operasional;
2) Pengelolaan kode program (*source code*) dan *library* harus mengikuti prosedur yang telah ditetapkan;
3) Pengelola TIK tidak boleh memiliki akses yang tidak terbatas ke kode program (*source code*) dan *library*;
4) Proses pemutakhiran kode program (*source code)* dan item terkait, serta pemberian kode program (*source code*) kepada

programmer hanya dapat dilakukan setelah melalui prose otorisasi;

5) *Listing program* harus disimpan dalam *secure areas;*

6) Catatan audit dari seluruh akses ke kode program *source code library* harus dipelihara; dan

7) Pemeliharaan dan penyalinan kode program *(source code) library* harus mengikuti prosedur pengendalian perubahan.

5. Keamanan dalam proses pengembangan dan pendukung (*support proceses*)

a. Prosedur pengendalian perubahan sistem operasi dan perangkat lunak, mencakup:

1) Memelihara catatan persetujuan sesuai dengan kewenangannya;

2) Memastikan permintaan perubahan diajukan oleh pihak yang berwenang;

3) Melakukan reviu untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;

4) Melakukan identifikasi terhadap perangkat lunak, informasi, basis data, dan perangkat keras yang perlu diubah;

5) Mendapatkan persetujuan formal dari pihak yang berwenang sebelum pelaksanaan perubahan;

6) Memastikan pihak yang berwenang menerima perubahan yang diminta sebelum dilakukan implementasi;

7) Memastikan bahwa dokumentasi sistem mutakhir dan dokumen versi sebelumnya diarsip;

8) Memelihara versi perubahan aplikasi;

9) Memelihara jejak audit perubahan aplikasi;

10) Memastikan dokumentasi penggunaan dan prosedur telah diubah sesuai dengan perubahan yang dilaksanakan; dan

11) Memastikan bahwa implementasi perubahan dilakukan pada waktu yang tepat dan tidak menganggu kegiatan.

b. Prosedur kajian teknis aplikasi setelah perubahan sistem operasi dan/ atau perangkat lunak, mencakup:

1) Melakukan reviu untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;

1) Melakukan reviu untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;
2) Memastikan rencana dan anggaran annual support yang mencakup reviu dan sistem testing dari perubahan sistem operasi;
3) Memastikan pemberitahuan perubahan sistem informasi dilakukan dalam jangka waktu yang tepat untuk memastikan tes dan reviu telah dilaksanakan sebelum implementasi; dan
4) Memastikan bahwa perubahan telah diselaraskan dengan rencana kelangsungan kegiatan.

c. Kebocoran informasi

Pengendalian yang dapat diterapkan untuk membatasi risiko kebocoran informasi, antara lain:

1) Melakukan pemantauan terhadap aktivitas pegawai dan pihak ketiga, sistem sesuai dengan ketentuan yang berlaku; dan
2) Melakukan pemantauan terhadap aktivitas penggunaan *desktop* dan perangkat *mobile.*

d. Pengembangan perangkat lunak oleh pihak ketiga harus mempertimbangkan

1) Perjanjian Lisensi; Kepemilikan source code, dan Hak Atas Kekayaan Intelektual (HAKI)
2) Penjanjian *escrow*;
3) Hak untuk melakukan audit terhadap kualitas dan akurasi pekerjaan;
4) Persyaratan kontrak mengenai kualitas dan fungsi keamanan aplikasi;
5) Uji coba terhadap aplikasi untuk memastikan tidak terdapat *malicious code* sebelum implementasi;

6. Pengelolaan Kerentanan Teknis, mencakup:

a. Penunjukan fungsi dan tanggung jawab yang terkait dengan pengelolaan kerentanan teknis termasuk di dalamnya pemantauan kerentanan, penilaian risiko kerentanan, *patching*, registrasi aset, dan koordinasi dengan pihak terkait;

b. Pengidentifikasian sumber informasi yang dapat digunakan untuk mengidentifikasi dan meningkatkan kepedulian terhadap kerentanan teknis;

c. Penentuan rentang waktu untuk melakukan aksi terhadap munculnya potensi kerentanan teknis. Apabila terjadi kerentanan teknis yang butuh penanganan maka harus diambil tindakan sesuai kontrol yang telah ditetapkan atau melaporkan kejadian tersebut melalui pelaporan kejadian dan kelemahan keamanan informasi;
d. Pengujian dan evaluasi penggunaan *patch* sebelum proses instalasi untuk memastikan *patch* dapat beketja secara efektif dan tidak menimbulkan risiko yang lain. Apabila *patch* tidak tersedia, harus melakukan hal sebagai berikut
   1) Mematikan *services* yang berhubungan dengan kerentanan;
   2) Menambahkan pengendalian akses seperti *firewall*;
   3) Meningkatkan pengawasan untuk mengidentifikasi atau mencegah terjadinya serangan atau kejadian;
   4) Meningkatkan kepedulian terhadap kerentanan teknis;
e. Penyimpanan *audit log* yang memuat prosedur dan langkah-langkah yang telah diambil;
f. Pemantauan dan evaluasi terhadap pengelolaan kerentanan teknis harus dilakukan secara berkala; dan
g. Pengelolaan kerentanan teknis diutamakan terhadap sistem informasi yang memiliki tingkat risiko tinggi.

X. PENGENDALIAN PENGELOLAAN GANGGUAN KEAMANAN INFORMASI

A. TUJUAN

Pengelolaan gangguan keamanan informasi bertujuan untuk memastikan kejadian dan kelemahan keamanan informasi yang terhubung dengan sistem informasi dikomunikasikan untuk dilakukan perbaikan, serta dilakukan pendekatan yang konsisten dan efektif agar dapat dihindari atau tidak terulang kembali.

B. RUANG LINGKUP

Kebijakan dan standar pengelolaan gangguan keamanan informasi ini meliputi:

1. Pelaporan kejadian dan kelemahan keamanan informasi; dan
2. Pengelolaan gangguan keamanan informasi dan perbaikannya.

C. KEBIJAKAN

1. Pelaporan Kejadian dan Kelemahan Keamanan Informasi
   a. Pegawai dan pihak ketiga harus melaporkan kepada unit TIK pusat dan unit TIK eselon I sesegera mungkin pada saat menemui kelemahan atau terjadi gangguan keamanan informasi dalam sistem atau layanan TIK Kementerian Perhubungan.
   b. Proses penanganan gangguan di Kementerian Perhubungan ditetapkan dalam ketentuan tersendiri.
2. Pengelolaan Gangguan Keamanan Informasi dan Perbaikannya
   a. Prosedur dan tanggung jawab

      Unit TIK pusat dan unit TIK eselon I masing-masing harus menyusun prosedur dan menguraikan tanggung jawab pegawai, terkait dalam rangka memastikan gangguan keamanan informasi dapat ditangani secara cepat dan efektif.
   b. Peningkatan penanganan gangguan keamanan informasi
      1) Seluruh gangguan keamanan informasi yang terjadi dan tindakan mengatasinya harus dicatat dalam suatu basis data dan/ atau buku catatan pelaporan gangguan keamanan informasi, dan akan menjadi masukan pada proses peningkatan penanganan gangguan keamanan informasi.
      2) Seluruh catatan gangguan keamanan informasi akan dievaluasi dan dianalisis untuk perbaikan dan pencegahan agar gangguan keamanan informasi tidak terulang.

   c. Pengumpulan bukti pelanggaran.

      Unit TIK pusat dan unit TIK eselon I harus mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap Kebijakan dan Standar SMKI di Lingkungan Kementerian Perhubungan.

D. STANDAR

1. Pelaporan Kejadian dan Kelemahan Keamanan Informasi
   a. Gangguan keamanan informasi antara lain:
      1) Hilangnya layanan, perangkat, atau fasilitas TIK;
      2) Kerusakan fungsi sistem atau kelebihan beban;
      3) Perubahan sistem diluar kendali;
      4) Kerusakan fungsi perangkat lunak atau perangkat keras;

5) Pelanggaran akses ke dalam sistem pengolah informasi TIK;
6) Kelalaian manusia; dan
7) Ketidaksesuaian dengan ketentuan yang berlaku.

b. Pegawai dan pihak ketiga harus menyadari tanggung jawab mereka untuk melaporkan setiap gangguan keamanan informasi secepat mungkin. Pelaporan gangguan harus mencakup:
1) Proses umpan balik yang sesuai untuk memastikan bahwa pihak yang melaporkan kejadian keamanan informasi mendapatkan pemberitahuan penanganan masalah;
2) Formulir laporan gangguan keamanan informasi untuk mendukung tindakan pelaporan dan membantu pelapor mengingat kronologis kejadian keamanan informasi;
3) Perilaku yang benar dalam menghadapi gangguan keamanan informasi, antara lain:
a) Mencatat semua rincian penting gangguan dengan segera, seperti jenis pelanggaran, jenis kerusakan, pesan pada layar, atau anomali sistem; dan
b) Segera melaporkan gangguan ke pihak berwenang sebelum melakukan tindakan penanganan sendiri.
4) Sebagai referensi yang digunakan dalam proses penanganan pelanggaran disiplin bagi pegawai dan pihak ketiga yang melakukan pelanggaran keamanan informasi.

2. Prosedur Pengelolaan Gangguan Keamanan Informasi

Prosedur pengelolaan gangguan keamanan informasi harus mempertimbangkan :

a. Prosedur yang harus ditetapkan untuk menangani berbagai jenis gangguan keamanan informasi, antara lain:
1) Kegagalan sistem informasi dan hilangnya layanan;
2) Serangan program yang membahayakan (*malicious code*);
3) Serangan *denial of service*;
4) Kesalahan akibat data tidak lengkap atau tidak akurat;
5) Pelanggaran kerahasiaan dan keutuhan; dan
6) Penyalahgunaan sistem informasi.

b. Untuk melengkapi rencana kontijensi, prosedur harus mencakup:
1) Analisis dan identifikasi penyebab gangguan;
2) Mengarantina atau membatasi gangguan;

3) Perencanaan dan pelaksanaan tindakan korektif untuk mencegah gangguan berulang;
4) Komunikasi dengan pihak-pihak yang terkena dampak pemulihan gangguan;dan
5) Pelaporan tindakan ke pihak berwenang.

c. Jejak audit dan bukti serupa harus dikumpulkan dan diamankan untuk:
1) Analisis masalah internal;
2) Digunakan sebagai bukti forensik yang berkaitan dengan potensi pelanggaran kontrak atau peraturan atau persyaratan dalam hal proses pidana atau perdata; dan
3) Digunakan sebagai bahan tuntutan ganti rugi pada pihak ketiga yang menyediakan perangkat lunak dan layanan.

d. Tindakan untuk memulihkan keamanan dari pelanggaran dan perbaikan kegagalan sistem harus dikendalikan secara hati-hati dan formal, prosedur harus memastikan bahwa:
1) Hanya pegawai yang sudah diidentifikasi dan berwenang yang diizinkan akses langsung ke sistem dan data;
2) Semua tindakan darurat yang diambil, didokumentasikan secara rinci;
3) Tindakan darurat dilaporkan kepada pihak berwenang; dan
4) Keutuhan sistem dan pengendaliannya dikonfirmasikan dengan pihak-pihak terkait sesegera mungkin.

XI. PENGENDALIAN KEAMANAN INFORMASI DALAM PENGELOLAAN KELANGSUNGAN KEGIATAN

A. TUJUAN

Keamanan informasi dalam pengelolan kelangsungan kegiatan bertujuan untuk melindungi sistem informasi, memastikan berlangsungnya kegiatan dan layanan pada saat keadaan darurat, serta memastikan pemulihan yang tepat.

B. RUANG LINGKUP

Kebijakan dan standar keamanan informasi dalam pengelolaan kelangsungan kegiatan ini meliputi :

1. Proses Pengelolaan Kelangsungan Kegiatan;
2. Penilaian Risiko dan Analisis Dampak Bisnis (*Business Impact Analysis/BIA*);

3. Penyusunan dan penerapan Rencana Kelangsungan Kegiatan (*Business Continuity Plan/BCP*);
4. Pengujian, Pemeliharaan dan Pengkajian Ulang Rencana Kelangsungan kegiatan.

C. KEBIJAKAN

1. Unit eselon I harus mengelola proses kelangsungan kegiatan pada saat keadaan darurat di lingkungan unit eselon 1 masing-masing.
2. Unit eselon I harus mengidentifikasi risiko dan menganalisis dampak yang diakibatkan pada saat terjadi keadaan darurat untuk menjamin kelangsungan kegiatan.
3. Unit eselon I harus menyusun dan menerapkan rencana kelangsungan kegiatan untuk menjaga dan mengembalikan kegiatan operasional dalam jangka waktu yang disepakati dan level yang dibutuhkan.
4. Unit eselon I harus memelihara dan memastikan rencana-rencana yang termuat dalam rencana kelangsungan kegiatanmasih sesuai dan mengidentifikasi prioritas untuk kegiatan uji coba.
5. Unit eselon I harus melakukan uji coba Rencana kelangsungan kegiatan secara berkala untuk memastikan Rencana kelangsungan kegiatan dapat dilaksanakan secara efektif.

D. STANDAR

1. Pengelolan Kelangsungan Kegiatan pada saat keadaan Darurat. Komponen yang harus diperhatikan dalam mengelola proses kelangsungan kegiatan.
   a. Identifikasi risiko dan analisis dampak yang diakibatkan pada saat terjadi keadaan darurat;
   b. Identifikasi seluruh aset informasi yang menunjang proses kritikal;
   c. Identifikasi sumber daya, mencakup biaya, struktur organisasi, teknis pelaksanaan, pegawai dan pihak ketiga;
   d. Memastikan keselamatan pegawai dan perlindungan terhadap perangkat pengolah informasi dan aset organisasi;
   e. Penyusunan dan pendokumentasian rencana kelangsungan kegiatan sesuai dengan Rencana Strategis (Renstra) Kementerian Perhubungan;

f. Pelaksanaan uji coba dan pemeliharaan rencana kelangsungan kegiatan secara berkala.

2. Proses identifikasi risiko mengenai Penerapan Manajemen Risiko di Lingkungan Kementerian Perhubunganditetapkandalam ketentuan tersendiri;
3. Proses analisis dampak kegiatan harus melibatkan pemilik proses bisnis dan dievaluasi secara berkala;
4. Penyusunan rencana kelangsungan kegiatan mencakup :
   a. Prosedur saat keadaan darurat mencakup tindakan yang harus dilakukan serta pengaturan hubungan dengan pihak berwenang;
   b. *Prosedur fallback*, mencakup tindakan yang harus diambil untuk memudahkan kegiatan kritikal atau layanan pendukung ke lokasi kerja sementara dan mengembalikan operasional kegiatan kritikal dalam jangka waktu sesuai dengan standar ketersediaan data yang ditetapkan dalam ketentuan tersendiri.
   c. Prosedur saat kondisi telah normal (*resumption*), adalah mengembalikan kegiatan operasional ke kondisi normal.
   d. Jadwal uji coba mencakup langkah-langkah dan waktu pelaksanaan uji coba serta proses pemeliharaannya.
   e. Pelaksanaan Pelatihan dan sosialisasi dalam rangka meningkatkan kepedulian dan pemahaman proses kelangsungan kegiatan dan memastikan proses kelangsungan kegiatan dilaksanakan secara efektif.
   f. Tanggung Jawab dan peran setiap petugas Pelaksana Pengelolaan Proses Kelangsungan.
   g. Daftar kebutuhan aset informasi kritikal dan sumber daya untuk dapat menjalankan prosedur saat keadaan darurat, *fallback* dan saat kondisi telah normal.
5. Uji Coba Rencana Kelangsungan Kegiatan harus dilaksanakan untuk memastikan setiap rencana yang disusun dapat dilakukan/ dipenuhi pada saat penerapannya. Kegiatan ujicoba Rencana Kelangsungan Kegiatan ini mencakup :
   a. Simulasi terutama untuk petugas Pelaksana Pengelola Proses Kelangsungan Kegiatan.
   b. Ujicoba *recovery* sistem informasi untuk memastikan sistem informasi dapat berfungsi kembali.

c. Ujicoba proses *recovery* di lokasi kerja sementara untuk menjalankan proses bisnis secara *parallel.*
d. Ujicoba terhadap perangkat dan layanan yang disediakan oleh pihak ketiga.
e. Ujicoba keseluruhan mulai dari organisasi, petugas, perangkat dan proses.

XII. PENGENDALIAN KEPATUHAN

A. TUJUAN

Pengendalian kepatuhan bertujuan untuk menghindari pelanggaran terhadap peraturan perundangan yang terkait keamanan informasi.

B. RUANG LINGKUP

Kebijakan dan standar kepatuhan ini meliputi :

1. Kepatuhan terhadap peraturan perundangan yang terkait keamanan informasi;
2. Kepatuhan Teknis; dan
3. Audit sistem informasi.

C. KEBIJAKAN

1. Kepatuhan terhadap Peraturan Perundangan yang terkait Keamanan Informasi :
   a. Seluruh Pegawai dan pihak ketiga harus menaati peraturan perundangan yang terkait dengan keamanan informasi;
   b. Identifikasi peraturan perundangan yang dapat diterapkan Unit TIK pusat dan Unit TIK eselon I harus mengidentifikasi mendokumentasikan dan memelihara kemutahiran semua peraturan perundangan yang terkait dengan sistem Keamanan Informasi;
   c. Hak Atas Kekayaan Intelektual
      Perangkat lunak yang dikelola unit TIK pusat dan unit TIK eselon I harus memenuhi ketentuan penggunaan lisensi. Penggandaan perangkat lunak secara tidak sah tidak diizinkan dan merupakan bentuk pelanggaran;
   d. Perlindungan Terhadap Rekaman;
      Rekaman milik Kementerian Perhubungan harus dilindungi dari kehilangan, kerusakan atau penyalahgunaan;

e. Pengamanan Data

Unit TIK pusat dan TIK eselon I melindungi kepemilikan dan kerahasiaan data. Data hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundangan dari kesepakatan.

2. Kepatuhan Teknis

Unit TIK pusat dan unit TIK eselon I harus melakukan pemeriksaan kepatuhan teknis secara berkala untuk menjamun efektifitas standar dan prosedur keamanan informasi yang ada di areal operasional.

3. Audit Sistem Informasi

a. Unit TIK pusat dan unit eselon I bersama dengan Inspektorat Jenderal harus membuat perancanaan persyaratan, ruang lingkup dan kegiatan audit yang melibatkan pemeriksaan sistem operasional untuk mengurangi kemungkinan risiko gangguan yang bisa terjadi terhadap kegiatan Kementerian Perhubungan selama proses audit.

b. Perlindungan terhadap alat bantu (*Tools*) audit sistem informasi. Penggunaan alat bantu (baik perangkat lunak maupun perangkat keras) untuk mengetahui kelemahan keamanan, memindai (*Scanning*) kata sandi, atau untuk melemahkan dan menerobos sistem keamanan informasi tidak diizinkan kecuali atas persetujuan Pimpinan Unit TIK Pusat dan Unit TIK eselon I.

c. Audit sistem informasi di Kementerian Perhubungan ditetapkan dalam ketentuan tersendiri.

D. STANDAR

1. Kepatuhan terhadap Hak Kekayaan Intelektual

Hal yang perlu diperhatikan dalam melindungi segala materi yang dapat dianggap kekayaan intelektual meliputi:

a. Mendapatkan perangkat lunak hanya melalui sumber yang dikenal dan memiliki reputasi baik, untuk memastikan hak cipta tidak dilanggar ;

b. Memelihara daftar aset informasi sesuai persyaratan untuk melindungi hak kekayaan intelektual;

c. Memelihara bukti kepemilikan lisensi, *master disk*, buku petunjuk, dan lain sebagainya;

d. Menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;

e. Melakukan pemeriksaan bahwa hanya perangkat lunak dan produk berlisensi yang dipasang;
f. Patuh terhadap syarat dan kondisi untuk perangkat lunak dan informasi yang didapat dari jaringan publik;
g. Dilarang melakukan duplikasi, konversi dan format lain atau mengambil dari rekaman komersial (film atau audio) selain yang diperbolehkan oleh undang-undang Hak Cipta, dan ;
h. Tidak menyalin secara penuh atau sebagian buku, artikel, laporan atau dokumen lainnya selain yang diizinkan oleh undang-undang Hak Cipta.

2. Kepatuhan terhadap Kebijakan dan Standar

Hal yang perlu dilakukan jika terdapat ketidakpatuhan teknis meliputi:

a. Menentukan dan mengevaluasi penyebab ketidakpatuhan.
b. Menentukan tindakan yang perlu dilakukan berdasarkan hasil evaluasi agar ketidakpastian tidak terulang kembali;
c. Menetukan dan melaksanakan tindakan perbaikan yang sesuai; dan
d. Mengkaji tindakan perbaikan yang perlu dilakukan.

3. Kepatuhan Teknis

Sistem informasi harus diperiksa secara berkala untuk memastikan pengendalian perangkat keras dan perangkat lunak telah diimplementasikan secara benar. Kepatuhan teknis juga mencakup pengujian penetrasi *(penetrating test)* untuk mendeteksi kerentanan dalam sistem, dan memeriksa pengendalian akses untuk mencegah kerentanan tersebut telah diterapkan.

4. Kepatuhan terkait Audit Sistem Informasi

Proses Audit Sistem Informasi harus memperhatikan hal berikut:

a. Persyaratan audit harus disetujui oleh CISO Kementerian Perhubungan;
b. Ruang lingkup pemeriksaan/ audit harus disetujui dan dikendalikan oleh pihak berwenang;
c. Pemeriksaan perangkat lunak dan data harus dibatasi untuk akses baca saja (*read-only*);
d. Selain akses baca sajahanya diizinkan untuk salinan dari file sistem yang diisolasi, yang harus dihapus bila audit telah selesai,

atau diberikan perlindungan yang tepat jika ada kewajiban untuk menyimpan file tersebut di bawah persyaratan dokumentasi audit;

e. Sumber daya untuk melakukan pemeriksaan harus secara jelas diidentifikasi dan tersedia;
f. Persyaratan untuk pengolahan khusus atau tambahan harus diidentifikasi dan disepakati;
g. Semua akses harus dipantau dan dicatat untuk menghasilkan jejak audit, dan untuk data dan sistem informasi sensitif harus mempertimbangkan pencatatan waktu (*timesstamp*) pada jejak audit;
h. Semua prosedur, persyaratan dan tanggung jawab harus didokumentasikan; dan
i. Auditor harus independen dari kegiatan yang diaudit.

MENTERI PERHUBUNGAN
REPUBLIK INDONESIA,

ttd

BUDI KARYA SUMADI

Salinan sesuai dengan aslinya

KEPALA BIRO HUKUM

SRI LESTARI RAHAYU
Pembina Utama Muda (IV/c)
NIP. 19620620 198903 2 001