



KEPUTUSAN MENTERI HUKUM DAN HAK ASASI MANUSIA  
REPUBLIK INDONESIA  
NOMOR : M.HH-01.TI.06.02 TAHUN 2017  
TENTANG  
SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN  
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA

MENTERI HUKUM DAN HAK ASASI MANUSIA REPUBLIK INDONESIA,

- Menimbang : a. bahwa dalam rangka keamanan data dan informasi di Lingkungan Kementerian Hukum dan Hak Asasi Manusia, perlu menyusun sebuah standar mengenai manajemen keamanan informasi, agar kerahasiaan, integritas, dan ketersediaan informasi tetap terjaga;
- b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Keputusan Menteri Hukum dan Hak Asasi Manusia tentang Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Hukum dan Hak Asasi Manusia;
- Mengingat : 1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);
2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
3. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);

4. Peraturan Presiden Nomor 44 Tahun 2015 tentang Kementerian Hukum dan Hak Asasi Manusia (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 4843);
5. Peraturan Menteri Komunikasi dan Informatika Nomor 41/PER/M.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 4843);
6. Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 29 Tahun 2015 tentang Organisasi dan Tata Kerja Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia (Berita Negara Republik Indonesia Tahun 2015 Nomor 1473), sebagaimana diubah dengan Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 6 Tahun 2016 tentang Perubahan Atas Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor Nomor 29 Tahun 2015 tentang Organisasi dan Tata Kerja Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia (Berita Negara Republik Indonesia Tahun 2016 Nomor 186);
7. Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor Nomor 15 Tahun 2016 tentang Tata Naskah Dinas Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia (Berita Negara Republik Indonesia Tahun 2016 Nomor 533);

**MEMUTUSKAN:**

Menetapkan : KEPUTUSAN MENTERI HUKUM DAN HAK ASASI MANUSIA REPUBLIK INDONESIA TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA.

KESATU : Sistem Manajemen Keamanan Informasi ini bertujuan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi di Lingkungan Kementerian Hukum dan Hak Asasi Manusia.

KEDUA : Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Hukum dan Hak Asasi Manusia disusun dengan

sistematika sebagai berikut:

Bab I Pendahuluan

Bab II Tanggung Jawab

Bab III Standar

Bab IV Penutup

**KETIGA** : Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Hukum dan Hak Asasi Manusia sebagaimana dimaksud dalam Diktum Kedua, tercantum dalam lampiran yang merupakan bagian yang tidak terpisahkan dari Keputusan Menteri ini.

**KEEMPAT** : Keputusan Menteri Hukum dan Hak Asasi Manusia ini mulai berlaku sejak tanggal ditetapkan.

Ditetapkan di Jakarta,  
pada tanggal 12 Desember 2017

MENTERI HUKUM DAN HAK ASASI MANUSIA  
REPUBLIK INDONESIA,



LAMPIRAN  
KEPUTUSAN MENTERI HUKUM DAN HAK ASASI MANUSIA  
REPUBLIK INDONESIA  
NOMOR : M.HH-01.TI.06.02 TAHUN 2017  
TENTANG  
SISTEM MANAJEMEN KEAMANAN INFORMASI DI  
LINGKUNGAN KEMENTERIAN HUKUM DAN HAK ASASI  
MANUSIA

BAB I  
PENDAHULUAN

A. Latar Belakang

Keamanan informasi merupakan hal penting dalam penyelenggaraan layanan. Dengan semakin meningkatnya risiko dan insiden keamanan informasi dalam penyelenggaraan sistem elektronik, upaya pengamanan terhadap sistem elektronik yang memiliki data dan informasi strategis dan penting wajib segera dilakukan. Keamanan informasi yang handal, akan meningkatkan kepercayaan masyarakat terhadap penyelenggaraan sistem elektronik untuk pelayanan publik.

Sehubungan dengan hal tersebut, dalam rangka keamanan data dan informasi di lingkungan Kementerian Hukum dan Hak Asasi Manusia, perlu menyusun sebuah standar tentang manajemen keamanan informasi, yang mengatur bagaimana informasi menjadi aman agar kerahasiaan, integritas, dan ketersediaan informasi tetap terjaga.

B. Tujuan

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

### C. Ruang Lingkup

Standar ini berlaku untuk pengelolaan pengamanan seluruh informasi Kementerian Hukum dan Hak Asasi Manusia yang dilaksanakan oleh seluruh unit kerja Kementerian Hukum dan Hak Asasi Manusia dan pihak ketiga baik sebagai pengelola dan/atau pengguna Teknologi Informasi dan Komunikasi (TIK).

### D. Pengertian Umum

1. Akun adalah identifikasi pengguna yang diberikan oleh unit Pengelola TIK, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem TIK.
2. Akun khusus adalah akun yang diberikan oleh unit 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. *Audit logging* adalah catatan mengenai perubahan data dalam aplikasi, yang dicatat biasanya kolom mana yang berubah, siapa yang mengubah, diubah dari apa menjadi apa, kapan berubah
4. Aset fisik adalah jenis aset yang memiliki wujud fisik, misalnya perangkat komputer, perangkat jaringan dan komunikasi, media yang dapat dipindahkan, dan perangkat pendukung lainnya.
5. Aset informasi Kementerian Hukum dan Hak Asasi Manusia adalah aset dalam bentuk:
  - a. Data/dokumen, meliputi: data peraturan perundangan, data hak asasi manusia, data pemasyarakatan, data administrasi hukum umum, data imigrasi, data hak kekayaan intelektual, data gaji, data kepegawaian, data penawaran dan kontrak, dokumen perjanjian kerahasiaan, kebijakan kementerian, hasil penelitian, bahan pelatihan, prosedur operasional, rencana kelangsungan kegiatan, dan hasil audit;
  - 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, meliputi: pengetahuan, pengalaman, keahlian, citra, dan reputasi.

6. Aset tak berwujud adalah jenis aset yang tidak memiliki wujud fisik, misalnya pengetahuan, pengalaman, 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 40 (empat puluh tahun).
7. *Backup* adalah sebuah proses pembuatan gandaan/duplikat/cadangan dari aset informasi yang dilakukan sebagai upaya pengamanan dan pemulihan sebagai bagian dari manajemen risiko.
8. *Conduit* adalah sebuah tabung atau saluran untuk melindungi kabel yang biasanya terbuat dari baja.
9. Daftar inventaris aset informasi adalah kumpulan informasi yang memuat bentuk, pemilik, lokasi, retensi, dan hal-hal yang terkait dengan aset informasi.
10. *Denial of service* adalah suatu kondisi dimana sistem tidak dapat memberikan layanan secara normal, yang disebabkan oleh suatu proses yang diluar kendali baik dari dalam maupun dari luar sistem.
11. Direktori adalah penamaan koleksi file (biasanya berbentuk hirarki). Ini merupakan cara untuk mengelompokkan file sehingga mudah untuk dikelola.
12. Dokumen SMKI Kementerian Hukum dan Hak Asasi Manusia adalah dokumen terkait pelaksanaan SMKI yang meliputi antara lain dokumen standar, prosedur, dan catatan penerapan SMKI.
13. *Fallback* adalah suatu tindakan pembalikan/menarik diri dari posisi awal.
14. *Fault logging* adalah pencatatan permasalahan sistem informasi.
15. Hak akses khusus adalah akses terhadap sistem informasi sensitif, termasuk di dalamnya dan tidak terbatas pada sistem operasi, perangkat penyimpanan, *file server*, dan aplikasi-aplikasi sensitif. Hanya diberikan kepada pengguna yang membutuhkan, pemakainnya terbatas dan dikontrol.
16. *Hash totals* adalah nilai pemeriksa kesalahan yang diturunkan dari penambahan satu himpunan bilangan yang diambil dari data (tidak wajib berupa data numerik) yang diproses atau dimanipulasi dengan cara tertentu.

17. Kata sandi adalah serangkaian kode yang dibuat Pengguna, bersifat rahasia dan pribadi yang digunakan bersamaan dengan Akun Pengguna.
18. Keamanan informasi adalah perlindungan aset informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.
19. 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-SIRTII), Unit *cybercrime* POLRI, ISC2, ISACA.
20. Koneksi eksternal (*remote access*) adalah suatu akses jaringan komunikasi dari luar organisasi ke dalam organisasi.
21. 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 prinsip yaitu enkripsi dan dekripsi.
22. *Malicious code* adalah semua jenis program yang membahayakan termasuk makro atau *script* yang dapat dieksekusi dan dibuat dengan tujuan untuk merusak sistem komputer.
23. *Master disk* adalah media yang digunakan sebagai sumber dalam melakukan instalasi perangkat lunak.
24. *Mobile computing* adalah penggunaan perangkat komputasi yang dapat dipindah, misalnya *notebook* dan *personal data assistant* (PDA) untuk melakukan akses, pengolahan data, dan penyimpanan.
25. Penanggung jawab pengendalian dokumen adalah pihak yang memiliki kewenangan dan bertanggung jawab dalam proses pengendalian dokumen SMKI.
26. Pengguna adalah pegawai Kementerian Hukum dan Hak Asasi Manusia dan atau pihak ketiga serta tidak terbatas pada pengelola TIK dan kelompok kerja yang diberikan hak mengakses sistem TIK di lingkungan Kementerian Hukum dan Hak Asasi Manusia.
27. Pemilik aset informasi adalah unit kerja yang memiliki kewenangan terhadap aset informasi.

28. Pencatatan waktu (*timestamp*) adalah catatan waktu dalam tanggal dan/atau format waktu tertentu saat suatu aktivitas/transaksi terjadi. Format ini biasanya disajikan dalam format yang konsisten, yang memungkinkan untuk membandingkan dua aktivitas/transaksi yang berbeda berdasarkan dengan waktu.
29. Perangkat jaringan adalah peralatan jaringan komunikasi data seperti: *modem, hub, switch, router*, dan lain-lain.
30. Perangkat lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya.
31. Perangkat pendukung adalah peralatan pendukung untuk menjamin beroperasinya perangkat keras dan perangkat jaringan serta untuk melindunginya dari kerusakan. Contoh perangkat pendukung adalah *Uninterruptible Power Supply (UPS)*, pembangkit tenaga listrik/ generator, antena komunikasi.
32. Perangkat pengolah informasi adalah setiap sistem pengolah informasi, layanan atau infrastruktur seperti komputer, faksimili, telepon, mesin *fotocopy*.
33. Perjanjian *escrow* adalah perjanjian dengan pihak ketiga untuk memastikan apabila pihak ketiga tersebut bangkrut (mengalami *failure*) maka Kementerian Hukum dan Hak Asasi Manusia berhak untuk mendapatkan kode program (*source code*).
34. Perjanjian kerahasiaan adalah perikatan antara para pihak yang mencantumkan bahan rahasia, pengetahuan, atau informasi yang mana pihak-pihak ingin berbagi satu sama lain untuk tujuan tertentu, tetapi ingin membatasi akses dengan pihak lain.
35. Petugas Pelaksana Pengelolaan Proses Kelangsungan Kegiatan adalah pegawai yang ditunjuk oleh Pimpinan Unit Eselon I untuk mengelola proses kelangsungan kegiatan pada saat keadaan darurat.
36. Pihak ketiga adalah semua unsur di luar pengguna unit TIK Kementerian Hukum dan Hak Asasi Manusia yang bukan bagian dari Kementerian Hukum dan Hak Asasi Manusia, misal mitra kerja Kementerian Hukum dan Hak Asasi Manusia (seperti: konsultan, penyedia jasa komunikasi, pemasok dan pemelihara perangkat pengolah informasi), dan kementerian/lembaga lain.
37. Proses pendukung adalah proses-proses penunjang yang mendukung suatu proses utama yang terkait seperti proses pengujian perangkat lunak dan proses perubahan perangkat lunak.

38. 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.
39. *Rollback* adalah sebuah mekanisme yang digunakan untuk mengembalikan sistem ke kondisi semula sebelum perubahan diimplementasikan. Mekanisme ini biasanya terdapat pada basis data.
40. *Routing* adalah sebuah mekanisme yang digunakan untuk mengarahkan dan menentukan rute/jalur yang akan dilewati paket dari satu perangkat ke perangkat yang berada di jaringan lain.
41. Sanitasi adalah proses penghilangan informasi yang disimpan secara permanen dengan menggunakan medan magnet besar atau perusakan fisik.
42. Sistem Informasi adalah serangkaian perangkat keras, perangkat lunak, sumber daya manusia, serta prosedur dan atau aturan yang diorganisasikan secara terpadu untuk mengolah data menjadi informasi yang berguna untuk mencapai suatu tujuan.
43. 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.
44. *Sub network (subnet)* adalah pengelompokan secara logis dari perangkat jaringan yang terhubung.
45. *System administrator* adalah sebuah akun khusus untuk mengelola sistem informasi.
46. *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, seperti *memory*, *disk*, *printer*, dan sebagainya.
47. *Teleworking* adalah penggunaan teknologi telekomunikasi untuk memungkinkan pegawai bekerja di suatu lokasi yang berada di luar kantor untuk mengakses jaringan internal kantor.

## BAB II TANGGUNG JAWAB

### A. Umum

1. SMKI di Lingkungan Kementerian Hukum dan Hak Asasi Manusia dikoordinasikan oleh pejabat yang berperan sebagai *Chief Information Officer* (CIO) Kementerian Hukum dan Hak Asasi Manusia, yang sekaligus berperan sebagai *Chief Information Security Officer* (CISO) Kementerian Hukum dan Hak Asasi Manusia, dalam hal ini adalah Kepala Pusat Data dan Teknologi Informasi;
2. Seluruh Satuan Kerja wajib membentuk Satuan Tugas Keamanan Informasi, dibawah koordinasi Kepala Pusat Data dan Teknologi Informasi yang berperan sebagai CISO;
3. Satuan Kerja yang menyelenggarakan sistem elektronik dengan kategori tinggi atau strategis wajib menerapkan SMKI yang ditetapkan dalam Keputusan Menteri Hukum dan Hak Asasi Manusia;
4. Pimpinan Unit TIK bertanggung jawab mengawasi penerapan SMKI di Satuan Kerja masing-masing;
5. Unit TIK bertanggung jawab melaksanakan pengamanan aset informasi di Satuan Kerja masing-masing dengan mengacu pada SMKI;
6. Unit TIK bertanggung jawab meningkatkan pengetahuan, ketrampilan, dan kepedulian terhadap keamanan informasi pada seluruh pengguna di Satuan Kerja masing-masing;
7. Unit TIK menerapkan prinsip manajemen risiko dalam rangka pelaksanaan pengamanan dan perlindungan aset informasi dengan mengikuti ketentuan mengenai Penerapan Manajemen Risiko di Lingkungan Kementerian Hukum dan Hak Asasi Manusia;
8. Unit TIK melakukan evaluasi terhadap pelaksanaan SMKI secara berkala untuk menjamin efektivitas dan meningkatkan keamanan informasi;
9. Inspektorat Jenderal Kementerian Hukum dan Hak Asasi Manusia melakukan audit internal SMKI di lingkungan Kementerian Hukum dan Hak Asasi Manusia untuk memastikan pengendalian, proses dan prosedur SMKI dilaksanakan secara efektif dan dipelihara dengan baik;

10. Inspektorat Jenderal menunjuk pihak yang berkompeten untuk melakukan audit eksternal independen terhadap sistem keamanan manajemen informasi di Kementerian;
11. Unit TIK wajib menindaklanjuti laporan hasil audit SMKI.
12. Setiap laporan audit terkait keamanan teknologi informasi oleh Inspektorat Jenderal disampaikan ke Unit TIK untuk keperluan koordinasi.
13. Setiap Unit TIK wajib melaporkan kinerja SMKI kepada Kepala Pusat Data dan Teknologi Informasi sekali dalam setahun.

B. Pengendalian organisasi keamanan informasi

1. Unit TIK mengkaji perjanjian kerahasiaan pihak-pihak internal dan eksternal secara berkala untuk menjaga aset informasi;
2. Menjalin kerja sama dengan pihak-pihak berwenang di luar Kementerian Hukum dan Hak Asasi Manusia yang terkait dengan keamanan informasi;
3. Menjalin kerja sama dengan komunitas keamanan informasi di luar Kementerian Hukum dan Hak Asasi Manusia melalui pelatihan, seminar, atau forum lain yang relevan dengan keamanan informasi; dan
4. Menerapkan pengendalian keamanan informasi berdasarkan hasil penilaian risiko untuk mencegah atau mengurangi dampak risiko terkait dengan pemberian akses kepada pihak ketiga.

C. Pengendalian pengelolaan aset informasi

1. Setiap Unit TIK bertanggung jawab terhadap keamanan aset informasi:
  - a. Mengidentifikasi aset informasi dan mendokumentasikannya dalam daftar inventaris aset informasi;
  - b. Menetapkan pemilik aset informasi di setiap unit TIK
  - c. Menetapkan aset informasi yang terkait dengan perangkat pengolah informasi; dan
  - d. Pemilik aset informasi menetapkan aturan penggunaan aset informasi.
2. Klasifikasi aset informasi  
Aset informasi diklasifikasikan sesuai tingkat kerahasiaan, nilai, tingkat kritikalitas, serta aspek hukumnya;

D. Pengendalian keamanan informasi dari sisi sumber daya manusia:

1. Seluruh pegawai bertanggung jawab untuk menjaga keamanan informasi Kementerian Hukum dan Hak Asasi Manusia;
2. Pihak ketiga wajib menyetujui dan menandatangani syarat dan perjanjian untuk menjaga keamanan informasi Kementerian Hukum dan Hak Asasi Manusia;
3. Peran dan tanggung jawab pegawai dan pihak ketiga terhadap keamanan informasi harus didefinisikan, didokumentasikan, dan dikomunikasikan kepada yang bersangkutan;
4. Satuan kerja melakukan pemeriksaan data pribadi yang diberikan oleh pegawai baru dan pihak ketiga sesuai dengan ketentuan yang berlaku;
5. Seluruh pegawai wajib mendapatkan pendidikan/pelatihan/sosialisasi keamanan sistem informasi secara berkala sesuai tingkat tanggung jawabnya;
6. Pihak ketiga diberikan sosialisasi untuk meningkatkan kepedulian terhadap keamanan informasi (jika diperlukan);
7. Seluruh pegawai dan pihak ketiga yang melanggar SMKI di lingkungan Kementerian Hukum dan Hak Asasi Manusia akan diberikan sanksi atau tindakan disiplin sesuai dengan ketentuan yang berlaku;
8. Kepatuhan pegawai terhadap SMKI di lingkungan Kementerian Hukum dan Hak Asasi Manusia wajib diawasi oleh atasan masing-masing;
9. Pegawai yang berhenti bekerja atau mutasi wajib mengembalikan seluruh aset informasi yang dipergunakan selama bekerja sesuai dengan ketentuan yang berlaku;
10. Pihak ketiga yang habis masa kontrak kerjanya wajib mengembalikan seluruh aset informasi yang dipergunakan selama bekerja di Kementerian Hukum dan Hak Asasi Manusia;
11. Satuan kerja wajib menghentikan hak penggunaan aset informasi bagi pegawai yang sedang dalam pemeriksaan dan/atau menjalani proses hukum terkait dengan dugaan pelanggaran SMKI di lingkungan Kementerian Hukum dan Hak Asasi Manusia; dan
12. Satuan kerja wajib mencabut hak akses terhadap akses informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi bekerja di Kementerian Hukum dan Hak Asasi Manusia.

## E. Pengendalian Keamanan Fisik dan Lingkungan

### 1. Pengamanan area

- a. Seluruh pegawai, pihak ketiga, dan tamu yang memasuki lingkungan area Pusat Data/Ruang Server wajib mematuhi aturan yang berlaku di Kementerian Hukum dan Hak Asasi Manusia;
- b. Ketentuan rinci tentang pengamanan area lingkungan kerja di Kementerian Hukum dan Hak Asasi Manusia diuraikan dalam standar keamanan fisik dan lingkungan.

### 2. Pengamanan perangkat

- a. Perangkat pengolah informasi dan perangkat pendukung wajib ditempatkan di lokasi yang aman dan diposisikan sedemikian rupa untuk mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang.
- b. Perangkat pendukung wajib dipasang untuk menjamin beroperasinya perangkat pengolah informasi dan secara berkala wajib diperiksa dan diuji ulang kinerjanya.
- c. Kabel sumber daya listrik wajib dilindungi dari kerusakan, dan kabel telekomunikasi yang mengalirkan informasi wajib dilindungi dari kerusakan dan penyadapan.
- d. Perangkat pengolah informasi wajib dipelihara secara berkala untuk menjamin ketersediaan, keutuhan, dan fungsinya.
- e. Penggunaan perangkat yang dibawa ke luar dari lingkungan Kementerian Hukum dan Hak Asasi Manusia wajib disetujui oleh Pejabat yang berwenang
- f. Perangkat pengolah informasi penyimpan data yang sudah tidak digunakan lagi wajib disanitasi sebelum digunakan kembali atau dihapuskan/dimusnahkan;
- g. Penanganan perangkat pengolah informasi penyimpan data di Kementerian Hukum dan Hak Asasi Manusia sesuai dengan standar penanganan media penyimpan data yang ditetapkan dalam Standar Pengelolaan Data Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia.

## F. Pengendalian pengelolaan operasional

### 1. Prosedur operasional dan tanggung jawab

- a. Wajib mendokumentasikan, memelihara, dan menyediakan seluruh prosedur operasional yang terkait dengan penggunaan perangkat pengolah informasi sesuai dengan peruntukannya.

- b. Mengendalikan perubahan terhadap perangkat pengolah informasi.
  - c. Melakukan pemisahan informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA untuk menghindari adanya pegawai yang memiliki pengendalian eksklusif terhadap seluruh aset informasi dan perangkat pengolahnya.
  - d. 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. Wajib 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. Wajib melakukan pemantauan terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh pihak ketiga secara berkala.
  - c. Wajib memperhatikan kritikalitas, proses yang terkait dan hasil penilaian ulang risiko layanan apabila terjadi perubahan pada layanan yang disediakan pihak ketiga.
3. Perencanaan dan penerimaan sistem
- a. Unit TIK wajib memantau penggunaan perangkat pengolah informasi dan membuat perkiraan pertumbuhan kebutuhan ke depan untuk memastikan ketersediaan kapasitas;
  - b. Unit TIK wajib menetapkan kriteria penerimaan untuk sistem informasi baru, pemutakhiran dan versi baru serta melakukan pengujian sebelum penerimaan.
4. Perlindungan terhadap ancaman program yang membahayakan.
- Wajib menerapkan sistem yang dapat melakukan pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan'
5. *Backup*
- a. Wajib melakukan *backup* informasi dan perangkat lunak yang berada di Pusat Data secara berkala.
  - b. Proses *backup* di Kementerian Hukum dan Hak Asasi Manusia sesuai dengan *backup* data yang ditetapkan dalam Standar Pengelolaan Data Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia.

6. Pengelolaan keamanan jaringan
  - a. Wajib mengelola dan melindungi jaringan dari berbagai bentuk ancaman;
  - b. Wajib 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. Setiap Unit TIK mempunyai prosedur yang mengatur penanganan media penyimpan data untuk melindungi aset informasi;
  - b. Penanganan media penyimpanan data di Kementerian Hukum dan Hak Asasi Manusia sesuai dengan standar penanganan media penyimpan data yang ditetapkan dalam Standar Pengelolaan Data Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia.
8. Pertukaran informasi
  - a. Pertukaran informasi dan perangkat lunak antara Kementerian Hukum dan Hak Asasi Manusia dengan pihak ketiga dilakukan atas kesepakatan tertulis kedua belah pihak;
  - b. Pemilik informasi wajib melakukan penilaian risiko yang memadai sebelum melaksanakan pertukaran informasi;
  - c. Wajib 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;
9. Pemantauan
  - a. Wajib 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. Wajib memantau penggunaan sistem dan mengkaji secara berkala hasil kegiatan pemantauan.
  - c. Wajib melindungi fasilitas pencatatan dan data yang dicatat dari kerusakan dan akses oleh pihak yang tidak berwenang.
  - d. Wajib menerapkan pencatatan kegiatan *system administrator* dan *system operator*.
  - e. Wajib menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindakan penanganan yang tepat.

- f. Wajib memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.

#### G. Pengendalian akses

1. Wajib menyusun, mendokumentasikan, dan mengkaji ketentuan akses ke aset informasi berdasarkan kebutuhan organisasi dan persyaratan keamanan.
2. Pengelolaan akses pengguna
  - a. Wajib menyusun prosedur pengelolaan hak akses pengguna sesuai dengan peruntukannya.
  - b. Wajib membatasi dan mengendalikan penggunaan hak akses khusus.
  - c. Wajib mengatur pengelolaan kata sandi pengguna;
  - d. Wajib memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya.
3. Tanggung jawab pengguna
  - a. Wajib mematuhi aturan pembuatan dan penggunaan kata sandi.
  - b. Memastikan perangkat pengolah informasi yang digunakan mendapatkan perlindungan terutama saat ditinggalkan; dan
  - c. Melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang.
4. Pengendalian akses jaringan
  - a. Wajib mengatur akses pengguna dalam mengakses jaringan Kementerian Hukum dan Hak Asasi Manusia sesuai dengan peruntukannya;
  - b. Wajib menerapkan proses otorisasi pengguna untuk setiap akses ke dalam jaringan internal melalui koneksi eksternal;
  - c. Akses ke perangkat keras dan perangkat lunak untuk diagnosa harus dikontrol berdasarkan prosedur dan hanya digunakan oleh pegawai yang diberikan wewenang untuk melakukan pengujian, pemecahan masalah, serta pengembangan system, dan *port* pada fasilitas jaringan yang tidak dibutuhkan dalam kegiatan atau fungsi layanan wajib dinonaktifkan.
  - d. Wajib memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi.
  - e. Wajib menerapkan mekanisme pengendalian akses pengguna sesuai dengan persyaratan pengendalian akses.

- f. Pengendalian *routing* jaringan internal Kementerian Hukum dan Hak Asasi Manusia wajib dilakukan sesuai pengendalian akses dan kebutuhan layanan informasi.
5. Pengendalian akses ke sistem operasi
    - a. Akses ke sistem operasi wajib dikontrol dengan menggunakan prosedur akses yang aman.
    - b. Setiap pengguna wajib memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya, dan proses otorisasi pengguna wajib menggunakan teknik autentikasi yang sesuai untuk memvalidasi identitas dari pengguna.
    - c. Sistem pengelolaan kata sandi wajib mudah untuk digunakan dan dapat memastikan kualitas sandi yang dibuat pengguna.
    - d. Wajib membatasi dan mengendalikan penggunaan *system utilities*;
    - e. Fasilitas *session time-out* wajib diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu.
    - f. Wajib membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA.
  6. Pengendalian akses ke aplikasi dan sistem informasi:
    - a. Wajib 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 wajib diletakkan pada lokasi terpisah untuk mengurangi kemungkinan diakses oleh pihak yang tidak berwenang.
  7. *Mobile computing* dan *teleworking*
    - a. Membangun kepedulian pengguna perangkat *mobile computing* dan *Teleworking* akan risiko-risiko keamanan yang terus meningkat terhadap informasi yang tersimpan dalam perangkat *mobile computing*;
    - b. Pengguna perangkat *mobile computing* dan *teleworking* wajib mengikuti prosedur yang terkait penggunaan perangkat *mobile computing* dan *teleworking* untuk menjaga keamanan perangkat dan informasi di dalamnya.

- H. Pengendalian keamanan informasi dalam pengadaan, pengembangan, dan pemeliharaan sistem informasi
1. Menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi yang relevan sebelum pengadaan, pengembangan, atau pemeliharaan sistem informasi baru.
  2. Pengelolaan informasi pada aplikasi:
    - a. Data yang akan dimasukkan ke aplikasi wajib diperiksa terlebih dahulu kebenaran dan kesesuaiannya.
    - b. Setiap aplikasi wajib disertakan proses validasi untuk mendeteksi bahwa informasi yang dihasilkan utuh dan sesuai dengan yang diharapkan.
    - c. Data keluaran aplikasi wajib divalidasi untuk memastikan data yang dihasilkan adalah benar.
  3. Pengendalian penggunaan kriptografi:
    - a. Wajib mengembangkan dan menerapkan sistem kriptografi untuk perlindungan informasi dan membuat rekomendasi yang tepat bagi penerapannya.
    - b. Sistem kriptografi wajib digunakan untuk melindungi aset informasi yang memiliki klasifikasi SANGAT RAHASIA, RAHASIA, dan TERBATAS.
  4. Keamanan file sistem
    - a. Wajib mempunyai prosedur untuk pengendalian perangkat lunak pada sistem operasional.
    - b. Menentukan sistem pengujian data, melindunginya dari kemungkinan kerusakan, kehilangan atau perubahan oleh pihak yang tidak berwenang.
    - c. Mengendalikan ke kode program secara ketat dan salinan versi terkini dari perangkat lunak disimpan di tempat yang aman.
  5. Keamanan dalam proses pengembangan dan pendukung
    - a. Wajib mengendalikan perubahan pada sistem operasi dengan penggunaan prosedur pengendalian perubahan.
    - b. Wajib mengendalikan perubahan terhadap perangkat lunak yang dikembangkan sendiri maupun pihak ketiga.
    - c. Wajib meninjau dan menguji sistem operasi dan/atau perangkat lunak untuk memastikan tidak ada dampak merugikan pada proses operasional atau keamanan informasi Kementerian Hukum dan Hak Asasi Manusia pada saat terjadi perubahan sistem operasi dan/atau perangkat lunak, untuk informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA.

- d. Wajib mencegah kemungkinan terjadinya kebocoran informasi.
  - e. Wajib melakukan supervisi dan memantau pengembangan perangkat lunak oleh pihak ketiga.
6. Pengelolaan kerentanan teknis
- a. Wajib mengumpulkan informasi kerentanan teknis secara berkala dari seluruh sistem informasi yang digunakan maupun komponen pendukung sistem informasi.
  - b. Wajib melakukan evaluasi dan penilaian risiko terhadap kerentanan teknis yang ditemukan dalam sistem informasi serta menetapkan pengendalian yang tepat terhadap risiko terkait.
- I. Pengendalian pengelolaan gangguan keamanan informasi
- 1. Pegawai dan pihak ketiga wajib melaporkan kepada unit TIK sesegera mungkin pada saat memenuhi kelemahan atau terjadi gangguan keamanan informasi dalam sistem atau layanan TIK Kementerian Hukum dan Hak Asasi Manusia.
  - 2. Pengelolaan gangguan keamanan informasi dan perbaikannya
    - a. Masing-masing wajib menyusun prosedur dan menguraikan tanggung jawab pegawai, terkait dalam rangka memastikan gangguan keamanan informasi dapat ditangani secara cepat dan efektif.
    - b. Seluruh gangguan keamanan informasi yang terjadi wajib dicatat dalam suatu basis data dan/atau buku catatan pelaporan gangguan keamanan informasi, yang menjadi masukan pada proses peningkatan penanganan gangguan keamanan informasi, serta dievaluasi dan dianalisa untuk perbaikan dan pencegahan agar gangguan keamanan informasi tidak terulang.
    - c. Mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap SMKI di Lingkungan Kementerian Hukum dan Hak Asasi Manusia.
- J. Pengendalian keamanan informasi dalam pengelolaan kelangsungan kegiatan
- 1. Wajib mengelola proses kelangsungan kegiatan pada saat keadaan darurat di lingkungan unit eselon I masing-masing;
  - 2. Mendefinisikan risiko, dan menganalisis dampak yang diakibatkan pada saat terjadi keadaan darurat untuk menjamin kelangsungan kegiatan;

3. Menyusun dan menerapkan Rencana Kelangsungan Kegiatan untuk menjaga dan mengembalikan kegiatan operasional dalam jangka waktu yang disepakati dan level yang dibutuhkan;
4. Memelihara dan memastikan rencana-rencana yang termuat dalam Rencana Kelangsungan Kegiatan masih sesuai, dan mengidentifikasi prioritas untuk kegiatan uji coba;
5. Melakukan uji coba Rencana Kelangsungan Kegiatan secara berkala untuk memastikan Rencana Kelangsungan Kegiatan dapat dilaksanakan secara efektif.

#### K. Pengendalian kepatuhan

1. Kepatuhan terhadap peraturan perundang-undangan
  - a. Seluruh pegawai dan pihak ketiga wajib menaati peraturan perundang-undangan yang terkait dengan dengan keamanan informasi ;
  - b. Mengidentifikasi, mendokumentasikan, dan memelihara kemutakhiran semua peraturan perundang-undangan yang terkait dengan sistem keamanan informasi.
  - c. Perangkat lunak yang dikelola unit TIK wajib mematuhi ketentuan penggunaan lisensi. Pengadaan perangkat lunak secara tidak sah tidak diizinkan dan merupakan bentuk pelanggaran.
  - d. Rekaman milik Kementerian Hukum dan Hak Asasi Manusia wajib dilindungi dari kehilangan, kerusakan atau penyalahgunaan.
  - e. Wajib melindungi kepemilikan dan kerahasiaan data. Data hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundang-undangan dan kesepakatan.
2. Kepatuhan teknis

Wajib melakukan pemeriksaan kepatuhan teknis secara berkala secara berkala untuk menjamin efektivitas standar dan prosedur keamanan informasi yang ada di area operasional.
3. Audit sistem informasi
  - a. Unit TIK bersama dengan Inspektorat Jenderal wajib membuat perencanaan persyaratan, ruang lingkup, dan kegiatan audit yang melibatkan pemeriksaan sistem operasional untuk mengurangi kemungkinan risiko gangguan yang bisa terjadi terhadap kegiatan Kementerian Hukum dan Hak Asasi Manusia selama proses audit;

- b. Penggunaan alat bantu (baik perangkat lunak maupun perangkat keras) untuk mengetahui kelemahan keamanan, memindai kata sandi, atau untuk melemahkan dan menerobos sistem keamanan informasi tidak diizinkan;
- c. Audit sistem informasi di Kementerian Hukum dan Hak Asasi Manusia akan ditetapkan dalam ketentuan tersendiri.

## BAB III STANDAR

### A. Umum

1. Penerapan kebijakan SMKI di Lingkungan Kementerian Hukum dan Hak Asasi Manusia
  - a. Wajib menggunakan catatan penerapan untuk mengukur kepatuhan dan efektivitas penerapan SMKI;
  - b. Catatan penerapan SMKI sebagaimana tersebut dalam angka 1, 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; dan
    - 7) Laporan Audit.
2. Penyusunan dokumen pendukung kebijakan keamanan informasi wajib memuat:
  - a. Tujuan dan ruang lingkup dokumen pendukung kebijakan keamanan informasi;
  - b. Kerangka kerja setiap tujuan/sasaran pengendalian keamanan informasi;
  - c. Metodologi penilaian risiko;
  - d. Penjelasan singkat mengenai standar, prosedur, dan kepatuhan termasuk persyaratan peraturan yang wajib dipenuhi, pengelolaan kelangsungan kegiatan, konsekuensi apabila terjadi pelanggaran.
3. Pengendalian dokumen
  - a. Wajib mengendalikan dokumen SMKI Kementerian Hukum dan Hak Asasi Manusia untuk menjaga kemutakhiran dokumen, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan dan mencegah akses oleh pihak yang tidak berwenang.
  - b. Menempatkan dokumen SMKI Kementerian Hukum dan Hak Asasi Manusia di semua area operasional sehingga mudah diakses oleh pengguna di unit kerja masing-masing sesuai peruntukannya.

B. Pengendalian organisasi keamanan informasi

1. Kepala Pusat Data dan Teknologi Informasi sebagai pejabat yang berperan sebagai CISO Kementerian Hukum dan Hak Asasi Manusia bertanggung jawab untuk:
  - a. Mengkoordinasikan perumusan dan penyempurnaan SMKI di Lingkungan Kementerian Hukum dan Hak Asasi Manusia;
  - b. Memelihara dan mengendalikan penerapan SMKI di seluruh area yang menjadi tujuan sasaran pengendalian;
  - c. Menetapkan target keamanan informasi setiap tahunnya serta menyusun rencana kerja;
  - d. Memastikan efektivitas dan konsistensi penerapan SMKI serta mengukur kinerja keseluruhan; dan
  - e. Melaporkan kinerja penerapan SMKI di Lingkungan Kementerian Hukum dan Hak Asasi Manusia serta pencapaian target kepada Komite TIK Kementerian Hukum dan Hak Asasi Manusia.
2. Satuan Tugas Keamanan Informasi bertanggung jawab untuk:
  - a. Memastikan SMKI di Lingkungan Kementerian Hukum dan Hak Asasi Manusia diterapkan secara efektif;
  - b. Memastikan langkah-langkah perbaikan sudah dilakukan berdasarkan saran dan rekomendasi yang diberikan dalam pelaksanaan evaluasi dan/atau audit penerapan SMKI;
  - c. Memastikan peningkatan kesadaran, kepedulian, dan kepatuhan seluruh pegawai terhadap SMKI;
  - d. Melaporkan kinerja penerapan SMKI sesuai ruang lingkup tanggung jawabnya kepada Kepala Pusat Data dan Teknologi Informasi sebagai pejabat yang berperan sebagai CISO, untuk digunakan sebagai dasar peningkatan keamanan informasi;
  - e. Mengkoordinasikan penanganan gangguan keamanan informasi di tingkat Kementerian Hukum dan Hak Asasi Manusia; dan
  - f. Memastikan terlaksananya audit internal terhadap penerapan SMKI paling sedikit 1(satu) kali dalam 3 (tiga) tahun.

C. Pengendalian pengelolaan aset informasi

1. Pemilik Aset Informasi menetapkan dan mengkaji secara berkala klasifikasi aset informasi dan jenis perlindungan keamanannya.
2. Pemilik Aset Informasi menetapkan pihak yang berwenang untuk mengakses aset informasi.
3. Aset informasi Kementerian Hukum dan Hak Asasi Manusia diklasifikasikan seperti berikut:

- a. SANGAT RAHASIA, yaitu aset informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menyebabkan kerugian akan ketahanan hukum dan hak asasi manusia nasional;
- b. RAHASIA, yaitu aset informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu kelancaran kegiatan atau mengganggu citra dan reputasi Kementerian Hukum dan Hak Asasi Manusia dan/atau yang menurut peraturan perundang-undangan dinyatakan rahasia;
- c. TERBATAS, yaitu aset informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu kelancaran kegiatan Kementerian Hukum dan Hak Asasi Manusia tetapi tidak akan mengganggu citra dan reputasi Kementerian Hukum dan Hak Asasi Manusia;
- d. PUBLIK, yaitu aset informasi yang secara sengaja disediakan Kementerian Hukum dan Hak Asasi Manusia untuk dapat diketahui masyarakat umum.

D. Pengendalian keamanan sumber daya manusia

Keamanan sumber daya manusia meliputi:

1. Peran dan tanggung jawab pegawai terhadap keamanan informasi adalah menjadi bagian dari penjabaran tugas dan fungsi, khususnya bagi yang memiliki akses terhadap aset informasi;
2. Pimpinan dari pegawai berkeahlian khusus atau yang berbeda di posisi kunci wajib memastikan ketersediaan pengganti pegawai tersebut dengan kompetensi yang setara apabila pegawai yang bersangkutan mutasi/berhenti;
3. Pemeriksaan latar belakang calon pegawai dan pihak ketiga Kementerian Hukum dan Hak Asasi Manusia wajib memperhitungkan privasi, perlindungan data pribadi dan/atau pekerjaan, 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; dan
  - d. Pemeriksaan lebih rinci, seperti pemeriksaan kredit atau pemeriksaan dari catatan kriminal.

E. Pengendalian keamanan fisik dan lingkungan

1. Perangkat wajib dipelihara sesuai dengan petunjuk manualnya.
2. Untuk pemeliharaan yang dilakukan oleh pihak ketiga, wajib diadakan Perjanjian Tingkat Layanan (*Service Level Agreement/SLA*) yang mendefinisikan tingkat pemeliharaan yang disediakan dan tingkat kinerja yang wajib dipenuhi pihak ketiga.
3. Dalam hal pemeliharaan perangkat dan tidak dapat dilakukan di tempat, maka pemindahan perangkat wajib mendapatkan persetujuan Pejabat yang berwenang. Terhadap data yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA yang disimpan dalam perangkat tersebut wajib dipindahkan terlebih dahulu.
4. Otorisasi penggunaan perangkat wajib dilakukan secara tertulis dan data-data yang terkait dengan aset informasi yang digunakan, seperti nama pemakai aset, dan tujuan penggunaan aset, wajib dicatat dan disimpan.
5. Pengamanan Area:
  - a. 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 klasifikasi SANGAT RAHASIA dan RAHASIA wajib dibatasi dan hanya diberikan kepada pegawai yang diberi wewenang;
  - c. Pihak ketiga yang memasuki ruang *server*, pusat data, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA wajib didampingi oleh pegawai unit TIK sepanjang waktu kunjungan.
  - d. Kantor, ruangan, dan perangkat yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA wajib 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 wajib selalu dijaga, diawasi dan dikendalikan, dan jika memungkinkan disterilkan dari perangkat pengolah informasi untuk menghindari akses dari pihak yang tidak berwenang.

6. Pengamanan kantor, ruangan, dan fasilitas:
  - a. Pengamanan kantor, ruangan, dan fasilitas wajib sesuai dengan peraturan dan standar keamanan dan keselamatan kerja yang berlaku;
  - b. Fasilitas utama wajib 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:
  - a. Bahan-bahan berbahaya atau mudah terbakar wajib disimpan pada jarak yang aman dari *batas aman*;
  - b. Perlengkapan umum seperti alat tulis tidak boleh disimpan di dalam *batas aman*;
  - c. Perangkat *pemulihan* dan media *backup* wajib diletakkan pada jarak yang aman untuk menghindari kerusakan dari bencana yang mempengaruhi fasilitas utama; dan
  - d. Perangkat pemadam kebakaran wajib disediakan dan diletakkan di tempat yang tepat.
8. Penempatan dan perlindungan perangkat:
  - a. Perangkat wajib diletakkan pada lokasi yang meminimalkan akses yang tidak perlu ke dalam area kerja;
  - b. Perangkat pengolah informasi yang menangani informasi sensitif wajib diposisikan dan dibatasi arah sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak yang tidak berwenang selama digunakan, untuk menghindari akses oleh pihak yang tidak berwenang;
  - c. Perangkat yang memerlukan perlindungan khusus seperti perangkat cetak khusus, perangkat jaringan di luar ruang *server* wajib 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 kerusakan;
  - e. Kondisi lingkungan, seperti suhu dan kelembaban wajib dimonitor untuk mencegah perubahan kondisi yang dapat mempengaruhi pengoperasian perangkat pengolah informasi;

- f. Perlindungan petir wajib diterapkan untuk semua bangunan dan filter perlindungan petir wajib dipasang untuk semua jalur komunikasi dan listrik; dan
  - g. Perangkat pengolah informasi sensitif wajib dilindungi untuk meminimalkan risiko kebocoran informasi.
9. Pengamanan kabel
- a. Pemasangan kabel sumber daya listrik dan kabel telekomunikasi ke perangkat pengolah informasi selama memungkinkan wajib terletak di bawah tanah, atau menerapkan alternatif perlindungan lain yang memadai;
  - b. Pemasangan kabel jaringan wajib 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 wajib 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 optic*;
    - 5) Penggunaan lapisan elektromagnet untuk melindungi kabel;
    - 6) Inisiasi penghapusan teknikal 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.

F. Pengendalian pengelolaan komunikasi dan operasional

- 1. Dokumentasi prosedur operasional, mencakup:
  - a. Tata cara pengolahan dan penanganan informasi;
  - b. Tata cara menangani masalah atau kondisi khusus yang terjadi beserta pihak yang wajib 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 pengguna dan catatan kejadian/kegiatan sistem.
2. Pemisahan perangkat pengembangan dan operasional
- a. Pengembangan dan operasional perangkat lunak wajib dioperasikan di sistem atau prosesor komputer dan *domain* atau direktori yang berbeda;
  - b. Instruksi kerja rilis dari pengembangan perangkat lunak ke operasional wajib ditetapkan dan didokumentasikan;
  - c. *Compiler*, *editor*, dan alat bantu pengembangan lain tidak boleh diakses dari sistem operasional ketika tidak dibutuhkan;
  - d. Lingkungan sistem pengujian wajib diusahakan sama dengan lingkungan sistem operasional;
  - e. Pengguna wajib menggunakan profil pengguna yang berbeda untuk sistem pengujian dan sistem operasional, serta aplikasi wajib 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, meliputi :
- 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 Hukum dan Hak Asasi Manusia;
  - c. Pengendalian dan pengaturan akses ke sistem jaringan internal atau eksternal Kementerian Hukum dan Hak Asasi Manusia;
  - d. Pencatatan informasi pihak ketiga yang diizinkan mengakses ke jaringan Kementerian Hukum dan Hak Asasi Manusia 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; dan
    - 3) Pendokumentasian arsitektur jaringan seluruh komponen perangkat keras jaringan dan perangkat lunak.
  - g. Penerapan fitur keamanan layanan jaringan mencakup:
    - 1) Teknologi keamanan seperti autentifikasi, 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 mencakup:
    - 1) Perlindungan pertukaran informasi dari pencetakan, penyalinan, modifikasi, *miss-routing*, dan perusakan;
    - 2) Pendeteksian dan perlindungan terhadap kode berbahaya yang dapat dikirim melalui penggunaan sistem 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 sistem elektronik, mengacu pada ketentuan yang berlaku.

- c. Pengendalian pertukaran informasi bila menggunakan sistem 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 otomatis;
  - 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 Hukum dan Hak Asasi Manusia bagi masyarakat umum wajib disetujui oleh pemilik informasi dan sesuai dengan kebutuhan 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
- b. Pola-pola *log-on* yang mengindikasikan penggunaan yang tidak wajar;
- c. Alokasi dan penggunaan hak akses khusus
- d. Penelusuran transaksi dari pengiriman *file* tertentu yang mencurigakan; dan
- e. Penggunaan sumber daya sensitif.

#### G. Pengendalian akses

- 1. Persyaratan untuk pengendalian akses
  - a. Penentuan kebutuhan keamanan dari pengolah aset informasi;

- b. Pemisahan peran pengendalian akses, seperti administrasi akses dan otorisasi akses.
2. Pengelolaan akses pengguna
    - a. Penggunaan akun yang unik untuk mengaktifkan pengguna agar terhubung dengan sistem informasi atau layanan, dan pengguna dapat bertanggungjawab dalam penggunaan sistem informasi atau layanan tersebut. Penggunaan akun khusus hanya diperbolehkan sebatas yang diperlukan untuk kegiatan atau alasan operasional, dan wajib disetujui Pejabat yang berwenang serta didokumentasikan;
    - b. Pemeriksaan bahwa pengguna memiliki otoritas dari pemilik sistem untuk menggunakan informasi atau layanan, dan jika diperlukan wajib mendapat persetujuan yang terpisah dari Pejabat yang berwenang;
    - c. Pemeriksaan bahwa tingkat akses yang diberikan sesuai dengan tujuan kegiatan dan konsisten dengan SMKI di Lingkungan Kementerian Hukum dan Hak Asasi Manusia;
    - 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 bebas 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
    - 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 peruntukannya 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*) wajib diutamakan untuk menghindari kebutuhan dalam memberikan hak akses khusus secara terus menerus kepada pengguna;
  - e. Hak akses khusus wajib diberikan secara terpisah dari akun yang digunakan untuk kegiatan umum, seperti akun *system administrator*, *database administrator*, dan *network administrator*.
4. Kajian hak akses pengguna
- a. Hak akses pengguna wajib dikaji ulang paling sedikit 6 (enam) bulan sekali atau setelah terjadi perubahan pada sistem, atau struktur organisasi;
  - b. Hak akses khusus wajib dikaji ulang paling sedikit 6 (enam) bulan sekali dalam jangka waktu lebih sering dibandingkan jangka waktu pengkajian hak akses pengguna, atau apabila terjadi perubahan pada sistem, atau struktur organisasi;
  - c. Pemeriksaan hak akses khusus wajib 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
- a. Pemisahan berdasarkan kelompok layanan informasi, pengguna, dan aplikasi;
  - b. Pemberian akses jaringan kepada tamu, hanya dapat diberikan akses terbatas misalnya internet dan/atau surat elektronik tanpa bisa terhubung ke jaringan internal Kementerian Hukum dan Hak Asasi Manusia.
7. *Mobile computing* dan *teleworking*
- a. Penggunaan perangkat *mobile computing* dan *teleworking* wajib mempertimbangkan:

- 1) Memenuhi keamanan informasi dalam penentuan lokasi;
  - 2) Menjaga keamanan akses;
  - 3) Menggunakan anti *malicious code*;
  - 4) Memakai perangkat lunak berlisensi; dan
  - 5) Mendapatkan persetujuan Pejabat yang berwenang/atasan langsung pegawai.
- b. Pencabutan hak akses dan pengembalian fasilitas perangkat *teleworking* apabila kegiatan telah selesai.
- H. Pengendalian keamanan informasi dalam pengadaan, pengembangan, dan pemeliharaan sistem informasi
1. Spesifikasi kebutuhan perangkat pengolah informasi yang dikembangkan oleh internal atau pihak ketiga wajib didokumentasikan secara formal;
  2. Pengembangan Sistem Informasi wajib mengikuti standar keamanan yang ditetapkan oleh Unit TIK.
  3. Pengendalian dan penggunaan kriptografi
    - a. Unit TIK menetapkan standar kriptografi yang digunakan Kementerian
    - b. Penggunaan kriptografi untuk keperluan tertentu oleh Satuan Kerja wajib mendapat persetujuan Unit TIK yang kemudian akan menjadi bagian dari standar yang ada.
    - c. Pihak yang diberi wewenang untuk mengelola kunci kriptografi yang digunakan ditetapkan oleh Menteri.
    - d. Pengamanan kunci kriptografi wajib dikoordinasikan dengan Pusat Data dan Teknologi Informasi
  4. Keamanan file sistem
    - a. Pengembangan prosedur pengendalian perangkat lunak pada sistem operasional wajib 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 atau *compiler*;
      - 3) Aplikasi dan perangkat lunak sistem operasi hanya dapat diimplementasikan setelah melewati proses pengujian yang ekstensif;

- 4) Sistem pengendalian konfigurasi wajib digunakan untuk mengendalikan seluruh perangkat lunak yang telah diimplementasikan beserta dokumentasi sistem;
  - 5) Sistem *rollback* wajib tersedia sebelum suatu perubahan diimplementasikan;
  - 6) Catatan audit wajib dipelihara untuk menjaga kemutakhiran *library* program operasional;
  - 7) Versi terdahulu dari suatu aplikasi wajib tetap disimpan untuk keperluan kontijensi; dan
  - 8) Versi lama dari suatu perangkat lunak wajib diarsip, bersama dengan informasi terkait dan prosedur, parameter, konfigurasi rinci, dan perangkat lunak pendukung.
- b. Perlindungan terhadap sistem pengujian data wajib mempertimbangkan:
- 1) Prosedur pengendalian akses, yang berlaku pada sistem aplikasi operasional, wajib 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 wajib mempertimbangkan:
- 1) Kode program tidak boleh disimpan pada sistem operasional;
  - 2) Pengelolaan kode program dan *library* wajib mengikuti prosedur yang telah ditetapkan;
  - 3) Pengelola TIK tidak boleh memiliki akses yang tidak terbatas ke kode program dan *library*;
  - 4) Proses pemutakhiran kode program dan item terkait, serta pemberian kode program kepada *programmer* hanya dapat dilakukan setelah melalui proses otorisasi;
  - 5) *Listing program* wajib disimpan dalam *secure areas*;
  - 6) Catatan audit dari seluruh akses ke kode program *library* wajib dipelihara; dan
  - 7) Pemeliharaan dan penyalinan kode program *library* wajib mengikuti prosedur pengendalian perubahan.

5. Keamanan dalam proses pengembangan dan pendukung
  - 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 mengganggu 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;
    - 2) Memastikan rencana dan anggaran *annual support* yang mencakup reviu dan *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;
  - 2) Melakukan pemantauan terhadap aktivitas penggunaan desktop dan perangkat *mobile*.
- d. Pengembangan perangkat lunak oleh pihak ketiga wajib mempertimbangkan:
- 1) Perjanjian lisensi, kepemilikan kode program, dan Hak Atas Kekayaan Intelektual (HAKI);
  - 2) Perjanjian *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 wajib 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 bekerja secara efektif dan tidak menimbulkan risiko yang lain. Apabila *patch* tidak tersedia, wajib 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; dan
    - 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 wajib dilakukan secara berkala; dan
- g. Pengelolaan kerentanan teknis diutamakan terhadap sistem informasi yang memiliki tingkat risiko tinggi.

I. Pengendalian pengelolaan gangguan keamanan informasi

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) Ketidaksiesuaian dengan ketentuan yang berlaku.

b. Pegawai dan pihak ketiga wajib menyadari tanggung jawab mereka untuk melaporkan setiap gangguan keamanan informasi secepat mungkin, 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;
  - b) Segera melaporkan gangguan ke pihak berwenang sebelum melakukan tindakan pengamanan 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

a. Prosedur yang wajib 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 wajib 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 yang berwenang.
- c. Jejak audit dan bukti serupa wajib 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 wajib dikendalikan secara hati-hati dan formal, prosedur wajib 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 dikonfirmasi dengan pihak-pihak terkait sesegera mungkin.

J. Pengendalian keamanan informasi dalam pengelolaan kelangsungan kegiatan

1. Pengelolaan kelangsungan kegiatan pada saat keadaan darurat
  - a. Identifikasi risiko dan analisis dampak yang diakibatkan pada saat terjadi keadaan darurat;
  - b. Identifikasi seluruh aset informasi yang menunjang proses kegiatan 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 Kementerian Hukum dan Hak Asasi Manusia; dan
  - f. Pelaksanaan uji coba dan pemeliharaan Rencana Kelangsungan Kegiatan secara berkala.
2. Proses identifikasi risiko mengikuti ketentuan mengenai penerapan manajemen risiko di Lingkungan Kementerian Hukum dan Hak Asasi Manusia;
  3. Proses analisis dampak kegiatan wajib melibatkan pemilik proses bisnis dan dievaluasi secara berkala;
  4. Penyusunan rencana kelangsungan kegiatan mencakup:
    - a. Prosedur saat keadaan darurat, mencakup tindakan yang wajib dilakukan serta pengaturan hubungan dengan pihak berwenang;
    - b. Prosedur *fallback*, mencakup tindakan yang wajib diambil untuk memindahkan 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 Standar Pengelolaan Data Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia;
    - c. Prosedur saat kondisi telah normal (*resumption*) adalah tindakan mengembalikan kegiatan operasional ke kondisi normal;
    - d. Jadwal uji coba, mencakup langkah-langkah dan waktu pelaksanaan uji coba serta proses pemeliharannya;
    - e. Pelaksanaan pelatihan dan sosialisasi dalam rangka meningkatkan kepedulian dan pemahaman proses kelangsungan kegiatan dan pemahaman proses kelangsungan kegiatan dilaksanakan secara efektif;
    - f. Tanggung jawab dan peran setiap Petugas Pelaksana Pengelolaan Proses Kelangsungan; dan
    - g. Daftar kebutuhan aset informasi kritikal dan sumber daya untuk dapat menjalankan prosedur saat keadaan darurat, *fallback* dan saat kondisi telah normal (*resumption*).
  5. Uji coba rencana kelangsungan kegiatan wajib dilaksanakan untuk memastikan setiap rencana yang disusun dapat diterapkan:
    - a. Simulasi terutama untuk Petugas Pelaksana Pengelolaan Proses Kelangsungan Kegiatan;
    - b. Uji coba *recovery* sistem informasi untuk memastikan sistem informasi dapat berfungsi kembali;

- c. Uji coba proses *recovery* di lokasi kerja sementara untuk menjalankan proses bisnis secara paralel;
- d. Uji coba terhadap perangkat dan layanan yang disediakan oleh pihak ketiga ; dan
- e. Uji coba keseluruhan mulai dari organisasi, petugas, peralatan, perangkat, dan prosesnya.

## K. Pengendalian kepatuhan

### 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 manual, 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 ke format lain atau mengambil dari rekaman komersial (film dan audio), selain yang diperbolehkan oleh Undang-Undang Hak Cipta; dan
- h. Tidak menyalin secara penuh atau sebagian buku, artikel, atau dokumen lainnya, selain yang diizinkan oleh Undang-Undang Hak Cipta.

### 2. Kepatuhan terhadap kebijakan 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 ketidakpatuhan tidak terulang kembali;
- c. Menentukan dan melaksanakan tindakan perbaikan yang sesuai; dan
- d. Mengkaji tindakan perbaikan yang dilakukan.

3. Kepatuhan Teknis

Sistem informasi wajib diperiksa secara berkala untuk memastikan pengendalian perangkat keras dan perangkat lunak telah diimplementasikan secara benar. Kepatuhan teknis juga mencakup pengujian penetrasi 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 wajib memperhatikan hal berikut:

- a. Persyaratan audit wajib disetujui oleh CIO Kementerian Hukum dan Hak Asasi Manusia dan/atau Pimpinan Unit Eselon I ;
- b. Ruang lingkup pemeriksaan/audit wajib disetujui dan dikendalikan oleh pihak berwenang;
- c. Pemeriksaan perangkat lunak dan data wajib dibatasi untuk akses baca saja;
- d. Selain akses baca saja diizinkan untuk salinan dari *file* sistem yang diisolasi, yang wajib 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 wajib secara jelas diidentifikasi dan tersedia;
- f. Persyaratan untuk pengolahan khusus atau tambahan wajib diidentifikasi dan dis
- g. Sepakati;
- h. Semua akses wajib dipantau dan dicatat untuk menghasilkan jejak audit, dan untuk data dan sistem informasi sensitif wajib mempertimbangkan pencatatan waktu (*timestamp*) pada jejak audit;
- i. Semua prosedur, persyaratan, dan tanggung jawab wajib didokumentasikan; dan
- j. Auditor wajib independen dari kegiatan yang diaudit.

BAB IV  
PENUTUP

Keputusan Menteri Hukum dan Hak Asasi Manusia tentang Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Hukum dan Hak Asasi Manusia ini ditetapkan sebagai pedoman dalam melindungi aset informasi Kementerian Hukum dan Hak Asasi Manusia dari berbagai bentuk ancaman baik dari dalam maupun dari luar, dengan tujuan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.

Hal-hal yang sifatnya terlalu teknis dan spesifik yang belum diatur dalam Keputusan Menteri Hukum dan Hak Asasi Manusia ini, secara khusus akan diatur dalam buku pedoman, atau dapat dilaksanakan langsung sesuai dengan standar operasional prosedur

MENTERI HUKUM DAN HAK ASASI MANUSIA  
REPUBLIK INDONESIA,



YASONNA H. LAOLY