SALINAN

MENTERI DALAM NEGERI
REPUBLIK INDONESIA

PERATURAN MENTERI DALAM NEGERI REPUBLIK INDONESIA
NOMOR 57 TAHUN 2021
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
ADMINISTRASI KEPENDUDUKAN

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI DALAM NEGERI REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk melindungi dan menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi dari ancaman keamanan perlu disusun sistem manajemen keamanan informasi;

b. bahwa sistem manajemen keamanan informasi administrasi kependudukan dilaksanakan dengan menerapkan standar nasional Indonesia *international organization for standardization/international electrotechnical commission* 27001 (SNI ISO/IEC 27001);

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Menteri Dalam Negeri tentang Sistem Manajemen Keamanan Informasi Administrasi Kependudukan;

Mengingat : 1. Pasal 17 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 124, Tambahan Lembaran

Negara Republik Indonesia Nomor 4674) sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2013 Nomor 232, Tambahan Lembaran Negara Republik Indonesia Nomor 5475);

3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 595);
4. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916);
5. Peraturan Pemerintah Nomor 40 Tahun 2019 tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana telah diubah dengan Undang-undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 102, Tambahan Lembaran Negara Republik Indonesia Nomor 6354);
6. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);

7. Peraturan Presiden Nomor 11 Tahun 2015 tentang Kementerian Dalam Negeri (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 12);
8. Peraturan Menteri Dalam Negeri Nomor 95 Tahun 2019 tentang Sistem Informasi Administrasi Kependudukan (Berita Negara Republik Indonesia Tahun 2019 Nomor 1478);
9. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);
10. Peraturan Menteri Dalam Negeri Nomor 13 Tahun 2021 tentang Organisasi dan Tata Kerja Kementerian Dalam Negeri (Berita Negara Republik Indonesia Tahun 2021 Nomor 398);

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI DALAM NEGERI TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI ADMINISTRASI KEPENDUDUKAN.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:

1. Administrasi Kependudukan adalah rangkaian kegiatan penataan dan penertiban dalam penerbitan dokumen dan Data Kependudukan melalui Pendaftaran Penduduk, Pencatatan Sipil, pengelolaan informasi Administrasi Kependudukan serta pendayagunaan hasilnya untuk pelayanan publik dan pembangunan sektor lain.
2. Sistem Administrasi Kependudukan yang selanjutnya disingkat SAK adalah sistem yang memanfaatkan teknologi informasi dan komunikasi untuk penyelenggaraan Administrasi Kependudukan.

3. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan dalam negeri.
4. Direktur Jenderal Kependudukan dan Pencatatan Sipil yang selanjutnya disebut Dirjen adalah direktur jenderal yang ruang lingkup tugas dan fungsinya membidangi kependudukan dan pencatatan sipil dan bertanggung jawab kepada Menteri.
5. Direktorat Jenderal Kependudukan dan Pencatatan Sipil yang selanjutnya disebut Ditjen Dukcapil adalah direktorat jenderal pada Kementerian Dalam Negeri yang bertanggung jawab untuk melaksanakan tugas menyelenggarakan perumusan dan pelaksanaan kebijakan di bidang kependudukan dan pencatatan sipil sesuai dengan ketentuan peraturan perundang-undangan.
6. Dinas Kependudukan dan Pencatatan Sipil Provinsi yang selanjutnya disebut Disdukcapil Provinsi adalah perangkat pemerintah provinsi yang membidangi urusan Administrasi Kependudukan.
7. Dinas Kependudukan dan Pencatatan Sipil Kabupaten/Kota yang selanjutnya disebut Disdukcapil Kabupaten/Kota adalah perangkat pemerintah kabupaten/kota selaku instansi pelaksana yang membidangi urusan Administrasi Kependudukan.
8. Perwakilan Republik Indonesia adalah Kedutaan Besar Republik Indonesia, Konsulat Jenderal Republik Indonesia, dan Konsulat Republik Indonesia di luar wilayah Negara Kesatuan Republik Indonesia yang membidangi urusan Administrasi Kependudukan.
9. Unit Pelaksana Teknis Dinas Kependudukan dan Pencatatan Sipil Kabupaten/Kota yang selanjutnya disebut UPT Disdukcapil Kabupaten/Kota adalah unit pelayanan Administrasi Kependudukan di tingkat kecamatan yang berkedudukan di bawah Disdukcapil Kabupaten/Kota.

10. Sistem Manajemen Keamanan Informasi Administrasi Kependudukan yang selanjutnya disebut SMKI adalah bagian dari sistem manajemen secara keseluruhan, berdasarkan pendekatan risiko bisnis, untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan, dan memelihara keamanan informasi terkait pelaksanaan SAK.
11. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, pengelolaan dan penyampaian, atau pemindahan informasi antar sarana/media.
12. Akun adalah identifikasi pengguna yang diberikan oleh unit pengelola TIK, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem TIK.
13. Keamanan Informasi adalah perlindungan aset informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan, dan memastikan ketersediaan sistem dan data Administrasi Kependudukan.
14. Aset Informasi Sistem Administrasi Kependudukan yang selanjutnya disebut Aset Informasi SAK adalah aset yang digunakan untuk memfasilitasi pengelolaan dan pemanfaatan informasi Administrasi Kependudukan.
15. Hak Akses Khusus adalah akses terhadap sistem informasi yang bersifat rahasia dan hanya diberikan kepada pihak yang menandatangani perjanjian kerahasiaan dengan pemakaian terbatas dan dikontrol oleh satuan tugas Keamanan Informasi.
16. Perjanjian Kerahasiaan adalah perikatan antara para pihak dengan Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, dan/atau Perwakilan Republik Indonesia berupa pelarangan penyebarluasan, atau penyalahgunaan bahan rahasia, pengetahuan, atau informasi.

17. Pihak Lain adalah semua unsur selain Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia.
18. Kriptografi adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal untuk meningkatkan Keamanan Informasi.
19. Perangkat Lunak adalah sistem atau aplikasi yang digunakan untuk mendukung SAK.
20. Perangkat Pendukung adalah peralatan pendukung untuk menjamin beroperasinya perangkat keras, Perangkat Lunak, dan perangkat jaringan serta melindungnya dari kerusakan.
21. Perangkat Pengolah Informasi adalah setiap sistem pengolah informasi, layanan atau infrastruktur fisik dan nonfisik.
22. Pusat Data adalah tempat/ruang penyimpanan perangkat keras, Perangkat Lunak, basis data, dan Perangkat Pendukung pada Ditjen Dukcapil yang menghimpun dan mengintegrasikan data kependudukan dari hasil pelayanan pendaftaran penduduk dan pencatatan sipil.
23. Pusat Data Cadangan adalah tempat/ruang penyimpanan perangkat keras, Perangkat Lunak, basis data cadangan, dan Perangkat Pendukung pada Ditjen Dukcapil yang berfungsi untuk pemulihan kejadian luar biasa/bencana yang tidak direncanakan pada Pusat Data guna menjamin keberlangsungan sistem.
24. Pegawai adalah pegawai negeri sipil dan pegawai pemerintah dengan perjanjian kerja yang melaksanakan tugas dalam jabatan, pekerjaan atau kegiatan yang terkait dengan pengamanan Aset Informasi SAK sesuai dengan tugas dan fungsinya.
25. Satuan Tugas Keamanan Informasi yang selanjutnya disebut STKI adalah satuan tugas yang memiliki tugas dan tanggung jawab dalam pengamanan Aset Informasi SAK.
26. Sistem Informasi Administrasi Kependudukan yang selanjutnya disingkat SIAK adalah sistem informasi yang

memanfaatkan teknologi informasi dan komunikasi untuk memfasilitasi pengelolaan informasi Administrasi Kependudukan di tingkat penyelenggara dan instansi pelaksana sebagai satu kesatuan.

27. Tempat Layanan Operasional SIAK adalah ruangan perangkat keras, Perangkat Lunak, perangkat jaringan komunikasi data, dan sumber daya manusia.
28. Standar Operasional Prosedur yang selanjutnya disingkat SOP adalah serangkaian instruksi tertulis yang dibakukan mengenai berbagai prosedur pengamanan Aset Informasi SAK, bagaimana dan kapan harus dilakukan, serta dimana dan oleh siapa dilakukan.
29. Unit Teknologi Informasi Komunikasi yang selanjutnya disebut Unit TIK adalah satuan pelaksana SAK yang bertanggung jawab melaksanakan pengamanan Aset Informasi SAK dengan mengacu pada kebijakan SMKI.

Pasal 2

(1) Penyelenggaran SMKI dilaksanakan dengan menerapkan standar nasional Indonesia *international organization for standardization/international electrotechnical commission* 27001.

(2) SMKI sebagaimana dimaksud pada ayat (1) meliputi:
   a. tata kelola Keamanan Informasi;
   b. keamanan sumber daya manusia;
   c. keamanan fisik dan lingkungan;
   d. keamanan operasional dan komunikasi;
   e. manajemen aset;
   f. manajemen insiden Keamanan Informasi;
   g. manajemen kelangsungan layanan;
   h. kendali/hak akses;
   i. pengendalian kepatuhan;
   j. pengembangan dan perawatan sistem; dan
   k. audit TIK.

BAB II
PENANGGUNG JAWAB DAN PELAKSANA SISTEM MANAJEMEN KEAMANAN INFORMASI ADMINSITRASI KEPENDUDUKAN

Pasal 3

(1) Dirjen bertanggung jawab atas pelaksanaan SMKI.

(2) SMKI sebagaimana dimaksud pada ayat (1) digunakan untuk melindungi, menjamin kerahasiaan, keutuhan, dan ketersediaan Aset Informasi SAK dalam bentuk:
   a. data dan/atau dokumen;
   b. Perangkat Lunak;
   c. aset berwujud; dan
   d. aset tidak berwujud.

Pasal 4

(1) Data dan/atau dokumen sebagaimana dimaksud dalam Pasal 3 ayat (3) huruf a, meliputi data Administrasi Kependudukan, data biometrik penduduk, data balikan dari lembaga pengguna, data aggregat kependudukan, daftar penduduk pemilih potensial pemilihan, file konfigurasi *secure access module card*, data Akun pengguna sistem, daftar *internet protocol* sistem, data hasil pemadanan data kepada pengguna, data konfigurasi perangkat keras, data kode sumber aplikasi, dokumen Perjanjian Kerahasiaan, dokumen Administrasi Kependudukan yang ditandatangani secara elektronik, dan dokumen hasil audit.

(2) Perangkat Lunak sebagaimana dimaksud dalam Pasal 3 ayat (3) huruf b meliputi Perangkat Lunak aplikasi, Perangkat Lunak sistem, lisensi, dan perangkat bantu pengembangan sistem.

(3) Aset berwujud sebagaimana dimaksud dalam Pasal 3 ayat (3) huruf c meliputi perangkat komputer, perangkat jaringan dan komunikasi, media penyimpanan data, dan Perangkat Pendukung.

(4) Perangkat Jaringan sebagaimana dimaksud pada ayat 3 merupakan perangkat jaringan komunikasi data antara lain berupa *modem, hub, switch, router, firewall,* dan *proxy.*

(5) Aset tidak berwujud sebagaimana dimaksud dalam Pasal 3 ayat (3) huruf d meliputi pengetahuan, pengalaman, keahlian, citra, dan reputasi.

Pasal 5

(1) Dirjen selaku penanggung jawab sebagaimana dimaksud dalam Pasal 3 ayat (2) dibantu oleh STKI selaku pelaksana SMKI.

(2) STKI sebagaimana dimaksud pada ayat (1) berkedudukan di Ditjen Dukcapil.

(3) STKI sebagaimana dimaksud pada ayat (2) dikoordinasikan oleh Sekretaris Ditjen Dukcapil dan beranggotakan pejabat pimpinan tinggi pratama di lingkungan Ditjen Dukcapil.

Pasal 6

STKI sebagaimana dimaksud dalam Pasal 5 memiliki tugas dan tanggung jawab meliputi:

a. memastikan pelaksanaan kebijakan SMKI;
b. mengendalikan dokumen SMKI untuk menjaga kemutakhiran dokumen dan efektivitas pelaksanaan operasional;
c. melakukan pemetaan keperluan Keamanan Informasi;
d. melakukan audit internal SMKI untuk memperbaiki penerapan SMKI dan menindaklanjuti temuan auditor;
e. melakukan pemantauan dan evaluasi terhadap pelaksanaan SMKI di Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota dan Perwakilan Republik Indonesia secara berkala untuk meningkatkan Keamanan Informasi;
f. mengidentifikasi dan mengkaji secara berkala persyaratan untuk menjaga kerahasiaan Aset Informasi SAK yang dituangkan dalam dokumen kerahasiaan; dan

g. menyampaikan laporan dan rekomendasi pelaksanaan SMKI kepada Dirjen melalui Sekretaris Ditjen Dukcapil selaku koordinator STKI.

Pasal 7

(1) STKI harus memiliki kompetensi dan keahlian yang memadai dalam melaksanakan tugas dan tanggung jawab untuk melakukan pemetaan keperluan Keamanan Informasi sebagaimana dimaksud dalam Pasal 6 huruf c.

(2) Pemetaan keperluan Keamanan Informasi sebagaimana dimaksud pada ayat (1) meliputi:
   a. menetapkan standar kompetensi/keahlian pelaksana;
   b. mengalokasikan sumber daya;
   c. melaksanakan program sosialisasi dan peningkatan pemahaman Keamanan Informasi;
   d. melaksanakan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana Keamanan Informasi;
   e. membuat langkah kelangsungan layanan TIK;
   f. membuat matrik, parameter dan proses pengukuran kinerja pengelolaan Keamanan Informasi; dan
   g. melaksanakan kebijakan dan langkah penanggulangan insiden Keamanan Informasi yang menyangkut pelanggaran hukum.

Pasal 8

Tugas dan tanggung jawab melakukan audit internal SMKI sebagaimana dimaksud dalam Pasal 6 huruf d STKI dapat menunjuk pihak yang berkompeten di bidang audit teknologi informasi.

Pasal 9

(1) Tugas dan tanggung jawab menyampaikan laporan dan rekomendasi pelaksanaan SMKI sebagaimana dimaksud dalam Pasal 6 huruf g dilakukan dengan cara menggunakan catatan penerapan kebijakan dan standar

SMKI untuk mengukur kepatuhan dan efektifitas penerapan SMKI.

(2) Catatan penerapan kebijakan dan standar SMKI sebagaimana dimaksud pada ayat (1) terdiri dari:
   a. formulir berdasarkan SOP yang ditetapkan oleh Menteri;
   b. catatan gangguan Keamanan Informasi;
   c. catatan dari sistem (*system log*);
   d. catatan Pegawai, Pihak Lain dan pengunjung di Pusat Data, Pusat Data Cadangan, atau Tempat Layanan Operasional SIAK;
   e. kontrak kerja dengan pihak pelaksana kegiatan;
   f. perjanjian kerja sama layanan pemanfaatan data;
   g. Perjanjian Kerahasiaan; dan
   h. laporan audit.

Pasal 10

(1) Pelaksanaan kebijakan SMKI sebagaimana dimaksud dalam Pasal 3 ayat (2) di Ditjen Dukcapil dilaksanakan oleh Sekretaris Ditjen Dukcapil selaku koordinator STKI, pejabat pimpinan tinggi pratama, pimpinan Unit TIK, dan Unit TIK.

(2) Pelaksanaan kebijakan SMKI sebagaimana dimaksud dalam Pasal 3 ayat (2) di Disdukcapil Provinsi dilaksanakan oleh kepala Disdukcapil Provinsi, pimpinan Unit TIK, dan Unit TIK.

(3) Pelaksanaan kebijakan SMKI sebagaimana dimaksud dalam Pasal 3 ayat (2) di Disdukcapil Kabupaten/Kota dilaksanakan oleh kepala Disdukcapil Kabupaten/Kota, pimpinan Unit TIK, dan Unit TIK.

(4) Pelaksanaan kebijakan SMKI sebagaimana dimaksud dalam Pasal 3 ayat (2) di UPT Disdukcapil Kabupaten/Kota dilaksanakan oleh kepala UPT Disdukcapil Kabupaten/Kota, pimpinan Unit TIK, dan Unit TIK.

(5) Pelaksanaan kebijakan SMKI sebagaimana dimaksud dalam Pasal 3 ayat (2) di Perwakilan Republik Indonesia

dilaksanakan oleh kepala Perwakilan Republik Indonesia, pimpinan Unit TIK, dan Unit TIK.

Pasal 11

(1) Dirjen selaku penanggung jawab pelaksanaan kebijakan SMKI sebagaimana dimaksud dalam Pasal 3 ayat (2) dapat melakukan kerja sama dengan:
   a. kementerian yang menyelenggarakan urusan pemerintahan di bidang informasi dan telekomunikasi; dan
   b. komunitas, badan hukum, dan lembaga yang bergerak dalam bidang Keamanan Informasi, melalui pendampingan teknis, pelatihan, seminar, atau forum lain yang relevan dengan Keamanan Informasi.
(2) Pejabat pimpinan tinggi pratama sebagaimana dimaksud dalam Pasal 10 ayat (1) sampai dengan ayat (3) bertugas untuk melaksanakan Kebijakan SMKI di lingkungan direktorat, Disdukcapil Provinsi, dan Disdukcapil Kabupaten/Kota.
(3) Kepala UPT Disdukcapil Kabupaten/Kota sebagaimana di maksud dalam Pasal 10 ayat (4) bertugas untuk melaksanakan kebijakan SMKI di UPT Disdukcapil Kabupaten/Kota.
(4) Kepala Perwakilan Republik Indonesia sebagaimana dimaksud Pasal 10 ayat (5) bertugas untuk melaksanakan Kebijakan SMKI di Perwakilan Republik Indonesia.
(5) Pimpinan Unit TIK sebagaimana dimaksud dalam Pasal 10 ayat (1) sampai dengan ayat (5) bertugas untuk mengatur pelaksanaan Kebijakan SMKI di lingkungan Unit TIK.
(6) Unit TIK sebagaimana dimaksud dalam Pasal 10 ayat (1) sampai dengan ayat (5) bertugas untuk melaksanakan kebijakan Keamanan Informasi di lingkungan Unit TIK dan bertanggung jawab terhadap pimpinan Unit TIK.

Pasal 12

(1) Pimpinan Unit TIK sebagaimana dimaksud dalam Pasal 11 ayat (5) memberikan informasi kepada Dirjen melalui

pejabat pimpinan tinggi pratama atau koordinator STKI untuk melakukan keputusan sepihak guna melindungi kerahasiaan, keutuhan, dan ketersediaan Aset Informasi SAK.

(2) Keputusan sepihak sebagaimana dimaksud pada ayat (1) dilakukan terhadap pihak:
   a. yang melanggar perjanjian; dan/atau
   b. lainnya yang meretas sistem secara melawan hukum.

(3) Pemberian informasi sebagaimana dimaksud pada ayat (1) dilakukan melalui media elektronik untuk mendapat persetujuan dari Dirjen.

(4) Ditjen Dukcapil tidak bertanggung jawab atas kerugian yang ditimbulkan oleh pihak yang melanggar perjanjian sebagaimana dimaksud pada ayat (1).

BAB III
TATA KELOLA KEAMANAN INFORMASI

Pasal 13

Tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf a dilakukan untuk mengamankan pengelolaan kebijakan keamanan Administrasi Kependudukan melalui kepastian prosedur kerja.

Pasal 14

(1) Tata kelola Keamanan Informasi di lingkungan Ditjen Dukcapil dilaksanakan oleh Dirjen bersama dengan Sekretaris Ditjen Dukcapil selaku koordinator STKI, serta pejabat pimpinan tinggi pratama, pimpinan Unit TIK, dan Unit TIK selaku anggota STKI.

(2) Tata kelola Keamanan Informasi di Disdukcapil Provinsi dilaksanakan oleh kepala Disdukcapil Provinsi, pimpinan Unit TIK, dan Unit TIK selaku satuan pelaksana SAK.

(3) Tata kelola Keamanan Informasi di Disdukcapil Kabupaten/Kota dilaksanakan oleh kepala Disdukcapil Kabupaten/Kota, pimpinan Unit TIK, dan Unit TIK selaku satuan pelaksana SAK.

(4) Tata kelola Keamanan Informasi di UPT Disdukcapil Kabupaten/Kota dilaksanakan oleh kepala UPT Disdukcapil Kabupaten/Kota, pimpinan Unit TIK, dan Unit TIK selaku satuan pelaksana SAK.

(5) Tata kelola Keamanan Informasi di Perwakilan Republik Indonesia dilaksanakan oleh kepala Perwakilan Republik Indonesia, pimpinan unit TIK, dan unit TIK selaku satuan pelaksana SAK.

Pasal 15

Dirjen sebagaimana dimaksud dalam Pasal 14 ayat (1) bertugas untuk:

a. membuat rencana dan target Keamanan Informasi setiap tahunnya; dan
b. mengukur efektivitas dan konsistensi penerapan Kebijakan dan Standar SMKI.

Pasal 16

Koordinator STKI sebagaimana dimaksud dalam Pasal 14 ayat (1) bertugas untuk:

a. memastikan kebijakan dan standar SMKI diterapkan secara efektif sesuai dengan standar indeks Keamanan Informasi yang ditetapkan oleh kementerian yang menyelenggarakan urusan pemerintahan di bidang informasi dan telekomunikasi;
b. memastikan langkah perbaikan sudah dilakukan berdasarkan saran dan rekomendasi yang diberikan STKI dalam pelaksanaan evaluasi dan/atau audit penerapan kebijakan dan standar SMKI;
c. memastikan peningkatan kesadaran, kepedulian, dan kepatuhan seluruh Pegawai terhadap kebijakan dan standar SMKI;
d. memastikan terlaksananya evaluasi dan/atau audit internal terhadap kebijakan dan standar SMKI sesuai dengan indeks Keamanan Informasi yang ditetapkan oleh kementerian/lembaga terkait;

e. memastikan pelaksanaan penanganan gangguan Keamanan Informasi antar unit kerja di lingkungan direktorat; dan
f. melaporkan kinerja pelaksanaan dan evaluasi penerapan kebijakan dan standar SMKI kepada Dirjen yang akan digunakan sebagai dasar peningkatan Keamanan Informasi.

Pasal 17

Pejabat pimpinan tinggi pratama di Kementerian Dalam Negeri, kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, kepala UPT Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia sebagaimana dimaksud dalam Pasal 14 bertanggung jawab untuk:

a. melaksanakan kebijakan dan standar SMKI pada Unit TIK;
b. mengawasi penerapan kebijakan dan standar SMKI pada Unit TIK;
c. memberikan masukan melalui koordinator STKI untuk meningkatkan penerapan kebijakan dan standar SMKI pada Unit TIK;
d. mendefinisikan kebutuhan, merekomendasikan, dan memfasilitasi penyelenggaraan pendidikan dan pelatihan Keamanan Informasi bagi Pegawai pada Unit TIK;
e. memantau, mencatat, menguraikan, dan menindaklanjuti gangguan Keamanan Informasi yang diketahui atau dilaporkan sesuai dengan prosedur pelaporan gangguan Keamanan Informasi pada Unit TIK; dan
f. memfasilitasi penyelesaian masalah Keamanan Informasi pada Unit TIK.

Pasal 18

(1) Pejabat pimpinan tinggi pratama, kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, kepala UPT Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia sebagaimana dimaksud dalam Pasal 17 menetapkan penanggung jawab Aset Informasi SAK pada Unit TIK.

(2) Penanggung jawab Aset Informasi SAK sebagaimana disebut pada ayat (1) menetapkan aturan penggunaan Aset Informasi SAK sesuai dengan SOP manajemen aset.

Pasal 19

Pimpinan Unit TIK sebagaimana dimaksud dalam Pasal 14 bertanggung jawab untuk:

a. melaksanakan kebijakan dan standar SMKI untuk pengamanan Aset Informasi SAK pada Unit TIK;
b. mengawasi penerapan kebijakan dan standar SMKI untuk pengamanan Aset Informasi SAK pada Unit TIK;
c. memantau, mencatat, menguraikan, dan menindaklanjuti gangguan Keamanan Informasi yang diketahui atau dilaporkan sesuai dengan prosedur pelaporan gangguan Keamanan Informasi pada Unit TIK;
d. memfasilitasi penyelesaian masalah Keamanan Informasi pada Unit TIK;
e. menindaklanjuti laporan hasil audit internal SMKI;
f. meningkatkan pengetahuan, keterampilan, dan kepedulian terhadap Keamanan Informasi pada seluruh pengguna di Unit TIK;
g. menerapkan prinsip manajemen resiko dalam pelaksanaan pengamanan dan perlindungan Aset Informasi SAK dalam penerapan manajemen resiko; dan
h. melaporkan kinerja SMKI kepada koordinator STKI, 2 (dua) kali dalam setahun dan sewaktu-waktu jika diperlukan.

Pasal 20

Unit TIK sebagaimana dimaksud dalam Pasal 14 bertanggung jawab untuk:

a. melaksanakan penerapan kebijakan dan standar SMKI di lingkungan Unit TIK;
b. memantau, mencatat dan menindaklanjuti gangguan Keamanan Informasi yang diketahui atau dilaporkan sesuai dengan prosedur pelaporan gangguan Keamanan Informasi di lingkungan Unit TIK;

c. melaksanakan identifikasi, mengklasifikasi, memberikan label inventaris Aset Informasi SAK, dan mendokumentasikan ke dalam daftar inventaris Aset Informasi SAK;
d. mengendalikan dokumen SMKI untuk menjaga kemutakhiran dokumen dan efektivitas pelaksanaan operasional;
e. mengendalikan operasional dari kerusakan dan mencegah akses oleh pihak yang tidak berwenang; dan
f. melaksanakan penyelesaian masalah Keamanan Informasi di lingkungan Unit TIK.

Pasal 21

(1) Klasifikasi daftar inventaris Aset Informasi SAK sebagaimana dimaksud dalam Pasal 20 huruf c diatur dalam SOP manajemen Aset Informasi SAK.
(2) Daftar inventaris Aset Informasi SAK sebagaimana dimaksud pada ayat (1) dipelihara dan dikelola perubahannya oleh Unit TIK.
(3) Pengendalian dokumen sebagaimana dimaksud dalam Pasal 20 huruf d dengan menempatkan dokumen SMKI pada semua area operasional agar mudah diakses oleh pengguna di Unit TIK sesuai dengan peruntukannya.

Pasal 22

(1) Pegawai Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia bertanggung jawab untuk menjaga keamanan Aset Informasi SAK sesuai dengan tugas dan fungsinya.
(2) Pegawai sebagaimana dimaksud pada ayat (1) menyetujui syarat dan menandatangani pakta integritas.
(3) Dalam hal Pegawai sebagaimana dimaksud pada ayat (1) tidak lagi menjadi bagian dalam pengelolaan Aset Informasi SAK, Aset Informasi SAK yang dikuasainya diserahkan kembali kepada Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil

Kabupaten/Kota, atau Perwakilan Republik Indonesia sesuai dengan kewenangan.

(4) Pelaksanaan kebijakan dan standar SMKI oleh Pegawai sebagaimana dimaksud pada ayat (1) harus dievaluasi secara berkala oleh atasan masing-masing dan menjadi bagian dari penilaian kinerja Pegawai.

Pasal 23

(1) Pihak Lain yang ikut serta terhadap pelaksanaan keamanan Aset Informasi SAK wajib menjaga kerahasiaan informasi.

(2) Pihak Lain sebagaimana dimaksud pada ayat (1) membuat perjanjian disertai dengan menyetujui syarat serta menandatangani pernyataan tertulis untuk menjaga keamanan Aset Informasi SAK dan kerahasiaan informasi.

(3) Perjanjian sebagaimana dimaksud pada ayat (2) paling sedikit memuat:

a. perlindungan kepemilikan informasi, rahasia organisasi, dan kekayaan intelektual;
b. izin menggunakan informasi rahasia;
c. hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia;
d. pelaporan terhadap penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan; dan
e. syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian.

(4) Dalam hal Pihak Lain tidak lagi menjadi bagian dalam pengelolaan Aset Informasi SAK, Aset Informasi SAK yang dikuasainya diserahkan kembali kepada Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, atau Perwakilan Republik Indonesia sesuai dengan kewenangan.

BAB IV

KEAMANAN SUMBER DAYA MANUSIA

Pasal 24

Keamanan sumber daya manusia sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b dilakukan untuk mengamankan dan mengendalikan sumber daya manusia dalam melaksanakan tugas kebijakan keamanan Administrasi Kependudukan.

Pasal 25

(1) Keamanan sumber daya manusia di lingkungan Ditjen Dukcapil dilaksanakan oleh Dirjen bersama dengan Sekretaris Ditjen Dukcapil selaku koordinator STKI, serta pejabat pimpinan tinggi pratama, pimpinan Unit TIK, dan Unit TIK selaku anggota STKI.
(2) Keamanan sumber daya manusia di Disdukcapil Provinsi dilaksanakan oleh kepala Disdukcapil Provinsi, pimpinan Unit TIK, dan Unit TIK selaku satuan pelaksana SAK.
(3) Keamanan sumber daya manusia di Disdukcapil Kabupaten/Kota dilaksanakan oleh kepala Disdukcapil Kabupaten/Kota, pimpinan Unit TIK, dan Unit TIK selaku satuan pelaksana SAK.
(4) Keamanan sumber daya manusia di UPT Disdukcapil Kabupaten/Kota dilaksanakan oleh kepala UPT Disdukcapil Kabupaten/Kota, pimpinan Unit TIK, dan Unit TIK selaku satuan pelaksana SAK.
(5) Keamanan sumber daya manusia di Perwakilan Republik Indonesia dilaksanakan oleh kepala Perwakilan Republik Indonesia, pimpinan Unit TIK, dan Unit TIK selaku satuan pelaksana SAK.

Pasal 26

(1) Dirjen sebagaimana dimaksud dalam Pasal 25 ayat (1) bertugas menetapkan tugas dan fungsi Sekretaris Ditjen Dukcapil, pejabat pimpinan tinggi pratama, pimpinan Unit

TIK, dan Unit TIK tentang keamanan sumber daya manusia.

(2) Kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, kepala UPT Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia sebagaimana dimaksud dalam Pasal 25 ayat (2) sampai dengan ayat (5) bertugas menetapkan tugas dan fungsi pimpinan Unit TIK dan Unit TIK tentang keamanan sumber daya manusia.

Pasal 27

Koordinator STKI, kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, kepala UPT Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia sebagaimana dimaksud dalam Pasal 25 bertugas untuk menyediakan Pegawai pengganti yang berkeahlian khusus sesuai dengan kompetensi yang setara dengan Pegawai yang mutasi atau berhenti.

Pasal 28

Pejabat pimpinan tinggi pratama, kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, kepala UPT Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia sebagaimana dimaksud dalam Pasal 25 bertugas untuk:

a. memahami substansi dan mendokumentasikan tugas dan fungsi Pegawai Unit TIK;
b. mengkomunikasikan peran dan tanggung jawab kepada Pegawai Unit TIK;
c. menghentikan hak penggunaan Aset Informasi SAK bagi Pegawai yang sedang dalam pemeriksaan dan/atau menjalani proses hukum terkait dengan dugaan pelanggaran SMKI;
d. mencabut hak akses terhadap akses informasi SAK yang dimiliki Pegawai dan Pihak Lain apabila yang bersangkutan tidak lagi bekerja di Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT

Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia;

e. membuat berita acara serah terima terkait mengembalikan seluruh Aset Informasi SAK yang dipergunakan selama bekerja bagi Pegawai Unit TIK yang berhenti bekerja atau mutasi;

f. melakukan pemeriksaan latar belakang Pihak Lain dengan memperhitungkan privasi, perlindungan data pribadi, dan/atau pekerjaan sesuai dengan standar SMKI; dan

g. mengikutsertakan Pegawai Unit TIK mendapatkan pendidikan/pelatihan/sosialisasi keamanan sistem informasi secara berkala sesuai dengan tingkat tanggung jawabnya.

Pasal 29

(1) Pemeriksaan latar belakang Pihak Lain sebagaimana dimaksud dalam Pasal 28 huruf f dilakukan terhadap pengguna dan nonpengguna.

(2) Pemeriksaan latar belakang Pihak Lain terhadap pengguna dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

(3) Pemeriksaan latar belakang Pihak Lain nonpengguna dengan melakukan wawancara dan menyerahkan dokumen kepada pejabat pimpinan tinggi pratama, kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, kepala UPT Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia.

(4) Wawancara sebagaimana dimaksud pada ayat (3) dilakukan paling sedikit terhadap substansi:
   a. pemahaman atas kebijakan Keamanan Informasi dan standar SMKI; dan
   b. pengalaman kerja sesuai dengan bidang keahlian.

(5) Dokumen sebagaimana dimaksud pada ayat (3) meliputi:
   a. daftar riwayat hidup pemohon;
   b. ijazah pendidikan yang dilegalisir;
   c. sertifikasi profesi;

d. surat keterangan pengalaman kerja; dan
e. surat keterangan catatan kepolisian.

Pasal 30

Pihak Lain nonpengguna sebagaimana dimaksud dalam Pasal 29 ayat (3) harus melakukan:

a. menyetujui syarat dan menandatangani pernyataan tertulis untuk menjaga keamanan Aset Informasi SAK;
b. bertanggung jawab memahami substansi, mendokumentasikan, dan memberikan informasi kepada pihak dalam perjanjian terhadap keamanan Aset Informasi SAK; dan
c. mengembalikan seluruh Aset Informasi SAK yang dipergunakan selama bekerja apabila berhenti bekerja atau berakhir masa kontraknya.

Pasal 31

Pimpinan Unit TIK sebagaimana dimaksud dalam Pasal 25 bertugas untuk memahami substansi dan mendokumentasikan tugas dan fungsi Pegawai Unit TIK.

Pasal 32

Pegawai, Pihak Lain, dan tamu yang memasuki lingkungan area Pusat Data, Pusat Data Cadangan, dan Tempat Layanan Operasional SIAK mematuhi standar keamanan fisik dan lingkungan.

BAB V

KEAMANAN FISIK DAN LINGKUNGAN

Pasal 33

Keamanan fisik dan lingkungan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf c dilakukan untuk memberikan pelindungan, pemeliharaan, dan pemindahan perangkat terhadap pengamanan fisik dan lingkungan.

Pasal 34

(1) Keamanan fisik dan lingkungan di Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh Unit TIK.

(2) Unit TIK sebagaimana dimaksud pada ayat (1) bertugas untuk melakukan:
   a. pemeliharaan perangkat wajib sesuai dengan petunjuk manualnya;
   b. pengamanan area;
   c. pengamanan kantor, ruangan, dan fasilitas;
   d. perlindungan terhadap ancaman eksternal dan lingkungan;
   e. penempatan dan perlindungan perangkat; dan
   f. pengamanan kabel di Pusat Data, Pusat Data Cadangan, dan/atau Tempat Layanan Operasional SIAK.

Pasal 35

(1) Pemeliharaan perangkat sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf a dilakukan dengan cara mencatat serta menyimpan data Aset Informasi SAK yang digunakan.

(2) Dalam hal pemeliharaan perangkat sebagaimana dimaksud pada ayat (1) tidak dapat dilakukan di tempat, pemindahan perangkat berdasarkan persetujuan pimpinan Unit TIK.

(3) Pemindahan perangkat sebagaimana dimaksud pada ayat (2) untuk data yang memiliki klasifikasi sangat rahasia dan rahasia yang disimpan pada perangkat tersebut dipindahkan terlebih dahulu.

(4) Dalam hal pemeliharaan sebagaimana dimaksud pada ayat (1) dilakukan oleh Pihak Lain, pelaksanaannya dilakukan dengan membuat perjanjian kerja sama.

(5) Perjanjian kerja sama sebagaimana dimaksud pada ayat (4) substansinya paling sedikit memuat pemeliharaan yang

disediakan dan tingkat kinerja yang harus dipenuhi Pihak Lain.

Pasal 36

Pengamanan area sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf b dilakukan dengan cara:

a. menyimpan Perangkat Pengolah Informasi di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai yaitu pintu elektronik, sistem pemadam kebakaran, alarm bahaya, dan perangkat pemutus aliran listrik;
b. akses ke Pusat Data, Pusat Data Cadangan, Tempat Layanan Operasional SIAK dan/atau area kerja yang berisi Aset Informasi SAK yang memiliki klasifikasi sangat rahasia dan rahasia harus dibatasi dan hanya diberikan kepada Pegawai yang diberi akses;
c. Pihak Lain yang memasuki Pusat Data, Pusat Data Cadangan, Tempat Layanan Operasional SIAK, dan/atau area kerja yang berisikan Aset Informasi SAK yang memiliki klasifikasi sangat rahasia dan rahasia harus didampingi oleh Pegawai yang ditugaskan sepanjang waktu kunjungan;
d. kantor, ruangan, dan perangkat yang berisikan Aset Informasi SAK yang memiliki klasifikasi sangat rahasia dan rahasia wajib dilindungi secara memadai; dan
e. pengamanan area Pusat Data, Pusat Data Cadangan dan Tempat Layanan Operasional SIAK sesuai dengan SOP pengamanan area.

Pasal 37

Pengamanan kantor, ruangan, dan fasilitas sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf c dilakukan dengan cara:

a. pengamanan kantor, ruangan, dan fasilitas sesuai dengan peraturan dan standar keamanan dan keselamatan kerja;
b. fasilitas utama wajib ditempatkan pada area khusus untuk menghindari akses publik; dan

c. pembatasan pemberian identitas atau tanda keberadaan aktivitas pengolahan informasi.

Pasal 38

Perlindungan terhadap ancaman eksternal dan lingkungan sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf d dilakukan dengan cara:

a. bahan berbahaya atau mudah terbakar wajib disimpan pada jarak yang aman dari batas aman;
b. perangkat pemulihan dan media data cadangan wajib diletakkan pada jarak yang aman untuk menghindari kerusakan dari bencana yang mempengaruhi fasilitas utama; dan
c. perangkat pemadam kebakaran wajib disediakan dan diletakkan di tempat yang mudah dijangkau.

Pasal 39

Penempatan dan perlindungan perangkat sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf e dilakukan dengan cara:

a. perangkat diletakkan pada lokasi yang meminimalkan akses yang tidak perlu ke dalam area kerja;
b. Perangkat Pengolah Informasi yang menangani informasi sensitif diposisikan dan dibatasi sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak tidak berwenang;
c. perangkat yang memerlukan perlindungan khusus wajib terisolasi;
d. melakukan langkah pengendalian untuk meminimalkan risiko potensi ancaman fisik;
e. kondisi lingkungan, seperti suhu dan kelembaban wajib dipantau sesuai dengan SOP Pusat Data/Pusat Data Cadangan; dan
f. perlindungan petir wajib diterapkan untuk semua bangunan dan filter perlindungan petir dipasang untuk semua jalur komunikasi dan listrik.

Pasal 40

Pengamanan kabel di Pusat Data, Pusat Data Cadangan, dan/atau Tempat Layanan Operasional SIAK sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf f dilakukan dengan mengikuti standar elektrikal/mekanikal Pusat Data dan/atau Pusat Data Cadangan.

BAB VI

KEAMANAN OPERASIONAL DAN KOMUNIKASI

Pasal 41

Keamanan operasional dan komunikasi sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf d dilakukan untuk memastikan operasional yang aman dan benar pada Aset Informasi SAK, mengimplementasikan dan memelihara keamanan Aset Informasi SAK, mengelola layanan yang diberikan oleh Pihak Lain, meminimalkan risiko kegagalan, melindungi keutuhan dan ketersediaan Aset Informasi SAK, dan memastikan keamanan akses dan pertukaran informasi melalui jaringan komunikasi.

Pasal 42

(1) Keamanan operasional dan komunikasi di lingkungan Ditjen Dukcapil, Dinas Dukcapil Provinsi, Dinas Dukcapil Kabupaten/Kota, UPT Dinas Dukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh Unit TIK.

(2) Unit TIK sebagaimana dimaksud pada ayat (1) bertugas untuk melakukan pengendalian:

a. SOP dan tanggung jawab;
b. pengelolaan layanan oleh Pihak Lain;
c. perencanaan dan penerimaan sistem;
d. perlindungan terhadap ancaman program yang membahayakan;
e. data cadangan;
f. pengelolaan keamanan jaringan;
g. penanganan media penyimpanan data;

h. pertukaran informasi;

i. pemantauan penggunaan sistem pengolah informasi; dan

j. pemisahan perangkat pengembangan dan operasional.

Pasal 43

(1) Pengendalian SOP dan tanggung jawab sebagaimana dimaksud dalam Pasal 42 ayat (2) huruf a dilakukan dengan cara:

a. mendokumentasikan, memelihara, dan menyediakan SOP 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 ekslusif terhadap seluruh Aset Informasi SAK dan perangkat pengolahnya, dan

d. memisahkan perangkat pengembangan, pengujian dan operasional untuk mengurangi resiko perubahan atau akses oleh pihak yang tidak berhak terhadap sistem operasional.

(2) SOP sebagaimana dimaksud pada ayat (1) ditetapkan oleh Menteri.

(3) SOP sebagaimana dimaksud pada ayat (2) memuat lingkup SMKI sebagaimana dimaksud dalam Pasal 2 ayat (2) dan SOP lainnya yang terkait.

Pasal 44

Pengendalian pengelolaan layanan oleh Pihak Lain sebagaimana dimaksud dalam Pasal 42 ayat (2) huruf b dilakukan dengan cara:

a. memastikan pengendalian Keamanan Informasi, definisi layanan, dan tingkat layanan yang termuat dalam

kesepakatan penyediaan layanan telah diterapkan, dioperasikan, dan dipelihara oleh Pihak Lain;

b. melakukan pemantauan terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh Pihak Lain secara berkala;

c. memperhatikan kritikalitas, proses yang terkait dan hasil penilaian ulang resiko layanan apabila terjadi perubahan pada layanan yang disediakan oleh Pihak Lain;

d. mengkaji laporan layanan Pihak Lain;

e. memberikan informasi tentang gangguan keamanan dan mengkaji informasi bersama Pihak Lain; dan

f. memeriksa jejak audit Pihak Lain dan pencatatan peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan.

Pasal 45

Pengendalian perencanaan dan penerimaan sistem sebagaimana dimaksud dalam Pasal 42 ayat (2) huruf c dilakukan dengan cara:

a. memantau penggunaan Perangkat Pengolah Informasi dan membuat perkiraan pertumbuhan kebutuhan ke depan untuk memastikan ketersediaan kapasitas; dan

b. menetapkan kriteria penerimaan untuk sistem informasi baru, pemutakhiran, dan versi baru serta melakukan pengujian sebelum penerimaan.

Pasal 46

(1) Pengendalian perlindungan terhadap ancaman program yang membahayakan sebagaimana dimaksud dalam Pasal 42 ayat (2) huruf d, dengan menerapkan sistem pada Pusat Data, Pusat Data Cadangan dan atau Tempat Layanan Operasional SIAK yang dapat melakukan pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan.

(2) Perlindungan sebagaimana dimaksud pada ayat (1) dilakukan dengan cara pemasangan paling sedikit meliputi:

a. perangkat *firewall*;
b. perangkat *antivirus*;
c. perangkat manajemen akses pengguna; dan
d. Perangkat Pendukung lainnya sesuai dengan perkembangan teknologi Keamanan Informasi.

Pasal 47

Pengendalian data cadangan sebagaimana dimaksud dalam Pasal 42 ayat (2) huruf e dilakukan dengan cara:

a. melakukan pembuatan data cadangan informasi dan Perangkat Lunak yang berada di Pusat Data, Pusat Data Cadangan, dan/atau Tempat Layanan Operasional SIAK secara berkala; dan
b. memproses pembuatan data cadangan sesuai dengan standar pembuatan data cadangan pada Pusat Data/Pusat Data Cadangan.

Pasal 48

Pengendalian pengelolaan keamanan jaringan sebagaimana dimaksud dalam Pasal 42 ayat (2) huruf f dilakukan dengan cara:

a. mengelola dan melindungi keamanan jaringan dari berbagai bentuk ancaman;
b. mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan serta mencantumkannya dalam kesepakatan penyediaan layangan jaringan termasuk layanan jaringan yang disediakan oleh Pihak Lain;
c. mencatat informasi Pihak Lain yang diizinkan mengakses ke jaringan dan menerapkan pemantauan serta pencatatan kegiatan selama menggunakan jaringan;
d. memutus layanan tanpa pemberitahuan sebelumnya jika terjadi gangguan Keamanan Informasi;
e. melindungi jaringan dari pihak yang tidak berhak mengakses dengan cara:

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.

f. menerapkan fitur keamanan layanan jaringan meliputi:
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.

Pasal 49

Pengendalian penanganan media penyimpanan data sebagaimana dimaksud dalam Pasal 42 ayat (2) huruf g dilakukan dengan cara:

a. menyusun prosedur yang mengatur penanganan media penyimpanan data untuk melidungi Aset Informasi SAK; dan
b. melakukan penanganan media penyimpanan data sesuai dengan standar penanganan media penyimpanan data pada Pusat Data/Pusat Data Cadangan.

Pasal 50

(1) Pengendalian pertukaran informasi sebagaimana dimaksud dalam Pasal 42 ayat (2) huruf h dilakukan dengan cara:
a. melakukan pertukaran informasi dan Perangkat Lunak antara Kementerian Dalam Negeri melalui Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil

Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dengan Pihak Lain berdasarkan kesepakatan tertulis kedua belah pihak dengan persetujuan Kementerian Dalam Negeri melalui Ditjen Dukcapil;

b. melakukan penilaian resiko yang memadai sebelum melakukan pertukaran informasi;

c. menerapkan pengendalian Keamanan Informasi untuk pengiriman informasi melalui surat elektronik atau pengiriman informasi melalui jasa layanan pengiriman untuk menghindari akses pihak yang tidak berhak;

d. memberikan perlindungan pertukaran informasi dari pencegatan, penyalinan, modifikasi, dan perusakan;

e. melakukan pendeteksian dan perlindungan terhadap kode berbahaya yang dapat dikirim melalui penggunaan sistem elektronik;

f. memberikan perlindungan informasi elektronik yang memiliki klasifikasi sangat rahasia dan rahasia;

g. memberikan pertimbangan resiko terkait penggunaan perangkat komunikasi nirkabel;

h. melakukan pertukaran informasi yang menggunakan sistem manual berpedoman sesuai dengan ketentuan peraturan perundang-undangan; dan

i. pengendalian terhadap SOP mengenai pertukaran informasi secara elektronik ditetapkan oleh Menteri.

(2) Pengiriman informasi melalui surat elektronik sebagaimana dimaksud pada ayat (1) huruf c harus menggunakan alamat surat elektronik milik Ditjen Dukcapil, Dinas Dukcapil Provinsi, Dinas Kabupaten/Kota, UPT Dinas Kabupaten/Kota, atau Perwakilan Republik Indonesia.

Pasal 51

(1) Pengendalian pemantauan penggunaan sistem pengolah informasi sebagaimana dimaksud dalam Pasal 42 ayat (2) huruf i dilakukan dengan cara:

a. 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 dan mengkaji secara berkala hasil pemantauan;
c. melindungi fasilitas pencatatan dan data yang dicatat dari kerusakan dan akses oleh pihak yang tidak berwenang;
d. menerapkan sistem pencatatan kegiatan *system administrator* dan *system operator*;
e. menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindak pengamanan yang tepat; dan
f. memastikan semua Perangkat Pengolah Informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.

(2) Pemantauan sebagaimana dimaksud pada ayat (1) dilakukan dengan cara memantau:
a. kegagalan akses;
b. penggunaan hak akses tidak wajar;
c. alokasi dan penggunaan Hak Akses Khusus;
d. penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan
e. penggunaan sumber daya sensitif.

Pasal 52

Pengendalian pemisahan perangkat pengembangan dan operasional sebagaimana dimaksud dalam Pasal 42 ayat (2) huruf j dilakukan dengan cara:
a. mengembangan dan mengoperasionalkan Perangkat Lunak pada sistem atau prosesor komputer yang berbeda;
b. mengimplementasikan pengembangan Perangkat Lunak mengikuti prosedur manajemen rilis;
c. menjaga agar perangkat pengembangan tidak boleh diakses dari sistem operasional layanan;

d. mengupayakan lingkungan sistem pengujian sama dengan lingkungan sistem operasional layanan;
e. membantu pengguna menggunakan profil pengguna yang berbeda untuk sistem pengujian dan sistem operasional layanan; dan
f. menjaga data yang memiliki klasifikasi sangat rahasia dan rahasia tidak boleh disalin ke dalam lingkungan pengujian sistem.

BAB VII
MANAJEMEN ASET

Pasal 53

Manajemen aset sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf e dilakukan untuk mengamankan Aset Informasi SAK sebagaimana dimaksud dalam Pasal 3 ayat (3) berdasarkan klasifikasi sangat rahasia, rahasia, terbatas, dan publik.

Pasal 54

(1) Manajemen Aset Informasi SAK di lingkungan Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh Unit TIK.
(2) Unit TIK sebagaimana dimaksud pada ayat (1) bertanggung jawab terhadap keamanan Aset Informasi SAK dan bertugas untuk:
    a. mengidentifikasi Aset Informasi SAK dan mendokumentasikannya dalam daftar inventaris Aset Informasi SAK;
    b. menetapkan pemilik Aset Informasi SAK di Unit TIK;
    c. menetapkan Aset Informasi SAK yang terkait dengan Perangkat Pengolah Informasi; dan
    d. menetapkan aturan penggunaan Aset Informasi SAK.
(3) Unit TIK mengkaji dan menetapkan secara berkala klasifikasi Aset Informasi SAK sebagaimana dimaksud pada ayat (2) dan jenis perlindungan keamanannya.

(4) Unit TIK sebagaimana dimaksud pada ayat (3) menetapkan pihak yang dapat mengakses Aset Informasi SAK.

Pasal 55

(1) Klasifikasi sangat rahasia sebagaimana dimaksud dalam Pasal 53 merupakan Aset Informasi SAK yang tidak boleh diketahui oleh orang lain dan apabila didistribusikan kepada yang tidak berhak akan menyebabkan kerugian dan/atau ketahanan SAK nasional.

(2) Klasifikasi rahasia sebagaimana dimaksud dalam Pasal 53 merupakan Aset Informasi SAK yang tidak boleh diketahui oleh orang lain dan apabila didistribusikan kepada yang tidak berhak akan mengganggu kelancaran kegiatan dan mengganggu reputasi Kementerian Dalam Negeri, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, atau Perwakilan Republik Indonesia.

(3) Klasifikasi terbatas sebagaimana dimaksud dalam Pasal 53 merupakan Aset Informasi SAK yang bersifat terbatas dan hanya dapat digunakan oleh pihak yang bersangkutan.

(4) Klasifikasi publik sebagaimana dimaksud dalam Pasal 53 merupakan Aset Informasi SAK yang terbuka untuk umum dengan persetujuan:
   a. Menteri melalui Dirjen untuk lingkup Kementerian Dalam Negeri;
   b. kepala Disdukcapil Provinsi untuk lingkup provinsi;
   c. kepala Disdukcapil Kabupaten/Kota untuk lingkup kabupaten/kota; atau
   d. kepala UPT Disdukcapil Kabupaten/Kota dan kepala Perwakilan Republik Indonesia untuk lingkup wilayah kerjanya.

Pasal 56

(1) Setiap Aset Informasi SAK yang berada di dalam Pusat Data, Pusat Data Cadangan, dan Tempat Layanan

Operasional SIAK dalam penguasaan Unit TIK secara fisik atau sistem.

(2) Aset Informasi SAK sebagaimana dimaksud pada ayat (1) yaitu aset fisik, perangkat keras, Perangkat Lunak, Perangkat Pendukung, dan seluruh data/dokumen elektronik.

(3) Penguasaan secara fisik sebagaimana dimaksud pada ayat (1) dilakukan oleh Unit TIK untuk mengakses dan mengontrol Aset Informasi SAK secara fisik sesuai dengan prosedur.

(4) Penguasaan secara sistem sebagaimana dimaksud pada ayat (1) yaitu Unit TIK mempunyai user akses tingkat administrator pada Perangkat Lunak seperti firmware, sistem operasi, dan aplikasi yang berada di dalam Aset Informasi SAK sesuai dengan prosedur.

Pasal 57

(1) Perangkat Pengolah Informasi dan Perangkat Pendukung di Pusat Data, Pusat Data Cadangan, dan Tempat Layanan Operasional SIAK untuk ditempatkan di lokasi yang aman guna mengurangi risiko Aset Informasi SAK dapat diakses oleh pihak yang tidak berwenang.

(2) Perangkat Pengolah Informasi sebagaimana dimaksud pada ayat (1) dipelihara secara berkala untuk menjamin ketersediaan, keutuhan, dan fungsinya.

(3) Perangkat Pendukung sebagaimana dimaksud pada ayat (1) digunakan untuk menjamin beroperasinya Perangkat Pengolah Informasi dan secara berkala harus diperiksa dan diuji ulang kinerjanya.

(4) Penggunaan perangkat yang dibawa ke luar dari lingkungan Pusat Data, Pusat Data Cadangan, atau Tempat Layanan Operasional SIAK harus disetujui oleh pimpinan Unit TIK.

(5) Perangkat Pengolah Informasi penyimpanan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dihapuskan/dimusnahkan.

(6) Penanganan Perangkat Pengolah Informasi untuk media penyimpan data di Pusat Data, Pusat Data Cadangan, dan Tempat Layanan Operasional SIAK sesuai dengan SOP pengelolaan data elektronik yang dikeluarkan oleh Dirjen.

BAB VIII
MANAJEMEN INSIDEN KEAMANAN INFORMASI

Pasal 58

Manajemen insiden Keamanan Informasi sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf f dilaksanakan untuk mengendalikan pengelolaan gangguan Keamanan Informasi.

Pasal 59

(1) Manajemen insiden Keamanan Informasi di lingkungan Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh Unit TIK.

(2) Unit TIK sebagaimana dimaksud pada ayat (1) bertugas melakukan pengendalian pengelolaan gangguan Keamanan Informasi, dilakukan dengan cara:
   a. melaporkan peristiwa terjadinya gangguan Keamanan Informasi sebagai bentuk pencegahan dan tindakan;
   b. melaksanakan SOP jika terjadi insiden Keamanan Informasi dalam sistem atau layanan TIK;
   c. memberikan tanggung jawab kepada Pegawai untuk memastikan insiden Keamanan Informasi ditangani secara cepat dan efektif; dan
   d. mengumpulkan, menyimpan dan menyajikan bukti pelanggaran terhadap SMKI.

(3) Bentuk pencegahan sebagaimana dimaksud pada ayat (2) huruf a dilakukan dengan menemukan kelemahan Keamanan Informasi dalam sistem atau layanan TIK.

Pasal 60

(1) Pegawai dan Pihak Lain harus melaporkan peristiwa terjadinya insiden Keamanan Informasi kepada pimpinan Unit TIK.

(2) Insiden Keamanan Informasi yang terjadi harus dicatat dalam basis data sebagai masukan dalam penanganan insiden Keamanan Informasi dan bahan evaluasi untuk perbaikan dan pencegahan.

(3) Dalam hal belum terdapat basis data sebagaimana dimaksud pada ayat (2) dicatat pada buku catatan pelaporan insiden Keamanan Informasi.

BAB IX
MANAJEMEN KELANGSUNGAN LAYANAN

Pasal 61

Manajemen kelangsungan layanan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf g dilakukan untuk mengamankan keberlangsungan kegiatan pelayanan pada saat keadaan darurat dan menetapkan kategori resiko sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 62

(1) Manajemen kelangsungan layanan di lingkungan Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota dan Perwakilan Republik Indonesia dilakukan oleh Unit TIK.

(2) Unit TIK sebagaimana dimaksud pada ayat (1) bertugas untuk melakukan:

a. pengelolaan proses kelangsungan kegiatan pada saat keadaan darurat sesuai dengan prosedur kelangsungan kegiatan pada Pusat Data dan/atau Pusat Data Cadangan;

b. penetapan kategori resiko sesuai dengan ketentuan peraturan perundang-undangan;

c. analisis dampak yang ditimbulkan pada saat terjadi keadaan darurat untuk menjamin kelangsungan kegiatan;

d. penyusunan dan penerapan rencana kelangsungan kegiatan untuk menjaga dan mengembalikan kegiatan operasional dalam jangka waktu yang

disepakati dan tingkat kelangsungan yang dibutuhkan;

e. pemeliharaan kelangsungan kegiatan dan memastikan rencana yang termuat dalam rencana kelangsungan kegiatan masih sesuai;

f. identifikasi prioritas untuk kegiatan uji coba rencana kelangsungan kegiatan; dan

g. uji coba rencana kelangsungan kegiatan secara berkala oleh Unit TIK bersama Unit Pengelola Pusat Data/Pusat Data Cadangan.

Pasal 63

Rencana kelangsungan kegiatan sebagaimana dimaksud dalam Pasal 62 ayat (2) huruf d sampai dengan huruf g, meliputi:

a. SOP pengelolaan kelangsungan kegiatan pada saat keadaan darurat, manajemen resiko, analisis dampak kegiatan, pengembalian kondisi semula (*fallback*), peralihan kondisi normal, dan ujicoba kelangsungan kegiatan;

b. menetapkan penanggung jawab dan peran Unit TIK dalam pelaksanaan kelangsungan kegiatan; dan

c. melaksanakan sosialisasi dan pelatihan kelangsungan kegiatan.

BAB X

KENDALI/HAK AKSES

Pasal 64

Kendali/hak akses sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf h dilakukan untuk mengamankan pengendalian akses ke Aset Informasi SAK dan pengendalian akses pengguna.

Pasal 65

(1) Kendali/hak akses terhadap Aset Informasi SAK di lingkungan Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil

Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh Unit TIK.

(2) Unit TIK sebagaimana dimaksud pada ayat (1) bertugas untuk melakukan:

a. penyusunan, pendokumentasikan, dan pengkajian ketentuan akses ke Aset Informasi SAK berdasarkan kebutuhan organisasi dan prasyarat keamanan;
b. pengelolaan akses pengguna;
c. pelaksanaan tanggung jawab pengguna;
d. pengendalian akses jaringan;
e. pengendalian akses ke sistem operasi;
f. pengendalian akses ke aplikasi dan sistem informasi; dan
g. pengendalian perangkat bergerak dan kerja jarak jauh.

Pasal 66

Pengelolaan akses pengguna sebagaimana dimaksud dalam Pasal 65 ayat (2) huruf b dilakukan dengan cara:

a. menyusun prosedur pengelolaan hak akses pengguna sesuai dengan peruntukannya;
b. membatasi dan mengendalikan penggunaan Hak Akses Khusus;
c. mengatur pengelolaan kata sandi pengguna; dan
d. memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya.

Pasal 67

Pelaksanaan tanggung jawab pengguna sebagaimana dimaksud dalam Pasal 65 ayat (2) huruf c dilakukan dengan cara:

a. 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 berhak.

Pasal 68

(1) Pengendalian akses jaringan sebagaimana dimaksud dalam Pasal 65 ayat (2) huruf d diiakukan dengan cara:
   a. mengatur akses pengguna daiam mengakses jaringan di lingkungan Ditjen Dukcapil, Pusat Data, Pusat Data Cadangan, dan/atau Tempat Layanan Operasional SIAK sesuai dengan peruntukannya;
   b. mengatur akses pengguna pemerintah daerah dan lembaga pengguna data ke Pusat Data dan/atau Pusat Data Cadangan sesuai dengan peruntukannya;
   c. menerapkan proses otorisasi penggunaan untuk setiap akses ke dalam jaringan internal melalui koneksi eksternal;
   d. mengakses ke perangkat keras dan Perangkat Lunak untuk melakukan diagnosa harus dikontrol berdasarkan SOP pada Pusat Data/Pusat Data Cadangan dan hanya digunakan untuk Pegawai yang bertugas untuk melakukan pengujian, pemecahan masalah, dan pengembangan sistem;
   e. memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi; dan
   f. menerapkan mekanisme pengendalian akses pengguna sesuai dengan persyaratan pengendalian akses.
(2) Koneksi eksternal sebagaimana dimaksud pada ayat (1) huruf c merupakan suatu akses jaringan komunikasi dari luar Pusat Data kependudukan dan/atau Pusat Data Cadangan kependudukan ke dalam Pusat Data kependudukan dan/atau Pusat Data Cadangan kependudukan.

Pasal 69

Pengendalian akses ke sistem operasi sebagaimana dimaksud dalam Pasal 65 ayat (2) huruf e dilakukan dengan cara:

a. akses ke sistem operasi wajib dikontrol dengan menggunakan sistem manajemen akses pengguna;
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 pengguna;
c. sistem pengelolaan kata sandi harus mudah digunakan dan dapat memastikan kualitas sandi yang dibuat pengguna;
d. 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; dan
f. membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi sangat rahasia dan rahasia.

Pasal 70

Pengendalian akses ke aplikasi dan sistem informasi sebagaimana dimaksud dalam Pasal 65 ayat (2) huruf f dilakukan dengan cara memastikan:

a. akses terhadap aplikasi dan sistem informasi hanya diberikan kepada pengguna sesuai dengan peruntukannya; dan
b. aplikasi dan sistem informasi yang memiliki klasifikasi sangat rahasia dan rahasia wajib diletakkan pada lokasi terpisah untuk mengurangi kemungkinan akses oleh pihak yang tidak berhak.

Pasal 71

Pengendalian perangkat bergerak dan kerja jarak jauh sebagaimana dimaksud dalam Pasal 65 ayat (2) huruf g dilakukan sesuai dengan prosedur penggunaan perangkat bergerak dan kerja jarak jauh untuk menjaga keamanan perangkat informasi di dalamnya.

Pasal 72

(1) Pengendalian akses pengguna sebagaimana dimaksud dalam Pasal 64 di lingkungan Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh Unit TIK.

(2) Unit TIK sebagaimana dimaksud pada ayat (1) bertugas untuk melakukan:
   a. pemenuhan persyaratan pengendalian akses;
   b. pengelolaan akses pengguna;
   c. pengelolaan Hak Akses Khusus;
   d. pengkajian hak akses pengguna dan Hak Akses Khusus;
   e. pengendalian akses jaringan;
   f. pemisahan dalam jaringan; dan
   g. pemantauan penggunaan sistem pengolah informasi.

Pasal 73

Pemenuhan persyaratan pengendalian akses sebagaimana dimaksud dalam Pasal 72 ayat (2) huruf a dilakukan dengan cara:

a. mematuhi Perjanjian Kerahasiaan;
b. menentukan kebutuhan keamanan dari pengolah aset informasi; dan
c. memisah peran pengendalian akses.

Pasal 74

Pengelolaan akses pengguna sebagaimana dimaksud dalam Pasal 72 ayat (2) huruf b dilakukan dengan cara:

a. menggunakan Akun yang unik;
b. menggunakan Akun khusus hanya diperbolehkan sebatas yang diperlukan untuk kegiatan atau alasan operasional;
c. Akun dan Akun khusus sebagaimana dimaksud dalam huruf a dan huruf b harus disetujui pimpinan Unit TIK dan didokumentasikan;
d. memeriksa tingkat akses yang diberikan sesuai dengan tujuan kegiatan dan konsisten dengan SMKI;

e. Pengguna menandatangani pernyataan ketentuan akses yang diberikan;
f. memberikan akses kepada pengguna setelah prosedur otorisasi dilaksanakan;
g. memelihara catatan pengguna layanan (*user log*);
h. menonaktifan akses pengguna yang telah berakhir penugasannya; dan
i. memeriksa dan menonaktifan Akun secara berkala.

Pasal 75

Pengelolaan Hak Akses Khusus sebagaimana dimaksud dalam Pasal 72 ayat (2) huruf c merupakan pengelolaan sistem informasi yang bersifat rahasia dan tidak terbatas pada sistem operasi, perangkat penyimpanan (*storage devices*), file server, dan aplikasi sensitif, yang dilakukan dengan cara:

a. mengidentifikasi Hak Akses Khusus untuk dialokasikan kepada pengguna yang terkait;
b. memberikan Hak Akses Khusus hanya kepada pengguna sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu;
c. mengelola proses otorisasi dan catatan dari seluruh Hak Akses Khusus; dan
d. memberikan Hak Akses Khusus wajib secara terpisah dari Akun yang digunakan untuk kegiatan umum.

Pasal 76

Pengkajian hak akses pengguna dan Hak Akses Khusus sebagaimana dimaksud dalam Pasal 72 ayat (2) huruf d, dilakukan dengan cara:

a. mengkaji ulang dalam periode 6 (enam) bulan sekali atau setelah terjadi perubahan pada sistem atau struktur organisasi atau sewaktu-waktu jika diperlukan; dan
b. memeriksa Hak Akses Khusus dilakukan secara berkala atau sewaktu-waktu.

Pasal 77

Pengendalian akses jaringan sebagaimana dimaksud dalam Pasal 72 ayat (2) huruf e dilakukan dengan cara:

a. menerapkan prosedur otorisasi untuk pemberian akses ke jaringan dan layanan jaringan;
b. menerapkan teknis autentikasi akses dari jaringan eksternal; dan
c. melakukan penghentian layanan jaringan pada area jaringan yang mengalami gangguan Keamanan Informasi.

Pasal 78

Pemisahan jaringan sebagaimana dimaksud dalam Pasal 72 ayat (2) huruf f, dilakukan dengan cara:

a. memisahkan jaringan berdasarkan kelompok layanan informasi, pengguna, dan aplikasi; dan
b. memberikan akses jaringan kepada tamu hanya untuk akses terbatas dan waktu tertentu.

Pasal 79

Pemantauan penggunaan sistem pengolah informasi oleh Unit TIK sebagaimana dimaksud dalam Pasal 72 ayat (2) huruf g dilakukan terhadap:

a. kegagalan akses;
b. penggunaan hak akses tidak wajar;
c. alokasi dan penggunaan Hak Akses Khusus;
d. penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan
e. penggunaan sumber daya sensitif.

BAB XI

PENGENDALIAN KEPATUHAN

Pasal 80

Pengendalian kepatuhan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf i dilaksanakan untuk melakukan pengamanan terhadap pengendalian kepatuhan terhadap penggunaan Aset Informasi SAK dan melakukan pemeriksaan kepatuhan

Pegawai dan Pihak Lain dalam melaksanakan SMKI sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 81

(1) Pengendalian kepatuhan di lingkungan Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh STKI dan/atau Unit TIK.

(2) STKI dan/atau Unit TIK sebagaimana dimaksud pada ayat (1) bertugas untuk:

a. mengidentifikasi, mendokumentasikan, dan memelihara kemutakhiran peraturan perundang-undangan terkait dengan sistem Keamanan Informasi;

b. membuat perencanaan persyaratan, ruang lingkup, dan kegiatan audit yang melibatkan pemeriksaan sistem untuk mengurangi kemungkinan gangguan resiko;

c. melakukan pemeriksaan Perangkat Lunak secara berkala terhadap Perangkat Lunak berlisensi;

d. melakukan pemeriksaan kepatuhan seluruh Pegawai dan Pihak Lain secara berkala untuk menjamin efektivitas pelaksanaan standar dan prosedur Keamanan Informasi; dan

e. memantau dan mengendalikan kepatuhan seluruh Pegawai dan Pihak Lain untuk menaati ketentuan peraturan perundang-undangan mengenai Keamanan Informasi.

Pasal 82

Anggota STKI, Pegawai pada satuan pelaksana SAK, atau Pihak Lain yang melaksanakan tugas di Unit TIK Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia wajib melindungi kepemilikan dan kerahasiaan SAK serta wajib melaksanakan kebijakan dan standar SMKI.

Pasal 83

Pengendalian Kepatuhan dalam melindungi kekayaan intelektual di lingkungan Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia oleh STKI dan Unit TIK dilakukan dengan cara:

a. mendapatkan Perangkat Lunak hanya melalui sumber yang dikenal dan memiliki reputasi baik, untuk memastikan tidak ada pelanggaran hak cipta;
b. memelihara daftar Aset Informasi SAK sesuai dengan 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 terpasang; dan
f. mematuhi terhadap syarat dan kondisi untuk Perangkat Lunak dan informasi yang didapat dari jaringan publik.

Pasal 84

Dalam hal terdapat ketidakpatuhan terhadap SMKI di lingkungan Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia, STKI dan Unit TIK melakukan:

a. evaluasi penyebab ketidakpatuhan;
b. tindakan berdasarkan hasil evaluasi; dan
c. reviu tindakan berdasarkan hasil evaluasi.

Pasal 85

(1) Pengendalian kepatuhan terhadap penggunaan perangkat keras, Perangkat Lunak, dan jaringan komunikasi data telah diimplementasikan secara benar pada sistem informasi di lingkungan Ditjen Dukcapil serta Tempat Layanan Operasional SIAK wajib diperiksa secara berkala atau sewaktu-waktu jika diperlukan.

(2) Pengendalian Kepatuhan sebagaimana dimaksud pada ayat (1) juga mencakup pengujian penetrasi.

(3) Pengujian penetrasi sebagaimana dimaksud pada ayat (2) dilakukan untuk mendeteksi kerentanan sistem dan memeriksa pengendalian akses terhadap sistem yang diterapkan.

BAB XII
PENGEMBANGAN DAN PERAWATAN SISTEM

Pasal 86

Pengembangan dan perawatan sistem sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf j dilakukan untuk memastikan bahwa Keamanan Informasi merupakan bagian yang terintegrasi dengan Aset Informasi SAK, mencegah terjadinya kesalahan, kehilangan, serta modifikasi oleh pihak yang tidak berwenang.

Pasal 87

(1) Pengembangan dan perawatan sistem di lingkungan Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota dan Perwakilan Republik Indonesia dilakukan oleh Unit TIK.

(2) Unit TIK sebagaimana dimaksud pada ayat (1), mempunyai tugas mengendalikan Keamanan Informasi dengan cara melakukan:

a. pendokumentasikan persyaratan Keamanan Informasi yang relevan sebelum pengadaan, pengembangan, atau pemeliharaan sistem informasi baru;
b. pengelolaan informasi pada aplikasi;
c. pengendalian penggunaan Kriptografi;
d. pengamanan file sistem;
e. pengamanan proses pengembangan dan pendukung;
f. pengelolaan kerentanan teknis; dan
g. pengendalian Keamanan Informasi dalam pengadaan, pengembangan, dan pemeliharaan sistem informasi.

Pasal 88

(1) Pengelolaan informasi pada aplikasi sebagaimana dimaksud dalam Pasal 87 ayat (2) huruf b paling sedikit dilakukan dengan cara:
   a. data yang dimasukkan ke dalam aplikasi untuk diperiksa terlebih dahulu kebenaran dan kesesuaiannya;
   b. setiap aplikasi disertakan proses validasi untuk mendeteksi informasi yang dihasilkan lengkap dan sesuai dengan standar pengelolaan informasi pada aplikasi; dan
   c. data keluaran aplikasi harus divalidasi untuk memastikan data yang dihasilkan benar.

(2) Dalam hal data keluaran sebagaimana dimaksud pada ayat (1) huruf c tervalidasi tidak benar, dilakukan penandaan dan pelaporan pengelolaan informasi pada aplikasi.

Pasal 89

Pengendalian penggunaan Kriptografi sebagaimana dimaksud dalam Pasal 87 ayat (2) huruf c digunakan untuk melindungi Aset Informasi SAK yang memiliki klasifikasi sangat rahasia, rahasia, dan terbatas.

Pasal 90

Pengamanan file sistem sebagaimana dimaksud dalam Pasal 87 ayat (2) huruf d dilakukan dengan cara:

a. melaksanakan prosedur pengendalian Perangkat Lunak pada sistem operasi;
b. menentukan sistem pengujian data, melindungi dari kemungkinan kerusakan, kehilangan, atau perubahan oleh pihak yang tidak berwenang; dan
c. mengendalikan kode program *(source code)* secara ketat dan menyalin versi terkini ke tempat yang aman.

Pasal 91

Pengamanan proses pengembangan dan pendukung sebagaimana dimaksud dalam Pasal 87 ayat (2) huruf e dilakukan sesuai dengan SOP pengembangan aplikasi, manajemen rilis, dan manajemen perubahan.

Pasal 92

Pengelolaan kerentanan teknis sebagaimana disebut dalam Pasal 87 ayat (2) huruf f dilakukan sesuai dengan SOP pengelolaan kerentanan teknis dengan cara:

a. mengumpulkan informasi kerentanan teknis secara berkala dari seluruh Aset Informasi SAK yang digunakan; dan
b. melakukan evaluasi dan penilaian resiko terhadap kerentanan teknis yang ditemukan.

Pasal 93

Pengendalian Keamanan Informasi dalam pengadaan, pengembangan, dan pemeliharaan sistem informasi sebagaimana disebut dalam Pasal 87 ayat (2) huruf g paling sedikit dengan cara melakukan:

a. spesifikasi kebutuhan Perangkat Pengolah Informasi yang dikembangkan oleh internal atau Pihak Lain didokumentasikan secara formal;
b. pengembangan sistem informasi mengikuti SOP pengembangan aplikasi;
c. pengendalian penggunaan Kriptografi; dan
d. penerapan SOP pengendalian Perangkat Lunak, pengujian sistem, pengendalian akses, pengendalian perubahan sistem operasi dan Perangkat Lunak, kajian teknis aplikasi, dan pengelolaan kerentanan teknis.

BAB XIII

AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI

Pasal 94

Audit TIK sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf k dilaksanakan untuk melakukan pengamanan pada saat pemeriksaan paling sedikit 1 (satu) kali dalam 1 (satu) tahun terhadap Aset Informasi SAK dan pengujian keamanan sistem.

Pasal 95

(1) Audit TIK di lingkungan Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh auditor TIK.

(2) Auditor TIK sebagaimana dimaksud pada ayat (1) bertugas untuk melakukan:
   a. pemeriksaan secara berkala terhadap Aset Informasi SAK untuk memastikan pengendalian perangkat keras, Perangkat Lunak, dan jaringan komunikasi data telah diimplementasikan secara benar; dan
   b. pengujian penetrasi untuk mendeteksi kerentanan dalam sistem, dan memeriksa pengendalian akses telah diterapkan.

Pasal 96

(1) Pemeriksaan terhadap Aset Informasi SAK sebagaimana dimaksud dalam Pasal 95 ayat (2) huruf a, dengan memenuhi:
   a. persyaratan audit disetujui Menteri melalui Dirjen;
   b. ruang lingkup pemeriksaan/audit disetujui oleh STKI; dan
   c. auditor harus independen dari kegiatan yang diaudit.

(2) Pemenuhan sebagaimana dimaksud dalam pada ayat (1) dilakukan dengan cara:
   a. melakukan pemeriksaan Perangkat Lunak dan data dibatasi untuk akses baca saja;
   b membuat salinan file sistem yang diisolasi dan dihapus bila audit telah selesai;

c. merekam semua akses yang diperiksa dan dipantau serta dicatat untuk menghasilkan jejak audit; dan

d. SOP, persyaratan, dan hasil pemeriksaan harus didokumentasikan.

BAB XIV
PENYIDIK PEGAWAI NEGERI SIPIL ADMINISTRASI KEPENDUDUKAN

Pasal 97

(1) Dalam hal terdapat dugaan pelanggaran SMKI yang berhubungan dengan tindak pidana tertentu, penyidik pegawai negeri sipil Administrasi Kependudukan berwenang melakukan penyidikan sesuai dengan kewenangannya berdasarkan lingkup undang-undang mengenai Administrasi Kependudukan.

(2) STKI memberikan dukungan informasi dan data kepada penyidik pegawai negeri sipil Administrasi Kependudukan dalam melakukan penyidikan sesuai dengan SMKI berdasarkan Peraturan Menteri ini.

(3) Penyidik pegawai negeri sipil Administrasi Kependudukan sebagaimana dimaksud pada ayat (1) diatur sesuai dengan ketentuan peraturan perundang-undangan.

BAB XV
PEMANTAUAN, EVALUASI, DAN PELAPORAN SISTEM MANAJEMEN KEAMANAN INFORMASI

Pasal 98

(1) Menteri melalui Dirjen melakukan pemantauan dan evaluasi terhadap pelaksanaan SMKI.

(2) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) meliputi tata kelola, pengelolaan resiko, kinerja pengelolaan, pengelolaan aset, serta pengelolaan teknologi, dan Keamanan Informasi.

Pasal 99

(1) Pimpinan Unit TIK di lingkungan Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, kepala UPT Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia menyampaikan laporan hasil pemantauan dan evaluasi pelaksanaan SMKI kepada kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, kepala UPT Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia setiap 6 (enam) bulan atau sewaktu-waktu jika dibutuhkan.

(2) Kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, kepala UPT Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia menyampaikan laporan hasil pemantauan dan evaluasi kepada Dirjen pada bulan Desember atau sewaktu-waktu jika dibutuhkan

Pasal 100

(1) STKI menyampaikan laporan atas hasil pemantauan dan evaluasi pelaksanaan SMKI kepada Sekretaris Ditjen Dukcapil setiap 6 (enam) bulan atau sewaktu-waktu jika dibutuhkan.

(2) Sekretaris Ditjen Dukcapil menyampaikan laporan atas hasil pemantauan dan evaluasi pelaksanaan SMKI kepada Dirjen pada bulan Desember atau sewaktu-waktu jika dibutuhkan.

BAB XVI

SANKSI ADMINISTRATIF

Pasal 101

Anggota STKI, Pegawai pada satuan pelaksana SAK, atau Pihak Lain yang melanggar ketentuan Pasal 82 yaitu terhadap perlindungan kepemilikan dan kerahasiaan SAK serta kebijakan dan standar SMKI, dikenakan sanksi administratif berupa:

a. teguran lisan; dan

b. teguran tertulis diberhentikan dari anggota STKI, satuan pelaksana SAK, atau Pihak Lain yang bertugas di Unit TIK.

BAB XVII
PENDANAAN

Pasal 102

Pendanaan pelaksanaan SMKI dibebankan pada anggaran pendapatan dan belanja negara, anggaran pendapatan dan belanja daerah, atau sumber lainnya yang sah dan tidak mengikat.

BAB XVIII
KETENTUAN PENUTUP

Pasal 103

Pada saat Peraturan Menteri ini mulai berlaku, Ditjen Dukcapil menyiapkan SMKI secara bertahap paling lambat Tahun 2023.

Pasal 104

Peraturan Menteri ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Menteri ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 10 November 2021

MENTERI DALAM NEGERI
REPUBLIK INDONESIA,

ttd

MUHAMMAD TITO KARNAVIAN

Diundangkan di Jakarta
pada tanggal 17 November 2021

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd

BENNY RIYANTO

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2021 NOMOR 1272

Salinan sesuai dengan aslinya
Kepala Biro Hukum,

R. Gani Muhamad, SH, MAP
Pembina Utama Muda (IV/c)
NIP. 19690818 199603 1001