

PERATURAN MENTERI DALAM NEGERI REPUBLIK INDONESIA
NOMOR 10 TAHUN 2026
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, sistem manajemen keamanan informasi administrasi kependudukan perlu dilaksanakan secara relevan, komprehensif dan selaras dengan standar keamanan dengan prioritas standar nasional Indonesia bidang keamanan informasi/keamanan siber sesuai dengan ketentuan peraturan perundang-undangan;

b. bahwa Peraturan Menteri Dalam Negeri Nomor 57 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Administrasi Kependudukan sudah tidak sesuai dengan perkembangan standar internasional tentang keamanan informasi untuk keamanan siber dan pelindungan data pribadi serta perkembangan peraturan perundang-undangan, sehingga perlu diganti;

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 Tahun 1945 Negara Kesatuan Republik Indonesia;

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 beberapa kali diubah, terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);
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) sebagaimana telah diubah dengan Undang-Undang Nomor 61 Tahun 2024 tentang Perubahan atas Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 225, Tambahan Lembaran Negara Republik Indonesia Nomor 6994);
5. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820);
6. 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);
7. 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);
8. Peraturan Presiden Nomor 47 tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 99);
9. Peraturan Presiden Nomor 149 Tahun 2024 tentang Kementerian Dalam Negeri (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 345);
10. Peraturan Menteri Dalam Negeri Nomor 95 Tahun 2019 tentang Sistem Informasi Administrasi Kependudukan (Berita Negara Republik Indonesia Tahun 2019 Nomor 1478);
11. 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);
12. Peraturan Menteri Dalam Negeri Nomor 9 Tahun 2025 tentang Organisasi dan Tata Kerja Kementerian Dalam

Negeri (Berita Negara Republik Indonesia Tahun 2025 Nomor 333);

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 terintegrasi mulai dari pendaftaran penduduk, pencatatan sipil, pengelolaan data/informasi, pembinaan aparatur hingga pemanfaatannya dalam rangka penyelenggaraan Administrasi Kependudukan.
3. 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.
4. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, pengelolaan dan penyampaian, atau pemindahan informasi antar sarana/media.
5. Akun adalah identifikasi pengguna yang diberikan oleh unit pengelola TIK, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem TIK.
6. Keamanan Informasi adalah pelindungan aset informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan, dan memastikan ketersediaan sistem dan data Administrasi Kependudukan.
7. Aset Informasi SAK adalah aset yang digunakan untuk memfasilitasi pengelolaan dan pemanfaatan informasi Administrasi Kependudukan.
8. 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.
9. Perjanjian Kerahasiaan *(non-disclosure agreement)* adalah perikatan antara para pihak dengan, Direktorat Jenderal

Kependudukan dan Pencatatan Sipil, Dinas Kependudukan dan Pencatatan Sipil Provinsi, Dinas Kependudukan dan Pencatatan Sipil Kabupaten/Kota dan/atau Perwakilan Republik Indonesia berupa pelarangan penyebarluasan, atau penyalahgunaan bahan rahasia, pengetahuan atau informasi.

10. Kriptografi adalah disiplin ilmu yang mencakup prinsip, cara, dan metode untuk mentransformasi data dengan tujuan menyembunyikan isi informasinya, mencegah modifikasi tanpa terdeteksi, atau mencegah penggunaan tanpa izin.
11. Perangkat Lunak adalah sistem atau aplikasi yang digunakan untuk mendukung sistem informasi Administrasi Kependudukan.
12. Perangkat Keras adalah perangkat komputer, perangkat jaringan dan komunikasi, media penyimpanan data dan perangkat pendukung.
13. Perangkat Pendukung adalah peralatan pendukung untuk menjamin beroperasinya Perangkat Keras, Perangkat Lunak, dan perangkat jaringan serta melindunginya dari kerusakan.
14. Perangkat Pengolah Informasi adalah setiap sistem pengolah informasi, layanan atau infrastruktur fisik dan nonfisik.
15. Pusat Data adalah tempat/ruang penyimpanan Perangkat Keras, Perangkat Lunak, basis data, dan Perangkat Pendukung pada Direktorat Jenderal Kependudukan dan Pencatatan Sipil yang menghimpun dan mengintegrasikan data kependudukan dari hasil pelayanan pendaftaran penduduk dan pencatatan sipil, dengan pertimbangan utama Keamanan Informasi.
16. Pusat Data Cadangan adalah tempat/ruang penyimpanan Perangkat Keras, Perangkat Lunak, basis data cadangan, dan Perangkat Pendukung pada Direktorat Jenderal Kependudukan dan Pencatatan Sipil yang berfungsi untuk pemulihan kejadian luar biasa/bencana yang tidak direncanakan pada Pusat Data guna menjamin keberlangsungan sistem, dengan pertimbangan utama Keamanan Informasi.
17. Satuan Tugas Keamanan Informasi yang selanjutnya disebut STKI adalah satuan tugas yang memiliki tugas dan tanggung jawab dalam pengamanan Aset Informasi SAK.
18. Sistem Informasi Administrasi Kependudukan yang selanjutnya disingkat SIAK adalah sistem informasi yang memanfaatkan TIK yang dilindungi melalui SMKI, untuk memfasilitasi pengelolaan informasi Administrasi Kependudukan di tingkat pusat dan Dinas Kependudukan dan Pencatatan Sipil provinsi/kabupaten/kota/ kecamatan sebagai satu kesatuan.
19. Tempat Layanan Operasional SIAK adalah ruangan Perangkat Keras, Perangkat Lunak, perangkat jaringan komunikasi data, dan sumber daya manusia.
20. 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.

21. Pelindungan Data Pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi.
22. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik *(electronic mail),* telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
23. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
24. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan dalam negeri.
25. Direktorat Jenderal Kependudukan dan Pencatatan Sipil yang selanjutnya disebut Ditjen adalah direktorat jenderal pada kementerian yang menyelenggarakan urusan pemerintahan dalam negeri yang bertanggung jawab untuk melaksanakan tugas menyelenggarakan perumusan dan pelaksanaan kebijakan di bidang kependudukan dan pencatatan sipil sesuai dengan ketentuan perundang-undangan.
26. 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.
27. Dinas Kependudukan dan Pencatatan Sipil Provinsi yang selanjutnya disebut Disdukcapil Provinsi adalah perangkat pemerintah provinsi yang membidangi urusan Administrasi Kependudukan.
28. Dinas Kependudukan dan Pencatatan Sipil Kabupaten/Kota yang selanjutnya disebut Disdukcapil Kabupaten/Kota adalah perangkat daerah kabupaten/kota selaku instansi pelaksana yang membidangi urusan Administrasi Kependudukan
29. Perwakilan Republik Indonesia adalah Kedutaan Besar Republik Indonesia, Konsulat Jenderal Republik Indonesia, dan Konsulat Republik Indonesia di luar wilayah Negara Kesatuan Republik Indonesia.
30. 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.

31. Pihak Lain adalah pihak selain Ditjen Dukcapil, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia yang terkait dengan pelaksanaan SMKI.
32. Pegawai adalah aparatur sipil negara dan pegawai lainnya yang melaksanakan tugas dalam jabatan, pekerjaan atau kegiatan yang terkait dengan pengamanan Aset Informasi SAK sesuai dengan tugas dan fungsinya.

BAB II
PENYELENGGARAAN SISTEM MANAJEMEN KEAMANAN INFORMASI

Bagian Kesatu
Umum

Pasal 2

(1) Penyelenggaraan SMKI dilaksanakan dengan menerapkan Standar Nasional Indonesia *International Organization for Standardization/International Electrotechnical Commission* 27001 (SNI ISO/IEC 27001).
(2) Penyelenggaraan 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.
(3) Dalam pelaksanaan SMKI sebagaimana dimaksud pada ayat (1) dan (2) dilakukan kontrol keamanan terhadap:
    a. organisasi;
    b. sumber daya manusia;
    c. fisik lingkungan; dan
    d. teknologi.

Bagian Kedua
Tata Kelola Keamanan Informasi

Pasal 3

Tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf a dilakukan untuk mengamankan pengelolaan Keamanan Informasi Administrasi Kependudukan.

Pasal 4

(1) Tata kelola Keamanan Informasi di lingkungan Ditjen dilaksanakan oleh Dirjen bersama dengan Sekretaris

Ditjen selaku koordinator STKI, serta pejabat pimpinan tinggi pratama, dan tim STKI.

(2) Tata kelola Keamanan Informasi di Disdukcapil Provinsi dilaksanakan oleh kepala Disdukcapil Provinsi bersama dengan Sekretaris Disdukcapil Provinsi selaku koordinator STKI di tingkat provinsi, dan tim STKI.

(3) Tata kelola Keamanan Informasi di Disdukcapil Kabupaten/Kota dan di UPT Disdukcapil Kabupaten/Kota dilaksanakan oleh kepala Disdukcapil Kabupaten/Kota bersama dengan Sekretaris Disdukcapil Kabupaten/Kota, selaku koordinator STKI di tingkat kabupaten/kota dan tim STKI.

(4) Tata kelola Keamanan Informasi di Perwakilan Republik Indonesia dilaksanakan oleh kepala Perwakilan Republik Indonesia.

Pasal 5

Koordinator STKI di Ditjen sebagaimana dimaksud dalam Pasal 4 ayat (1) bertugas untuk:

a. membuat rencana dan target Keamanan Informasi setiap tahunnya;
b. memastikan kebijakan dan standar SMKI diterapkan secara efektif sesuai dengan standar indeks Keamanan Informasi yang ditetapkan oleh kementerian/lembaga terkait;
c. memastikan langkah perbaikan sudah dilakukan berdasarkan saran dan rekomendasi yang diberikan Tim STKI dalam pelaksanaan evaluasi dan/atau audit penerapan kebijakan dan standar SMKI;
d. memastikan peningkatan kesadaran, kepedulian, dan kepatuhan seluruh Pegawai terhadap kebijakan dan standar SMKI;
e. memastikan terlaksananya audit internal dan kaji ulang manajemen (*management review)* terhadap kebijakan dan standar SMKI sesuai dengan indeks Keamanan Informasi yang ditetapkan oleh kementerian/lembaga terkait;
f. memastikan pelaksanaan penanganan gangguan Keamanan Informasi antar unit kerja di lingkungan Ditjen; dan
g. melaporkan kinerja pelaksanaan dan evaluasi penerapan kebijakan dan standar SMKI kepada Dirjen yang akan digunakan sebagai dasar peningkatan Keamanan Informasi.

Pasal 6

Koordinator STKI di Provinsi, dan koordinator STKI Kabupaten/Kota sebagaimana dimaksud dalam Pasal 4 ayat (2) dan ayat (3) bertugas untuk:

a. memastikan kebijakan dan standar SMKI diterapkan secara efektif sesuai dengan standar indeks Keamanan Informasi yang ditetapkan oleh kementerian/lembaga terkait;
b. memastikan langkah perbaikan sudah dilakukan berdasarkan saran dan rekomendasi yang diberikan Tim STKI Ditjen dalam pelaksanaan evaluasi 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 dan kaji ulang manajemen (*management review)* 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 Disdukcapil; dan
f. melaporkan kinerja pelaksanaan dan evaluasi penerapan kebijakan dan standar SMKI kepada kepala Disdukcapil yang akan digunakan sebagai dasar peningkatan Keamanan Informasi.

Pasal 7

Pejabat pimpinan tinggi pratama pada Ditjen, kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, kepala UPT Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia sebagaimana dimaksud dalam Pasal 4 bertanggung jawab untuk:
a. melaksanakan kebijakan dan standar SMKI;
b. mengawasi penerapan kebijakan dan standar SMKI;
c. memberikan masukan melalui koordinator STKI untuk meningkatkan penerapan kebijakan dan standar SMKI;
d. mendefinisikan kebutuhan, merekomendasikan, dan memfasilitasi penyelenggaraan pendidikan dan pelatihan Keamanan Informasi bagi Pegawai;
e. memantau, mencatat, menguraikan, dan menindaklanjuti gangguan Keamanan Informasi yang diketahui atau dilaporkan sesuai dengan prosedur pelaporan gangguan Keamanan Informasi; dan
f. memfasilitasi penyelesaian masalah Keamanan Informasi.

Pasal 8

Pejabat pimpinan tinggi pratama pada Ditjen, kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia sebagaimana dimaksud dalam Pasal 7 bertugas untuk:
a. menyusun tim STKI;
b. menghentikan hak penggunaan Aset Informasi SAK Pegawai yang sedang dalam pemeriksaan dan/atau menjalani proses hukum terkait dengan dugaan pelanggaran SMKI;
c. mencabut hak akses terhadap akses informasi SAK Pegawai dan Pihak Lain tidak lagi bekerja pada Ditjen, Perwakilan Republik Indonesia, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, dan UPT Disdukcapil Kabupaten/Kota;
d. mengembalikan seluruh Aset Informasi SAK tim STKI yang berhenti bekerja atau mutasi dengan berita acara serah terima;
e. melakukan pemeriksaan dokumen latar belakang kompetensi, pekerjaan dan hal lain Pihak Lain yang akan bekerja sama dalam penggunaan Aset Informasi SAK

dengan memperhitungkan privasi dan Pelindungan Data Pribadi berdasarkan standar SMKI sesuai dengan peraturan perundang-undangan; dan

f. melaksanakan pendidikan, pelatihan dan/atau sosialisasi keamanan sistem informasi kepada tim STKI dan Pegawai lainnya yang terkait.

Pasal 9

Pemeriksaan latar belakang Pihak Lain sebagaimana dimaksud dalam Pasal 8 huruf e dilakukan melalui wawancara dengan pemeriksaan dokumen.

Pasal 10

Pihak Lain dalam melaksanakan keamanan aset informasi SAK:

a. menggunakan perangkat komputer yang sudah dilakukan proses *hardening* oleh tim STKI selama bekerja di lingkungan Ditjen khususnya di area Pusat Data, Pusat Data Cadangan, dan/atau Tempat Layanan Operasional SIAK;
b. mematuhi untuk tidak menyimpan Aset Informasi SAK di dalam perangkat elektronik apapun selama bekerja di lingkungan Ditjen khususnya di area Pusat Data, Pusat Data Cadangan, dan/atau Tempat Layanan Operasional SIAK; dan
c. mengembalikan seluruh Aset Informasi SAK yang dipergunakan selama bekerja, apabila berhenti bekerja atau berakhir masa kontraknya.

Pasal 11

(1) Pejabat pimpinan tinggi pratama di Ditjen, kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia sebagaimana dimaksud dalam Pasal 7 menetapkan penanggung jawab Aset Informasi SAK, sesuai dengan tugas dan fungsi dari struktur jabatan.
(2) Penanggungjawab Aset Informasi SAK sebagaimana dimaksud pada ayat (1) menerapkan aturan penggunaan Aset Informasi SAK sesuai dengan SOP Tata Kelola Aset Informasi SAK, dengan bantuan teknis dari tim STKI.

Pasal 12

Pengendalian dokumen yang terkait dengan pelaksanaan SMKI di Ditjen, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota oleh tim STKI dengan menempatkan dokumen di semua area operasional agar mudah diakses oleh pengguna di tingkat Ditjen, provinsi dan kabupaten/kota.

Pasal 13

(1) Pegawai pada Ditjen, 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 dalam melaksanakan tanggung jawab sebagaimana dimaksud pada ayat (1) menandatangani

Perjanjian Kerahasiaan (*non-disclosure agreement*) dengan Dirjen, kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia.

Pasal 14

(1) Pihak Lain yang ikut serta terhadap pelaksanaan keamanan Aset Informasi SAK wajib menjaga kerahasiaan informasi.
(2) Pihak Lain dalam menjaga kerahasiaan informasi sebagaimana dimaksud pada ayat (1) menandatangani Perjanjian Kerahasiaan (*non-disclosure agreement*) dengan Dirjen, kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, kepala UPT Disdukcapil Kabupaten/Kota, dan kepala Perwakilan Republik Indonesia.
(3) Perjanjian Kerahasiaan (*non-disclosure agreement*) sebagaimana dimaksud dalam Pasal 13 ayat (2), paling sedikit memuat:
    a. pelindungan 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.

Bagian Ketiga
Keamanan Sumber Daya Manusia

Pasal 15

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

Pasal 16

(1) Peningkatan kapasitas sumber daya manusia terkait dengan pelaksanaan SMKI di lingkungan Ditjen dan Perwakilan Republik Indonesia dilakukan oleh Dirjen bersama dengan Sekretaris Ditjen selaku koordinator STKI, serta pejabat pimpinan tinggi pratama dan tim STKI.
(2) Peningkatan kapasitas sumber daya manusia di Disdukcapil Provinsi dilakukan oleh kepala Disdukcapil Provinsi dan tim STKI.
(3) Peningkatan kapasitas terhadap sumber daya manusia di Disdukcapil Kabupaten/Kota dan terhadap sumber daya manusia di UPT Disdukcapil Kabupaten/Kota dilakukan oleh kepala Disdukcapil Kabupaten/Kota dan tim STKI.

Bagian Keempat
Keamanan Fisik dan Lingkungan

Pasal 17

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 18

(1) Keamanan fisik dan lingkungan di Ditjen, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilaksanakan oleh tim STKI.
(2) Dalam melaksanakan keamanan fisik dan lingkungan Tim STKI sebagaimana dimaksud pada ayat (1) melakukan:
    a. pemeliharaan perangkat elektronik sesuai dengan petunjuk manualnya;
    b. pengamanan area Pusat Data, Pusat Data Cadangan, dan/atau Tempat Layanan Operasional SIAK;
    c. pengamanan kantor, ruangan, dan fasilitas;
    d. pelindungan terhadap ancaman eksternal dan lingkungan;
    e. penempatan dan pelindungan perangkat; dan
    f. pengamanan instalasi kabel, power (tenaga listrik) dan sistem pendingin di Pusat Data, Pusat Data Cadangan, dan/atau Tempat Layanan Operasional SIAK.

Pasal 19

(1) Pemeliharaan perangkat elektronik sebagaimana dimaksud dalam Pasal 18 ayat (2) huruf a dilakukan dengan cara mencatat serta menyimpan data Aset Informasi SAK yang digunakan.
(2) Dalam hal pemeliharaan sebagaimana dimaksud pada ayat (1) dilakukan oleh Pihak Lain, pelaksanaannya dilakukan dengan membuat perjanjian kerjasama dan Perjanjian Kerahasiaan *(non-disclosure agreement).*

Pasal 20

Pengamanan area Pusat Data, Pusat Data Cadangan, dan/atau Tempat Layanan Operasional SIAK sebagaimana dimaksud dalam Pasal 18 ayat (2) huruf b dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 21

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

Pasal 22

Pengamanan kantor, ruangan, dan fasilitas sebagaimana dimaksud dalam Pasal 18 ayat (2) huruf c dilakukan dengan cara pembatasan pemberian identitas atau tanda keberadaan aktivitas pengolahan informasi.

Bagian Kelima
Keamanan Operasional dan Komunikasi

Pasal 23

Keamanan operasional dan komunikasi sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf d dilakukan untuk:

a. memastikan operasional yang aman dan benar pada Aset Informasi SAK;
b. mengimplementasikan dan memelihara keamanan Aset Informasi SAK;
c. mengelola layanan yang diberikan oleh Pihak Lain;
d. meminimalkan risiko kegagalan;
e. melindungi keutuhan dan ketersediaan Aset Informasi SAK; dan
f. memastikan keamanan akses dan pertukaran informasi melalui jaringan komunikasi yang bersifat tertutup/ *Virtual Private Network (VPN).*

Pasal 24

(1) Keamanan operasional dan komunikasi di lingkungan Ditjen, Disdukcapil Provinsi, Disdukcapil Kabupaten/ Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh tim STKI.
(2) Tim STKI 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. pelindungan terhadap ancaman program yang membahayakan;
    e. Pelindungan Data Pribadi;
    f. data cadangan;
    g. pengelolaan keamanan sistem informasi;
    h. penanganan media penyimpanan data;
    i. pertukaran informasi;
    j. pemantauan penggunaan sistem pengolah informasi; dan.
    k. pemisahan perangkat pengembangan dan operasional.

Bagian Keenam
Manajemen Aset

Pasal 25

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

Pasal 26

(1) Manajemen Aset Informasi SAK di lingkungan Ditjen, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh tim STKI.

(2) Tim STKI sebagaimana dimaksud pada ayat (1) bertanggung jawab terhadap keamanan Aset Informasi SAK untuk:
   a. mengidentifikasi Aset Informasi SAK dan mendokumentasikannya dalam daftar inventaris Aset Informasi SAK;
   b. menetapkan pemilik Aset Informasi SAK di tim STKI;
   c. menetapkan Aset Informasi SAK yang terkait dengan Perangkat Pengolah Informasi; dan
   d. menetapkan aturan penggunaan Aset Informasi SAK.

(3) Tim STKI mengkaji dan menetapkan secara berkala klasifikasi Aset Informasi SAK sebagaimana dimaksud pada ayat (1) dan jenis pelindungan keamanannya.

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

Pasal 27

(1) Klasifikasi sangat rahasia sebagaimana dimaksud dalam Pasal 25 merupakan Aset Informasi SAK yang tidak boleh diketahui oleh orang lain dan apabila didistribusikan kepada yang tidak berhak akan menyebabkan kerugian dan/atau kerentanan SAK nasional.

(2) Klasifikasi rahasia sebagaimana dimaksud dalam Pasal 25 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 yang menyelenggarakan urusan pemerintahan dalam negeri, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, atau Perwakilan Republik Indonesia.

(3) Klasifikasi terbatas sebagaimana dimaksud dalam Pasal 25 merupakan Aset Informasi SAK yang bersifat terbatas dan hanya dapat digunakan oleh pihak yang bersangkutan.

(4) Klasifikasi publik sebagaimana dimaksud dalam Pasal 25 merupakan Aset Informasi SAK yang terbuka untuk umum dengan persetujuan:
   a. Dirjen untuk lingkup Ditjen dan Perwakilan Republik Indonesia;
   b. kepala Disdukcapil Provinsi untuk lingkup provinsi; dan
   c. kepala Disdukcapil Kabupaten/Kota untuk lingkup kabupaten/kota.

Pasal 28

(1) Setiap Aset Informasi SAK yang berada di dalam Pusat Data, Pusat Data Cadangan, dan/atau Tempat Layanan Operasional SIAK dalam penguasaan tim STKI secara fisik atau sistem.

(2) Penguasaan secara fisik sebagaimana dimaksud pada ayat (1) dilakukan oleh tim STKI untuk mengakses dan mengontrol Aset Informasi SAK secara fisik sesuai dengan SOP.

(3) Penguasaan secara sistem sebagaimana dimaksud pada ayat (1) yaitu tim STKI mempunyai user akses tingkat

administrator pada Perangkat Lunak seperti *firmware*, sistem operasi, dan aplikasi yang berada di dalam Aset Informasi SAK sesuai dengan SOP.

Pasal 29

(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 kerahasiaan, keutuhan, ketersediaan, 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 dari luar ke lingkungan Pusat Data, Pusat Data Cadangan, atau Tempat Layanan Operasional SIAK atau sebaliknya harus dilakukan proses *hardening* dan disetujui oleh tim STKI.
(5) Perangkat Pengolah Informasi penyimpanan data yang sudah tidak digunakan lagi harus disanitasi secara aman sebelum digunakan kembali atau dihapuskan/dimusnahkan.

Bagian Ketujuh
Manajemen Insiden Keamanan Informasi

Pasal 30

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

Pasal 31

(1) Manajemen insiden Keamanan Informasi di lingkungan Ditjen, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh tim STKI.
(2) Tim STKI 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 mencakup manajemen insiden siber.
    b. mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap SMKI.

Pasal 32

(1) Pegawai dan Pihak Lain harus melaporkan peristiwa terjadinya insiden Keamanan Informasi kepada tim STKI.
(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.

Bagian Kedelapan
Manajemen Kelangsungan Layanan

Pasal 33

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

Pasal 34

(1) Manajemen kelangsungan layanan di lingkungan Ditjen, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh tim STKI.
(2) Tim STKI sebagaimana dimaksud pada ayat (1) melakukan:
    a. pengelolaan proses kelangsungan kegiatan pada saat keadaan darurat di Pusat Data dan/atau Pusat Data Cadangan sesuai dengan SOP;
    b. penetapan kategori risiko 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; dan
    e. pemeliharaan kelangsungan kegiatan dan memastikan rencana yang termuat dalam rencana kelangsungan kegiatan masih sesuai.

Pasal 35

Rencana kelangsungan kegiatan dan pemeliharaan kelangsungan kegiatan sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf d dan e meliputi:
a. penyusunan SOP pengelolaan kelangsungan kegiatan pada saat keadaan darurat, manajemen risiko, analisis dampak kegiatan, pengembalian kondisi semula *(fallback)* dan peralihan kondisi normal; dan
b. menetapkan penanggungjawab dan tim STKI dalam pelaksanaan kelangsungan kegiatan.

Bagian Kesembilan
Kendali Hak Akses

Pasal 36

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

Pasal 37

Kendali hak akses terhadap Aset Informasi SAK di lingkungan Ditjen, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia, dilakukan oleh tim STKI.

Pasal 38

Pengelolaan akses pengguna dilakukan dengan cara:

a. menyusun SOP pengelolaan hak akses pengguna sesuai dengan peruntukannya;
b. membatasi dan mengendalikan penggunaan Hak Akses Khusus;
c. mengatur pengelolaan kata sandi pengguna;
d. memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya; dan
e. memonitor dan menutup hak akses yang tidak aktif hasil evaluasi.

Pasal 39

Pelaksanaan tanggung jawab pengguna dilakukan dengan cara:

a. mematuhi aturan pembuatan dan penggunaan kata sandi;
b. memastikan Perangkat Pengolah Informasi yang digunakan mendapatkan pelindungan terutama saat ditinggalkan; dan
c. melindungi informasi agar tidak diakses oleh pihak yang tidak berhak.

Pasal 40

Pengendalian akses jaringan dilakukan dengan cara:

a. mengatur akses pengguna dalam mengakses jaringan di lingkungan Ditjen, 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.

Pasal 41

Pengendalian akses ke aplikasi dan sistem informasi dilakukan dengan cara memastikan akses terhadap aplikasi dan sistem

informasi hanya diberikan kepada pengguna sesuai dengan peruntukannya.

Pasal 42

Pengendalian perangkat bergerak dan kerja jarak jauh dilakukan sesuai dengan SOP penggunaan perangkat bergerak dan kerja jarak jauh untuk menjaga keamanan perangkat informasi di dalamnya.

Pasal 43

Dalam rangka pengendalian akses informasi SAK dan akses pengguna dilakukan pemantauan dan evaluasi oleh tim STKI 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. berkas digital (*log files)* atau *security incident event management* (SIEM).

Bagian Kesepuluh
Pengendalian Kepatuhan

Pasal 44

Pengendalian kepatuhan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf i dilaksanakan untuk melakukan pengamanan terhadap penggunaan Aset Informasi SAK dan melakukan pemeriksaan kepatuhan pengguna dan/atau Pihak Lain sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 45

Pengendalian kepatuhan di lingkungan Ditjen, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh tim STKI.

Pasal 46

Tim STKI, Pegawai pada satuan pelaksana SAK, dan/atau Pihak Lain yang melaksanakan tugas di Ditjen, 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 47

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

a. mendapatkan Perangkat Lunak hanya melalui sumber resmi dan memiliki reputasi baik;
b. membuat daftar Aset Informasi SAK sesuai dengan persyaratan;

c. mendokumentasikan bukti kepemilikan lisensi, *master disk*, *source code*, buku manual, dan lain sebagainya;
d. melakukan pemeriksaan dan memastikan bahwa hanya Perangkat Lunak dan produk berlisensi yang terpasang; dan
e. mematuhi terhadap syarat dan kondisi yang sudah ditentukan untuk Perangkat Lunak dan informasi yang didapat dari jaringan publik.

Pasal 48

Dalam hal terdapat ketidakpatuhan terhadap SMKI di lingkungan Ditjen, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia tim STKI melakukan:
a. evaluasi penyebab ketidakpatuhan;
b. tindakan berdasarkan hasil evaluasi; dan
c. reviu tindakan berdasarkan hasil evaluasi.

Pasal 49

Pengendalian kepatuhan terhadap penggunaan Perangkat Keras, Perangkat Lunak, dan jaringan komunikasi data pada SIAK di lingkungan Ditjen serta Tempat Layanan Operasional SIAK wajib diperiksa secara berkala atau sewaktu-waktu jika diperlukan.

Bagian Kesebelas
Pengembangan dan Perawatan Sistem

Pasal 50

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, untuk mencegah terjadinya kesalahan, kehilangan, serta modifikasi oleh pihak yang tidak berwenang.

Pasal 51

(1) Pengembangan dan perawatan sistem di lingkungan Ditjen, Disdukcapil Provinsi, Disdukcapil Kabupaten/ Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh tim STKI.
(2) Tim STKI sebagaimana dimaksud pada ayat (1), mengendalikan Keamanan Informasi dengan cara melakukan:
    a. pendokumentasian dan pengendalian Keamanan Informasi yang relevan sebelum pengadaan, pengembangan, atau pemeliharaan sistem informasi;
    b. pengelolaan informasi pada aplikasi;
    c. pengendalian penggunaan Kriptografi;
    d. pengujian penetrasi;
    e. pengamanan file atau data;
    f. pengamanan proses pengembangan dan pendukung; dan
    g. pengelolaan kerentanan teknis.

Pasal 52

Pengendalian Keamanan Informasi yang relevan sebelum pengadaan, pengembangan, dan pemeliharaan sistem informasi sebagaimana dimaksud dalam Pasal 51 ayat (2) huruf a 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.

Pasal 53

(1) Pengelolaan informasi pada aplikasi sebagaimana dimaksud dalam Pasal 51 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 54

Pengendalian penggunaan Kriptografi sebagaimana dimaksud dalam Pasal 51 ayat (2) huruf c digunakan untuk melindungi Aset Informasi SAK yang memiliki klasifikasi sangat rahasia, rahasia, dan terbatas.

Pasal 55

Pengamanan file atau data sebagaimana dimaksud dalam Pasal 51 ayat (2) huruf e dilakukan dengan cara:

a. melaksanakan SOP pengendalian Perangkat Lunak;
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 pemutakhiran versi terkini ke tempat yang aman.

Pasal 56

Pengamanan proses pengembangan dan pendukung sebagaimana dimaksud dalam Pasal 51 ayat (2) huruf f dilakukan sesuai dengan SOP pengembangan aplikasi, manajemen rilis, dan manajemen perubahan.

Pasal 57

Pengelolaan kerentanan teknis sebagaimana disebut dalam Pasal 51 ayat (2) huruf g dilakukan sesuai dengan SOP pengelolaan kerentanan teknis dengan cara:

a. mengumpulkan informasi kerentanan teknis secara berkala dari seluruh Aset Informasi SAK yang digunakan;
b. melakukan evaluasi dan penilaian risiko terhadap kerentanan teknis yang ditemukan; dan
c. melakukan koreksi dan tindakan korektif jika ditemukan kerentanan teknis sesuai dengan SOP.

Bagian Kedua Belas
Audit Teknologi Informasi dan Komunikasi

Pasal 58

Audit TIK sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf k dilaksanakan untuk memastikan Keamanan Informasi paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan/atau sewaktu-waktu jika dibutuhkan terhadap Aset Informasi SAK dan pengujian keamanan sistem.

Pasal 59

(1) Audit TIK di lingkungan Ditjen, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia dilakukan oleh tim STKI.
(2) Tim STKI 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 60

Pemeriksaan secara berkala terhadap Aset Informasi SAK sebagaimana dimaksud dalam Pasal 59 ayat (2) huruf a, dengan memenuhi persyaratan audit merujuk pada Standar Nasional Indonesia *International Organization for Standardization/International Electrotechnical Commission* 27001 (SNI ISO/IEC 27001).

BAB III
PENANGGUNGJAWAB DAN PELAKSANA
SISTEM MANAJEMEN KEAMANAN INFORMASI ADMINISTRASI KEPENDUDUKAN

Pasal 61

Dalam pelaksanaan SMKI Menteri melalui Dirjen bertanggungjawab untuk melindungi dan menjamin kerahasiaan, keutuhan, dan ketersediaan Aset Informasi SAK dalam bentuk:

a. data dan/atau dokumen;
b. Perangkat Lunak;

c. Perangkat Keras;
d. perangkat jaringan; dan
e. pengguna *(brainware).*

Pasal 62

(1) Data dan/atau dokumen sebagaimana dimaksud dalam Pasal 61 huruf a, merupakan Informasi Elektronik dan/atau Dokumen Elektronik.
(2) Data dan/atau dokumen sebagaimana dimaksud pada ayat (1) paling sedikit terdiri dari:
    a. data kependudukan,
    b. data demografik,
    c. data biometrik penduduk,
    d. data balikan dari lembaga pengguna,
    e. data agregat kependudukan,
    f. daftar penduduk pemilih potensial pemilihan,
    g. file konfigurasi *secure access module card*,
    h. data Akun pengguna sistem,
    i. daftar *internet protocol* sistem,
    j. data hasil pemadanan data kepada pengguna,
    k. data konfigurasi Perangkat Keras,
    l. data kode sumber *(source code)* aplikasi,
    m. dokumen Perjanjian Kerahasiaan *(non-disclosure agreement),*
    n. dokumen Administrasi Kependudukan yang ditandatangani secara elektronik,
    o. dokumen hasil audit Keamanan Informasi, dan
    p. data masking *(hash)* dan data enkripsi.
(3) Perangkat Lunak sebagaimana dimaksud dalam Pasal 61 huruf b paling sedikit aplikasi, sistem operasi, lisensi, *firmware* dan perangkat bantu pengembangan sistem/aplikasi.
(4) Perangkat Keras sebagaimana dimaksud dalam Pasal 61 huruf c paling sedikit komputer *client*, *server*, perangkat jaringan komunikasi, media penyimpanan data, dan Perangkat Pendukung seperti *uninterruptible power supply,* genset, dan *cooling system.*
(5) Perangkat jaringan sebagaimana dimaksud dalam Pasal 61 huruf d merupakan perangkat jaringan komunikasi dan data termasuk paling sedikit *modem, hub, switch, router, firewall, proxy, machine-to-machine (mobile connectivity service),* sistem pengkabelan dan perangkat keamanan.
(6) Pengguna *(brainware)* sebagaimana dimaksud dalam Pasal 61 huruf e merupakan sumber daya manusia dengan kompetensi paling sedikit pengetahuan, pengalaman, keahlian dan sikap kerja.

Pasal 63

(1) Dirjen dalam melaksanakan tanggung jawab sebagaimana dimaksud dalam Pasal 61 dibantu oleh STKI selaku pelaksana SMKI.
(2) STKI sebagaimana dimaksud pada ayat (1) berkedudukan di Ditjen, Disdukcapil Provinsi dan Disdukcapil Kabupaten/Kota.

(3) STKI di Ditjen sebagaimana dimaksud pada ayat (2) dikoordinasikan oleh Sekretaris Ditjen dan beranggotakan pejabat pimpinan tinggi pratama dengan dibantu oleh ASN dan/atau tenaga ahli di lingkungan Ditjen.
(4) STKI di Disdukcapil Provinsi sebagaimana dimaksud pada ayat (2) dikoordinasikan oleh Sekretaris Disdukcapil Provinsi serta beranggotakan pejabat administrator dengan dibantu oleh ASN di lingkungan Disdukcapil Provinsi.
(5) STKI di Disdukcapil Kabupaten/Kota sebagaimana dimaksud pada ayat (2) dikoordinasikan oleh Sekretaris Disdukcapil Kabupaten/Kota serta beranggotakan pejabat administrator dengan dibantu oleh ASN di Disdukcapil Kabupaten/Kota, dan ASN di UPT Disdukcapil Kabupaten/Kota.
(6) Struktur STKI sebagaimana dimaksud pada ayat (3) ditetapkan dengan Keputusan Menteri.
(7) Struktur STKI sebagaimana dimaksud pada ayat (4) dan ayat (5) ditetapkan dengan Keputusan Kepala Daerah.

Pasal 64

STKI sebagaimana dimaksud dalam Pasal 63 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 Pelindungan Data Pribadi;
d. melakukan pemetaan keperluan Keamanan Informasi;
e. melakukan audit internal SMKI dan kaji ulang manajemen *(management review);*
f. melakukan pemantauan dan evaluasi terhadap pelaksanaan SMKI di Ditjen, Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota dan Perwakilan Republik Indonesia secara berkala untuk meningkatkan Keamanan Informasi;
g. mengidentifikasi dan mengkaji secara berkala persyaratan untuk menjaga kerahasiaan Aset Informasi SAK yang dituangkan dalam dokumen kerahasiaan; dan
h. menyampaikan laporan dan rekomendasi pelaksanaan SMKI kepada Dirjen melalui Sekretaris Ditjen selaku koordinator STKI.

Pasal 65

(1) Dalam melaksanakan tugas dan tanggung jawab untuk melakukan pemetaan Keamanan Informasi sebagaimana dimaksud dalam Pasal 64 huruf d STKI harus memiliki kompetensi dan/atau keahlian yang memadai.
(2) Pemetaan 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 66

(1) Tugas dan tanggungjawab melakukan audit internal SMKI sebagaimana dimaksud dalam Pasal 64 huruf e STKI dapat menunjuk pihak yang berkompeten di bidang audit teknologi informasi.
(2) Audit internal SMKI dan kaji ulang manajemen sebagaimana dimaksud dalam Pasal 64 huruf e dilakukan oleh Sekretaris Disdukcapil Provinsi, Kabupaten/Kota dengan menyampaikan laporan dan rekomendasi pelaksanaan SMKI kepada kepala Disdukcapil sebagai penanggungjawab SMKI di tingkat provinsi dan kabupaten/kota.

Pasal 67

(1) Tugas dan tanggung jawab menyampaikan laporan dan rekomendasi pelaksanaan SMKI sebagaimana dimaksud dalam Pasal 64 huruf h 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 atas:
a. formulir yang ditetapkan dalam SOP Keamanan Informasi;
b. catatan gangguan Keamanan Informasi;
c. catatan dari sistem*;*
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 (*non-disclosure agreement*);
h. laporan audit internal dan kaji ulang manajemen (*management review*); dan
i. laporan hasil asesmen pihak eksternal dalam rangka sertifikasi Standar Nasional Indonesia *International Organization for Standardization/International Electrotechnical Commission* 27001 (SNI ISO/IEC 27001).

Pasal 68

(1) Pelaksanaan SMKI sebagaimana dimaksud dalam Pasal 61 di Ditjen dilaksanakan sesuai dengan Keputusan Menteri sebagaimana dimaksud dalam Pasal 63 ayat (6).
(2) Pelaksanaan SMKI sebagaimana dimaksud dalam Pasal 61 di Disdukcapil Provinsi dilaksanakan sesuai dengan

Keputusan Kepala Daerah sebagaimana dimaksud dalam Pasal 63 ayat (7).

(3) Pelaksanaan SMKI sebagaimana dimaksud dalam Pasal 61 di Disdukcapil Kabupaten/Kota dan di UPT Disdukcapil Kabupaten/Kota dilaksanakan sesuai dengan Keputusan Kepala Daerah sebagaimana dimaksud dalam Pasal 63 ayat (7).

(4) Pelaksanaan SMKI sebagaimana dimaksud dalam Pasal 61 di Perwakilan Republik Indonesia dilaksanakan oleh kepala Perwakilan Republik Indonesia.

Pasal 69

(1) Dirjen dalam melaksanakan tanggung jawab pelaksanaan SMKI sebagaimana dimaksud dalam Pasal 61 dapat melakukan kerja sama dengan:
   a. kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan digital;
   b. lembaga negara non-kementerian yang menyelenggarakan urusan siber, sandi dan Keamanan Informasi; dan
   c. 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 sebagai anggota STKI sebagaimana dimaksud dalam Pasal 63 ayat (3), dalam melaksanakan tugas dan tanggungjawab memastikan pelaksanaan kebijakan SMKI sebagaimana dimaksud dalam pasal 64 huruf a dengan memastikan tata kelola di Disdukcapil Provinsi dan Kabupaten/Kota.

Pasal 70

(1) Koordinator STKI sesuai dengan tugas dan tanggung jawabnya sebagaimana dimaksud dalam Pasal 64 guna melindungi kerahasiaan, keutuhan, dan ketersediaan Aset Informasi SAK dapat melakukan keputusan pemutusan secara sepihak.

(2) Keputusan pemutusan secara sepihak sebagaimana dimaksud pada ayat (1) disampaikan secara langsung atau dapat dilakukan melalui media elektronik untuk mendapat persetujuan dari Dirjen.

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

Pasal 71

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

(2) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) dilaksanakan terhadap SMKI sebagaimana dimaksud dalam Pasal 2 ayat (2).

(3) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan/atau sewaktu-waktu jika dibutuhkan.

Pasal 72

(1) Tim STKI di lingkungan Disdukcapil Provinsi, Disdukcapil Kabupaten/Kota, UPT Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia menyampaikan laporan hasil pemantauan dan evaluasi pelaksanaan SMKI kepada kepala Disdukcapil Provinsi, kepala Disdukcapil Kabupaten/Kota, dan Perwakilan Republik Indonesia setiap paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan/atau sewaktu-waktu jika dibutuhkan.
(2) Kepala Disdukcapil Provinsi, kepala 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 73

(1) Tim STKI di Ditjen menyampaikan laporan atas hasil pemantauan dan evaluasi pelaksanaan SMKI kepada Sekretaris Ditjen selaku Koordinator STKI paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan/atau sewaktu-waktu jika dibutuhkan.
(2) Sekretaris Ditjen menyampaikan laporan atas hasil pemantauan dan evaluasi pelaksanaan SMKI kepada Dirjen paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan/atau sewaktu-waktu jika dibutuhkan.
(3) Dirjen sebagaimana dimaksud pada ayat (2) menyampaikan laporan hasil pemantauan dan evaluasi pelaksanaan SMKI kepada Menteri paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan/atau sewaktu-waktu jika dibutuhkan.

BAB V
SANKSI ADMINISTRATIF

Pasal 74

Tim STKI, Pegawai pada satuan pelaksana SAK, atau Pihak Lain yang melanggar ketentuan Pasal 56 dikenai sanksi administratif berupa:
a. teguran lisan;
b. teguran tertulis; dan/atau
c. diberhentikan dari keanggotaan tim STKI dan/atau satuan pelaksana SAK.

BAB VI
PENDANAAN

Pasal 75

Pendanaan penyelenggaraan SMKI bersumber dari:
a. anggaran pendapatan dan belanja negara;
b. anggaran pendapatan dan belanja daerah; atau
c. sumber lainnya yang sah dan tidak mengikat.

BAB VII
KETENTUAN PENUTUP

Pasal 76

Pada saat Peraturan Menteri ini mulai berlaku, Peraturan Menteri Dalam Negeri Nomor 57 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Administrasi Kependudukan (Berita Negara Republik Indonesia Tahun 2021 Nomor 1272), dicabut dan dinyatakan tidak berlaku.

Pasal 77

Pada saat 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 26 Februari 2026

MENTERI DALAM NEGERI
REPUBLIK INDONESIA,

ttd.

MUHAMMAD TITO KARNAVIAN

Diundangkan di Jakarta
pada tanggal 10 Maret 2026

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM REPUBLIK INDONESIA,

ttd.

DHAHANA PUTRA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2026 NOMOR 167