PEMERINTAH KOTA YOGYAKARTA
DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL
Jl. Kenari No. 56 Yogyakarta Kode Pos: 55165 Telp. (0274) 563925, 557062, 587490, 515865, 562682
EMAIL: dukcapil@jogjakota.go.id
HOTLINE SMS: 08122780001 HOTLINE EMAIL: upik@jogjakota.go.id
WEBSITE: www.jogjakota.go.id

SURAT KEPUTUSAN KEPALA DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL KOTA YOGYAKARTA
NOMOR: 111/DKPS/2024
TENTANG
PENETAPAN STANDAR OPERASIONAL PROSEDUR KEAMANAN DATA DAN INFORMASI ADMINISTRASI KEPENDUDUKAN

PADA DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL KOTA YOGYAKARTA

Menimbang:

a. bahwa dalam rangka pelaksanaan sistem keamanan data dan informasi administrasi kependudukan di Dinas Kependudukan dan Pencatatan Sipil Kota Yogyakarta, maka perlu menetapkan Standar Operasional Prosedur;

b. bahwa untuk melaksanakan maksud tersebut di atas, maka perlu menetapkan Standar Operasional Prosedur yang ditetapkan dengan Keputusan Kepala Dinas Kependudukan dan Pencatatan Sipil Kota Yogyakarta;

Mengingat:

1. Undang-undang Nomor 16 Tahun 1950 tentang Pembentukan Daerah-daerah Kota Besar dalam Lingkungan Propinsi Jawa Timur, Jawa Tengah, Jawa Barat dan dalam Daerah Istimewa Yogyakarta;
2. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Tahun 2006 Nomor 124 Tambahan Lembaran Negara 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 Tahun 2013 Nomor 232 Tambahan Lembaran Negara Nomor 5475);
3. Undang-undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah, sebagaimana telah diubah dengan Undang-undang Nomor 2 Tahun 2015 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 tahun 2014 tentang Perubahan atas Undang- Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah;
4. 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
5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
6. Peraturan Menteri Pendayagunaan Aparatur Negera dan Reformasi Birokrasi Nomor 35 Tahun 2012 tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan (Berita Negara Republik Indonesia Tahun 2012 Nomor 649).

7. Peraturan Menteri Dalam Negeri No. 7 Tahun 2019 tentang Pelayanan Administrasi Kependudukan Secara Daring (Berita Negara Republik Indonesia Tahun 2019 Nomor
8. Peraturan Menteri Dalam Negeri Nomor 95 Tahun 2019 tentang Sistem Informasi Administrasi Kependudukan (Berita Negara Republik Indonesia Tahun 2019 Nomor 1478).
9. Peraturan Menteri Dalam Negeri Nomor 57 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Administrasi Kependudukan
10. Peraturan Walikota Yogyakarta Nomor 113 Tahun 2019 Tentang Sistem Manajemen Keamanan Informas
11. Peraturan Walikota Yogyakarta Nomor 102 tahun 2021 tentang Kedudukan, Susunan organisasi, Tugas , Fungsi, dan Tata Kerja Dinas Kependudukan dan Pencatatan Sipil

M E M U T U S K A N

Menetapkan : KEPUTUSAN KEPALA DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL KOTA YOGYAKARTA TENTANG PENETAPAN STANDAR OPERASIONAL PROSEDUR KEAMANAN DATA DAN INFORMASI ADMINISTRASI KEPENDUDUKAN PADA DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL KOTA YOGYAKARTA

KESATU : Menetapkan Standar Operasional Prosedur (SOP) pada Dinas Kependudukan dan Pencatatan Sipil Kota Yogyakarta yang terdiri dari :
1. SOP Pengelolaan Hak Akses
2. SOP Pengelolaan Gangguan dan Manajemen Insiden
3. SOP Pengamanan Informasi untuk Pegawai dan Pihak Ketiga

KEDUA : Standar Operasional Prosedur (SOP) sebagaimana dimaksud Diktum Kesatu terlampir dalam Keputusan ini merupakan pedoman dalam melaksanakan mekanisme penyelenggaraan administrasi pemerintahan pada Dinas Kependudukan dan Pencatatan Sipil Kota Yogyakarta

KETIGA : Keputusan ini berlaku sejak tanggal ditetapkan.

Ditetapkan di Yogyakarta
pada tanggal : 1 Agustus 2024
Kepala

PEMERINTAH KOTA YOGYAKARTA
DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL

Dra. SEPTI SRI REJEKI
NIP. 196809231995032007

Lampiran
SK No. : 111/DKPS/2024

DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL

KOTA YOGYAKARTA

STANDAR OPERASIONAL PROSEDUR

PENGELOLAAN HAK AKSES *(ACCESS CONTROL)*

STANDAR OPERASIONAL PROSEDUR
PENGELOLAAN HAK AKSES *(ACCESS CONTROL)*

A. PENDAHULUAN

Proses ini bertujuan untuk mengendalikan akses kepada seluruh pegawai DITJEN DUKCAPIL dan pihak ketiga yang bekerja di lingkungan DITJEN DUKCAPIL untuk pengamanan informasi DITJEN DUKCAPIL. Pengendalian hak akses yang diatur meliputi:

- Identifikasi pengguna *(user)*
- Pemberian Hak Akses *(user)*

B. STANDAR

1. Pengelolaan Akses

1.1. Pendaftaran dan Pencabutan Akses Pengguna

a. Pemberian akses kontrol atas sistem di lingkungan DITJEN DUKCAPIL menjadi wewenang Koordinator STKI, sedangkan untuk akses kontrol atas informasi menjadi wewenang masing-masing direktorat pemilik informasi tersebut. Pemberian akses kontrol tersebut dilakukan dengan tata cara umum sebagai berikut:
   - Pihak-pihak yang membutuhkan akses terhadap suatu informasi dan sistem informasi mengajukan permohonan akses kontrol kepada pemilik akses kontrol.
   - Unit fungsi/direktorat terkait harus memastikan bahwa pihak-pihak pengguna yang membutuhkan akses terhadap informasi yang bersifat rahasia telah menandatangani perjanjian kerahasiaan sesuai dengan ketentuan yang ada.
   - Untuk informasi yang berbentuk non-elektronik, persetujuan diberikan oleh direktorat pemilik informasi untuk disampaikan kepada pengguna sebagai pemberitahuan.
   - Untuk informasi yang berbentuk elektronik dan/atau dari sistem di lingkungan DITJEN DUKCAPIL, persetujuan diberikan oleh Koordinator STKI.
   - Dokumentasi dari permintaan dan pemberian akses kontrol harus dibuat dan dipelihara sebagai bukti *(records)* untuk permintaan dan pemberian akses kontrol.

b. Seluruh direktorat hanya memberikan atau membuka akses apabila seluruh persyaratan sudah dipenuhi, serta berhak untuk membatasi akses kontrol dari setiap pengguna sesuai dengan kebutuhan yang telah ditentukan dan sesuai dengan perijinan yang diberikan oleh pemilik informasi.

c. Seluruh direktorat di DITJEN DUKCAPIL sebagai pemilik informasi dalam pemberian akses kontrol kepada pihak eksternal harus memperhatikan hal-hal sebagai berikut:
   - Pihak eksternal yang akan mengakses informasi yang berada di sistem harus mengajukan permohonan penggunaan VPN dan jaringan internet data yang terenkripsi ke DITJEN DUKCAPIL.
   - Jenis akses, yaitu akses fisik (masuk ke lingkungan DITJEN DUKCAPIL), akses logikal (masuk ke sistem DITJEN DUKCAPIL) dan sambungan jaringan antara DITJEN DUKCAPIL dengan pihak eksternal, baik akses *on-site, off-site*, *remote site* atau *direct connection.*
   - Klasifikasi keamanan informasi dengan mempertimbangkan nilai dan sensitivitas informasi serta tingkat risiko DITJEN DUKCAPIL.

- Aspek pengendalian yang diperlukan untuk melindungi informasi yang tidak boleh diakses oleh pihak eksternal.
- Perbedaan pemahaman dan pengendalian yang dilakukan pihak eksternal dalam hal penyimpanan, pemprosesan, komunikasi, pertukaran, dan perubahan informasi.
- Dampak tidak tersedianya akses kontrol bagi pihak eksternal saat dibutuhkan atau dampak kesalahan informasi yang diterima oleh pihak eksternal.

d. Jenis akses fisik dan logikal dikelola oleh masing-masing direktorat.

1.2. Pengelolaan *Privilege* (Akses Khusus)

a. Seluruh unit fungsi/direktorat bertanggung jawab menjaga catatan pengelolaan akses kontrol serta memastikan bahwa pihak-pihak yang memiliki akses kontrol khusus telah dikendalikan dengan memadai.
b. Beberapa ketentuan mengenai pengaturan *privilege:*
   - *Privilege* harus dialokasikan kepada pengguna berdasarkan kebutuhan.
   - Proses otorisasi dan catatan dari semua *privilege* yang dialokasikan seharusnya tetap terjaga.
   - Perlu adanya penyesuaian aplikasi yang diakses secara rutin setiap 3 (tiga) bulan sekali untuk mengurangi pemberian *privilege* kepada pegawai.

1.3. Prosedur Pemberian/Penggantian Hak Akses Personil Administrator

a. Masing-masing direktorat melakukan seleksi kebutuhan akan akses Personil Administrator.
b. Masing-masing direktorat melakukan verifikasi kebutuhan akan akses Personil Administrator.
c. Masing-masing direktorat memberikan surat keputusan bahwa pegawai yang ditunjuk bertindak sebagai Personil Administrator.
d. Apabila ada pengubahan atau penggantian Personil Administrator, maka kembali ke proses awal.

1.4. Evaluasi *User Access*

Seluruh direktorat melakukan *review* secara periodik terhadap akses kontrol informasi, termasuk pemeriksaan tingkatan akses yang diberikan dan penghapusan atau pemblokiran terhadap kelebihan penerbitan akses kontrol, dan harus segera merubah atau memblokir akses kontrol apabila pegawai pindah jabatan ataupun pindah penugasan/keluar dari DITJEN DUKCAPIL. Beberapa ketentuan *review* adalah sebagai berikut:

a. Akses kontrol pegawai harus ditinjau secara berkala, yaitu setiap jangka waktu 1 (satu) tahun sekali, dan setiap ada setelah perubahan apapun, seperti promosi, penurunan pangkat, atau pemutusan hubungan kerja.
b. Bagi pegawai DITJEN DUKCAPIL yang sudah tidak bertugas maka akses kontrolnya harus dicabut segera setelah hari terakhir bekerjanya.
c. Informasi mengenai mutasi pegawai atau berakhirnya masa tugas mengacu kepada dokumen Surat Keputusan (SK) bagi ASN atau Surat Pengunduran Diri bagi Tenaga Ahli atau *Supporting Staff (SS).*
d. Pegawai pengguna akses kontrol harus ditinjau dan dialokasikan kembali ketika berpindah/mutasi dari satu unit kerja ke unit kerja lain.
e. Alokasi *privilege access rights* harus diperiksa secara berkala untuk memastikan

bahwa *privilege access rights* tersebut diperoleh secara sah.

f. Perubahan *privilege access rights* harus dicatat untuk diperiksa secara periodik.

1.5. Akses Ruangan *Server*

a. Pimpinan direktorat terkait memastikan pengunjung melakukan pengisian formulir secara lengkap serta menyerahkan tanda pengenal diri yang sah, misalnya KTP.
b. Penanggung Jawab Area memastikan selama berada di dalam ruangan *server* pengunjung harus senantiasa ditemani dan diawasi agar pengunjung dapat dipastikan tidak melakukan hal-hal diluar ijin kunjungannya atau hal-hal yang dapat berisiko terhadap ruangan *server* dan isinya, serta tanda pengenal senantiasa dikenakan.
c. Seusai kunjungan Penanggung Jawab Area memastikan formulir dilengkapi dengan daftar dan nomor seri perangkat yang dibawa (jika ada) dan jam keluar, serta pengembalian tanda pengenal ditukar dengan tanda pengenal diri yang diserahkan pada awal kunjungan.

1.6. *Remote Access*

a. Pemberian *remote access* sangat terbatas dan hanya diperbolehkan untuk pihak yang telah diberikan otorisasi oleh Koordinator STKI dan/atau direktorat terkait di DITJEN DUKCAPIL.
b. Keamanan dalam mengakses sistem/aplikasi/jaringan di DITJEN DUKCAPIL setidaknya memenuhi persyaratan sebagai berikut:
   - Menggunakan autentikasi yang telah ditetapkan.
   - Melakukan *log-off* pada perangkat yang digunakan apabila akan meninggalkan meja/area kerja.
   - Memastikan kegiatan mengakses sistem/aplikasi/jaringan dilakukan oleh pihak/orang yang memiliki otorisasi.
   - Menggunakan lisensi yang sesuai pada perangkat yang digunakan untuk mengakses sistem/aplikasi/jaringan.
   - Lingkup pekerjaan, jam kerja, klasifikasi informasi serta aplikasi sistem dan layanan yang diperbolehkan untuk diakses harus dilaporkan kepada Koordinator STKI.
   - Pemutusan wewenang dan hak akses serta kembalinya peralatan yang digunakan ketika izin berakhir.
c. Koordinator STKI berkewajiban untuk memastikan autentikasi yang telah disediakan dan transfer data yang terjadi telah terenkripsi.
d. Aturan mengenai pemberian *remote access* kepada pihak ketiga adalah:
   - Pimpinan direktorat terkait menerima surat permintaan *remote access* dari pihak ketiga.
   - Pimpinan direktorat terkait menentukan apakah ijin akan diberikan atau tidak. Jika ijin diberikan, tenaga teknis membuat akun untuk *remote access* dan memberikan kepada pihak ketiga serta mengisi form pemberian *remote access.*
   - Setelah selesai, pihak ketiga memberitahukan kepada tenaga teknis agar akun *remote access* ditutup dan memutahirkan form pemberian *remote access.*

1.7. *Teleworking*

a. Pegawai DITJEN DUKCAPIL yang bekerja secara *remote/teleworking* harus mengajukan Form Penggunaan Aset Pribadi (FR.04-SOP-06/DITJEN-DUKCAPIL) untuk didata disertai alasannya.
b. Adapun perangkat pribadi yang digunakan yang digunakan adalah:

- *Smart phone/handphone.*
- *Tablet*
- *PC/laptop/notebook.*
- *Removable media (harddisk external, flash disk).* Perangkat perangkat tersebut diberikan proteksi yang memadai sesuai dengan kebijakan keamanan informasi.

c. Buatkan pembagian klasifikasi penggunaan perangkat (keperluan pegawai dan DITJEN DUKCAPIL).
d. Jika terjadi kehilangan atas perangkat pribadi tersebut, pegawai DITJEN DUKCAPIL yang melakukan pekerjaan secara *remote/teleworking* harus segera melaporkan kepada *Administrator* atau Koordinator STKI untuk menghapus data DITJEN DUKCAPIL yang ada di perangkat mereka.

2. *Network Access*
   a. Akses ke jaringan DITJEN DUKCAPIL harus mendapat persetujuan dari Direktur terkait dan Koordinator STKI.
   b. Akses secara *remote* harus dilengkapi dengan teknik pengamanan yang memadai, misalnya kriptografi, SSH, *hardware token*, *challenge/response protocol* dan *Virtual Private Network (VPN).*
   c. Identifikasi Perangkat yang Terhubung ke Jaringan
      - Identifikasi perangkat dapat digunakan untuk otentikasi akses dari lokasi atau perangkat tertentu, yang sedapat mungkin dilakukan secara otomatis. Contohnya, PC pegawai yang berhak mengakses sistem aplikasi tertentu harus memiliki identifikasi tertentu (misalnya: *unique hostname, MAC address)* yang terdaftar pada sistem aplikasi.
      - Identifikasi perangkat dapat dikombinasikan dengan identitas pegawai untuk memastikan keabsahan akses ke jaringan.
      - Ada pembagian wilayah akses untuk setiap perangkat yang akan terhubung ke jaringan. Perangkat terdaftar hanya terhubung ke jaringan melalui titik akses tertentu.
   d. Pegamanan terhadap Akses *Port Diagnostic* dan Konfigurasi
      - Akses terhadap *port diagnostic* dan konfigurasi hanya dapat diberikan kepada pegawai yang berwenang.
      - Akses secara fisik terhadap *port diagnostic* dan konfigurasi perlu dilindungi, misalnya dengan penggunaan kunci pada rak.
      - *Port* dan fasilitas komunikasi lain pada *PC, notebook, server atau* perangkat jaringan yang tidak dibutuhkan untuk keperluan aplikasi, harus dinonaktifkan atau ditutup.
   e. Pemisahan Akses Jaringan
      - Untuk membatasi akses terhadap aset informasi melalui jaringan, maka dapat dilakukan hal-hal sebagai berikut:
        - Jaringan komunikasi data dibagi menjadi segmen-segmen/domain logikal yang dilindungi dengan pengamanan teknologi informasi yang memadai misalnya dengan menggunakan *firewall* dan/atau VPN.
        - Jaringan komunikasi data dapat dipisahkan secara logikal dengan melakukan setting pada perangkat jaringan seperti *IP Switching*, VLAN atau dipisahkan secara fisikal.
      - Kriteria pemisahan jaringan harus didasarkan pada kebutuhan akses, ketentuan pengendalian akses, kinerja dan biaya yang dibutuhkan, nilai dan klasifikasi informasi.
   f. Pengendalian Layanan Jaringan

- Akses kontrol jaringan oleh pegawai harus dikelola dan dilakukan pembaruan secara berkala sesuai ketentuan Kebijakan Keamanan Informasi (PL-01/DITJEN-DUKCAPIL) untuk pengendalian akses.
- Akses oleh pegawai dapat dibatasi dengan menyaring trafik pada *network gateway* atau membatasi akses pada waktu atau tanggal tertentu Oam kerja).
- Perjanjian keamanan informasi dengan pihak ketiga melingkupi penggunaan teknologi keamanan (enkripsi, autentikasi, *network control)*, penetapan parameter *(port* yang dibuka, penggunaan protokol).
- Secara berkala akan dilakukan *review* terhadap *SLA network service provider.*

Pengendalian *Routing* Jaringan

- Implementasi pengendalian *routing* jaringan berdasarkan pada ketentuan pengendalian akses yang berlaku.
- Pengendalian *routing* berdasarkan pada alamat sumber *(source)* dan tujuan *(destination)* yang telah ditentukan, misalnya dengan penggunaan *Access Control Matrix* (ACM).
- Persyaratan kebutuhan untuk kendali *routing* jaringan mengacu pada kebijakan kendali akses.

3. *Logon* yang Aman
   a. *Logon* ke Sistem Operasi secara aman harus:
      - Menghindari penggunaan fasilitas bantuan selama proses *logon* yang dapat dimanfaatkan oleh pegawai yang tidak terotorisasi, misalnya tidak menampilkan *User ID* yang *logon* sebelumnya atau tidak ada fasilitas *automatic password.*
      - Membatasi jumlah *logon* yang gagal dilakukan maksimal tiga kali yang dilanjutkan dengan pemblokiran dan/atau penundaan *logon (freeze)* selama jangka waktu tertentu.
      - Menyembunyikan/tidak menampilkan karakter *password* saat diketik atau dapat ditampilkan berupa simbol.
   b. *Logon* aman sedapat mungkin memenuhi beberapa hal sebagai berikut:
      - Menampilkan peringatan bahwa komputer hanya dapat diakses oleh pegawai yang terotorisasi.
      - Tidak menampilkan identitas atau fungsi-fungsi pada sistem operasi atau sistem aplikasi sebelum *logon* berhasil dilakukan.
      - Memberikan informasi validasi *logon* hanya setelah seluruh proses *logon* dilakukan serta tidak menyebutkan rincian penyebab kegagalan *logon.*
      - Membatasi waktu maksimum dan minimum yang dibutuhkan untuk melakukan proses *logon.* Jika terlampaui, maka sistem menghentikan proses *logon.*

4. Penggunaan Sistem Utilitas
   a. Setiap pegawai pengguna informasi diwajibkan untuk menggunakan pedoman identifikasi, otentifikasi, dan otorisasi dalam menggunakan sistem utilitas operasi.
   b. Penggunaan sistem utilitas operasi dibatasi dan harus terdapat catatan/rekaman/log dari seluruh penggunaannya dan diberikan masa retensi.
   c. Pemisahan sistem utilitas dari perangkat lunak aplikasi.
   d. Pembatasan penggunaan sistem utilitas untuk pengguna tertentu dan jangka waktu tertentu.
   e. Pencabutan dan penghentian semua utilitas dan perangkat lunak sistem yang tidak perlu.
   f. Mendefinisikan dan mendokumentasikan level otoritas penggunaan sistem utilitas.

5. *Session Time-Out*
    a. Seluruh piranti lunak yang sudah tidak digunakan harus dihapus/dibuang/dinonaktifkan/di-d/sob/e.
    b. *Session time-out* diaktifkan.
    c. Rentang *session time-out* disesuaikan dengan klasifikasi informasi yang diakses atau aplikasi yang digunakan, risiko pengamanan fisik dan risiko yang berhubungan dengan penggunaan peralatan teknologi informasi.
    d. Pengaktifan *session time-out* dapat menggunakan fasilitas sistem operasi atau aplikasi.

6. Pembatasan Waktu Koneksi
    a. Terdapat batas minimum dan maksimum waktu penggunaan akses atas sistem informasi selain seluruh Tenaga Teknis.
    b. Tidak dilakukan pembatasan waktu terhadap koneksi ke jaringan.

7. Pembatasan Akses Informasi

    a. Pembatasan akses berdasarkan pada spesifikasi kebutuhan masing-masing sistem aplikasi.
    b. Kebijakan pengendalian akses di dalam sistem aplikasi sesuai dengan ketentuan pengendalian akses yang berlaku.
    c. Pembatasan akses kontrol mencakup sekurang-kurangnya:
        - Penyediaan fasilitas untuk membatasi akses terhadap fungsi-fungsi yang ada pada sistem aplikasi.
        - Pengendalian akses kontrol pengguna (CRUD = *create, read, update, delete).*
        - Pengendalian akses kontrol dari aplikasi yang terhubung.
        - Pengendalian keluaran sistem aplikasi yang menangani informasi rahasia agar hanya berisi informasi yang dibutuhkan dan hanya dikirim ke pegawai yang terotorisasi dan/atau terminal/PC di lokasi yang terotorisasi.

8. Penempatan Sistem Aplikasi Sensitif/Kritis

    Beberapa hal berikut seharusnya diperhatikan dalam penempatan sistem aplikasi sensitif/kritis:
    a. Sistem aplikasi sensitif/kritis secara eksplisit diidentifikasi dan didokumentasi oleh Direktorat Pemilik Sistem Aplikasi.
    b. Sistem aplikasi sensitif/kritis ditempatkan secara fisikal dan logikal pada wilayah tertutup.
    c. Apabila sistem aplikasi sensitif/kritis tidak dimungkinkan untuk ditempatkan pada wilayah tertutup, maka diidentifikasi risiko yang dapat ditimbulkan dan mitigasinya serta disetujui oleh Direktorat Pemilik Sistem Aplikasi sensitif/kritis dan Koordinator STKI.
    d. Beberapa aplikasi sensitif/kritis yang berpotensi melahirkan kerugian seharusnya hanya membagikan sumber daya dengan sistem aplikasi yang terpercaya.

C. DEFINISI

1. Kebijakan adalah ketetapan yang disahkan oleh Dirjen Dukcapil yang merupakan salah satu bukti komitmen untuk memenuhi persyaratan, peraturan dan perundang-undangan serta terus menerus meningkatkan keefektifan SMKI, menyediakan kerangka kerja untuk menetapkan tujuan dan meninjau sasaran, dikomunikasikan dan dipahami dalam lingkup DITJEN DUKCAPIL, dilakukan peninjauan secara terjadwal sehingga dapat dilakukan penyesuaian terus menerus.

2. *Administrator* adalah pegawai DITJEN DUKCAPIL yang ditunjuk secara langsung oleh DITJEN DUKCAPIL sebagai *Administrator* yang memiliki peran untuk dapat mengatur hak akses di lingkup DITJEN DUKCAPIL.
3. Hak Akses adalah izin atau hak istimewa yang diberikan kepada pegawai, program atau *Workstation* untuk membuat, mengubah, menghapus atau melihat data dan *file* dalam sebuah sistem, sebagaimana ditetapkan oleh aturan yang dibuat oleh pemilik data dan sesuai kebijakan keamanan informasi. Biasanya hak akses dibagi menjadi beberapa level *(user level)* seperti *Administrator, user, author, editor,* dan lain-lain.
4. Kontrol Akses *(Access Control)* adalah sistem yang dapat atau untuk membatasi pegawai untuk mengakses suatu sistem dengan menempatkan sistem perangkat kontrol tertentu.
5. *Remote access* adalah ijin untuk mengakses sistem/aplikasi/jaringan secara *remote* (diluar area kerja DITJEN DUKCAPIL).
6. *Mobile Devices* adalah perangkat yang digunakan untuk melaksanakan pekerjaan yang bersifat dinamis/mobile yang dapat digunakan di luar area kerja DITJEN DUKCAPIL atau di luar area yang disiapkan oleh DITJEN DUKCAPIL untuk melaksanakan pekerjaan khususnya perangkat yang digunakan untuk mengakses ke dalam sistem/aplikasi/jaringan atau menyimpan data perusahaan.
7. *Teleworking* adalah melaksanakan pekerjaan di luar area kantor dan menggunakan jaringaninternet pribadi untuk mengakses sistem dan sistem/aplikasi/jaringan DITJEN DUKCAPIL.
8. *BYOD/Bring Your Own Device adalah* sebuah kebijakan di mana organisasi memperbolehkan pegawainya untuk membawa gadget mereka untuk digunakan dalam bekerja, seperti laptop, ponsel pintar *(smart phone),* atau *computer tablet.* BYOD ini bisa juga disebut dengan BYOT *(Bring Your Own Technology),* BYOP *(Bring Your Own Phone)* atau BYOPC *(Bring Your Own PC).*
9. *Password* (Kata Sandi) adalah kode rahasia/kata sandi yang merupakan kunci untuk bisa mengakses atau membuka suatu sistem yang dikunci baik itu sistem komputer yang menggunakan sistem operasi Windows atau bukan, yang berupa karakter tulisan, suara, atau ciri-ciri khusus yang harus diingat. *Password* merupakan rahasia, jika ada orang lain yang mengetahui *Password* tersebut, bisa jadi orang yang tidak berhak tersebut akan menghapus atau mencuri informasi yang ada. Jadi sebaiknya dalam selang waktu tertentu *Password* sebaiknya diganti dan agar kerahasiaannya terjamin.
10. Informasi adalah satu atau lebih entitas data yang saling berhubungan dan mempunyai makna tertentu.
11. Kerahasiaan Informasi adalah perlindungan informasi agar tidak dapat diakses (dilihat/diketahui) oleh pihak yang tidak berhak.
12. Dokumen Informasi adalah Informasi rahasia yang berbentuk *softcopy* dan *hardcopy.*

D. REFERENSI

1. ISO/IEC 27001:2013 - Annex A.6.2. Mobile Devices & *Teleworking.*
2. ISO/IEC 27001:2013 - Annex A 9. *Access Control.*
3. ISO/IEC 27001:2013 - Annex A 9.1. *Business Requirements of Access Control.*
4. ISO/IEC 27001:2013 - Annex A 9.1.1. *Access Control Policy.*
5. ISO/IEC 27001:2013 - Annex A 9.1.2. *Access to Network and Network Services.*
6. ISO/IEC 27001:2013 - Annex A 9.2. *UserAcess Management.*
7. ISO/IEC 27001:2013 - Annex A 9.2.1. *User Registration and De - Registration.*
8. ISO/IEC 27001:2013 - Annex A 9.2.3. *Management of Privileged Access Rights.*
9. ISO/IEC 27001:2013 - Annex A 9.2.4. *Management of Secret Authentication Information of*

User.
10. ISO/IEC 27001:2013 - Annex A 9.2.5. *Review of User Access Rights.*
11. ISO/IEC 27001:2013 - Annex A 9.2.6. *Removal or Adjustment of Access Reight.*
12. ISO/IEC 27001:2013 - Annex A 9.3. *User Responsibility.*
13. ISO/IEC 27001:2013 - Annex A.9.3.1. *Use of Secret Authentication Information.*
14. ISO/IEC 27001:2013 - Annex A 9.4. *System and Application Access Control.*

Nomor Standar Operasional Prosedur	SOP-1/SMKI-PIAK
Tanggal Pembuatan	10 Mei 2022
Tanggal Revisi	-
Tanggal Pengesahan	02 Juni 2022
Disahkan Oleh	Kepala Dinas Kependudukan dan Pencatatan Sipil Kota Yogyakarta Dra. Septi Sri Rejeki NIP. 196809231995032007
Nama Standar Operasional Prosedur	**Pengelolaan Akses (Access Control)**

TUJUAN

Prosedur ini dibuat dengan tujuan untuk mengatur proses manajemen akses dengan tata cara dan penggunaan kewenangan akses yang diberikan sehingga proses manajemen akses di lingkungan Dinas Kependudukan dan Pencatatan Sipil dapat berjalan dengan baik dan teratur.

RUANG LINGKUP

1. Pengendalian akses pengguna, jaringan, sistem operasi, informasi dan aplikasi.
2. Pemberian *remote* akses kepada pihak-pihak yang telah diberikan otorisasi oleh DITJEN DUKCAPIL.

DASAR HUKUM

1. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Tahun 2006 Nomor 124 Tambahan Lembaran Negara 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 Tahun 2013 Nomor 232 Tambahan Lembaran Negara Nomor 5475).
2. 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).
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182).
4. Peraturan Menteri Dalam Negeri Nomor 4 Tahun 2011 tentang Standar Operasional Prosedur di Lingkungan Kemendagri (Berita Negara Republik Indonesia Tahun 2011 Nomor 24

KUALIFIKASI PELAKSANA

1. Pendidikan minimal D-lll atau sederajat.
2. Memahami konsep dasar SMKI.
3. Memahami konsep teknis sistem/aplikasi/perangkat sesuai dengan ijin aksesnya.
4. Mengenal perimeter keamanan fisik

5. Peraturan Menteri Pendayagunaan Aparatur Negera dan Reformasi Birokrasi Nomor 35 Tahun 2012 tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan (Berita Negara Republik Indonesia Tahun 2012 Nomor 649).
6. Peraturan Menteri Dalam Negeri Nomor 43 Tahun 2015 tentang Organisasi dan Tatakerja Kemendagri (Berita Negara Republik Indonesia Tahun 2015 Nomor 564).
7. Peraturan Menteri Dalam Negeri No. 7 Tahun 2019 tentang Pelayanan Administrasi Kependudukan Secara Daring (Berita Negara Republik Indonesia Tahun 2019 Nomor 152).
8. Peraturan Menteri Dalam Negeri Nomor 95 Tahun 2019 tentang Sistem Informasi Administrasi Kependudukan (Berita Negara Republik Indonesia Tahun 2019 Nomor 1478). dan
9. Peraturan Menteri Dalam Negeri Nomor 57 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Administrasi Kependudukan. _____

KETERKAITAN

1. MN-01/DITJEN-DUKCAPIL - Pedoman Sistem Manajemen Keamanan Informasi.
2. MN-02/DITJEN-DUKCAPIL - Pedoman Kebijakan Keamanan Informasi.
3. SOP Manajemen Aset.

PERALATAN PERLENGKAPAN

1. Komputer kerja.
2. Jaringan komputer.
3. Alat komunikasi.
4. ISO/IEC 27001:2013.

PERINGATAN

1. Dilarang membuat/mencabut hak akses tanpa perintah dari Koordinator STKI dan DIRJEN DUKCAPIL.
2. Dalam hal perintah pembuatan/pencabutan hak akses secara tidak tertulis, wajib menyusul surat tertulisnya yang telah disetujui oleh DIRJEN DUKCAPIL.
3. Setiap perubahan kewenangan/tugas/fungsi pegawai harus dilaporkan untuk dikaji ulang hak aksesnya.
4. Hak akses pegawai harus dikaji ulang secara berkala, minimal dalam 1 (satu) tahun sekali, untuk memastikan validitas kewenangannya.

PENCATATAN DAN PENDATAAN

1. Form Permohonan Akses.
2. Form Review Hak Akses.
3. Log Serah Terima Account Administrator.
4. Form Pencatatan Akses Server.
5. Form Pencatatan Remote Akses.

DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL

KOTA YOGYAKARTA

STANDAR OPERASIONAL PROSEDUR PENGELOLAAN GANGGUAN DAN MANAJEMEN INSIDEN

STANDAR OPERASIONAL PROSEDUR
PENGELOLAAN GANGGUAN DAN MANAJEMEN INSIDEN

A. PENDAHULUAN

Penanganan jika terjadi gangguan (insidenj/permasalahan sangat penting. Pengklasifikasian (kategorisasi dan penentuan skala prioritas) dan dukungan awal bagi pegawai pada saat terjadi insiden, jika tidak ditangani secara serius dapat menimbulkan insiden seperti di bawah ini:

1. Insiden Tl

Pencurian / kehilangan aset	Pencurian atau hilangnya informasi atau aset / perangkat teknologi (termasuk *portable media* dan *fixed media),* yang mungkin telah digunakan, atau telah digunakan, untuk mengolah atau menyimpan informasi Dinas Kependudukan dan Pencatatan Sipil
Akses tidak sah pada sistem/informasi	Seorang penyerang menjalankan suatu *"exploit tool"* untuk memperoleh akses pada file password dari server. Seorang penyaru mendapatkan akses setingkat *administrator* yang tidak sah pada suatu sistem dan data sensitif yang ada didalamnya, kemudian mengancam bahwa detail dari data yang tersimpan pada sistem tersebut akan disebarluaskan melalui media jika Dinas Kependudukan dan Pencatatan Sipil tidak membayar sejumlah uang yang ditentukan.
Infeksi *malware*	Suatu cacing *(worm)* menggunakan *"open file share"* untuk menginfeksi ratusan *workstation* di lingkungan Dinas Kependudukan dan Pencatatan Sipil Pegawai Dinas Kependudukan dan Pencatatan Sipil menerima peringatan *(warning)* dari pemasok anti virus bahwa suatu cacing baru sedang menyebar dengan cepat melalui surat elektronik diseluruh Internet. *Worm* tersebut memanfaatkan suatu kelemahan yang ada pada suatu host di DITJEN DUKCAPIL. Berdasar insiden antivirus sebelumnya, pegawai DITJEN DUKCAPIL memperkirakan bahwa *worm* baru tersebut akan menginfeksi beberapa *host-nya* dalam beberapa jam kedepan.
Pegacauan, penyusupan,atau gangguan terhadap jaringan	Pengacauan yang secara spesifik ditujukan pada infrastruktur internal DITJEN DUKCAPIL. Ini mencakup, tapi tidak terbatas pada: • *Denial-of-Service (DoS)/distributed Denial-of-Service* (DDoS) • *Website defacement • Brute force attempts* Pengacauan, yang setelah analisis, tidak dapat dikaitkan dengan apa yang dianggap konsisten dengan *internet noise.* Sebagai contoh, percobaan pengacauan yang secara konsisten mengancam infrastruktur jaringan internal, pengguna atau layanan-layanan yang diberikan untuk penggunaan eksternal seperti aplikasi web.

Denial-of-service (DoS)	*Denial of service* (DoS) adalah suatu tindakan yang menghalangi penggunaan sah atas jaringan, sistem, atau aplikasi dengan cara menggunakan habis sumber daya seperti *central processing unit* (CPU), *memory, bandwith,* dan *disk space.* Contoh serangan DoS: • Menggunakan seluruh *bandwith* yang tersedia dengan cara membangkitkan volume trafik yang sangat besar.
Penyalahgunaan hak	Perubahan-perubahan *setting* penggunaan hak khusus *(privelege)* pada perangkat mandiri *(stand alone)* atau dalam jaringan, termasuk profil jaringan, pengguna local atau file konfigurasi perangkat yang belum mendapat persetujuan melalui proses manajemen perubahan Dinas Kependudukan dan Pencatatan Sipil
Perubahan tidak sah pada informasi, aplikasi, sistem atau perangkat keras.	Perubahan apapun yang tidak sah pada sistem file Dinas Kependudukan dan Pencatatan Sipil, termasuk media, melalui penyisipan, modifikasi, atau penghapusan, misalnya perubahan-perubahan *standard operating environment,* penambahan *executable* atau perubahan dari suatu konfigurasi *executable.* Setiap pemasangan perangkat pengolahan, komunikasi atau *storage,* yang tidak sah, ke dalam jaringan Tl. Ini mencakup, tapi tak terbatas pada:
Pelanggaran kebijakan keamanan informasi	Seorang pegawai memberikan salinan piranti lunak illegal kepada pegawai lain melalui layanan *peer-to-peer file sharing.* Seseorang mengancam orang lain melalui surat elektronik. Semua pelanggaran kebijakan kemananan informasi atau aspek terkait keamanan informasi dari *code of conduct.*
Perilaku atau kegagalan sistem (perangkat keras/lunak, komunikasi) yang mencurigakan	Kegiatan-kegiatan yang tidak diketahui yang memengaruhi/menurunkan kinerja jaringan dengan peningkatan penggunaan bandwith jaringan dan menurunkan *response time,* peningkatan permintaan jaringan yang mencurigakan atau peningkatan peringatan *Intrusion Detection System (\DS)/lntrusion Prevention System* (IPS) yang mengakibatkan *application crash.* Malafungsi dalam sirkuit elektronik, komponen-komponen elektromekanik dari sistem komputer/komunikasi, atau malfungsi/ketidakmampuan dari suatu program untuk melanjutkan pengolahan karena *logic* yang salah.
Gangguan kerahasiaan *password*	Penggunaan bersama, pencurian, kehilangan *password* atau token otentikasi lainnya.
Sabotase/kerusakan fisik	Tiap kerusakan atau pengrusakan informasi fisik atau perangkat elektronik.
Kejadian-kejadian lain	Kejadian-kejadian alami dan kejadian-kejadian lain yang mengakibatkan kerusakan informasi dan sistem. Hal ini mencakup tapi tak terbatas pada: • Kebakaran • Banjir • Panas berlebihan • Badai • Agen biologikal • Penyebaran racun • Pemadaman listrik • Kekacauan

2. Insiden Non-TI

Kerusakan perangkat (CCTV, *Access Door, Electrical Failure,* dan lain-lain)	Kerusakan pada perangkat yang berpotensi terjadinya insiden keamanan informasi.
Pelanggaran dari pegawai	Kelalaian, abai terhadap kebijakan SMKI *(clear desk* dan *clear screen policy, password policy,* dan lain-lain) yang berpotensi terjadinya insiden kemanan informasi.
Potensi penyusup	Adanya pihak eksternal yang tidak dikenal yang berada dekat fasilitas, kantor atau adanya aktivitas mencurigakan dari pihak tidak dikenal.
Kejadian-kejadian lain	Penyuapan, gratifikasi, korupsi, dan lain-lain.

B. STANDAR

1. <u>Tahapan Manajemen Insiden</u>

Identifikasi insiden *(incident identification)*	Proses manajemen insiden *(incident management)* dimulai dengan identifikasi. Identifikasi yang paling umum dilakukan adalah melalui layanan service desk dan laporan dari staf teknisi.
Pencatatan insiden *(incident logging)*	Langkah ini wajib dilakukan untuk setiap jenis insiden baik yang berskala besar maupun kecil.
Pengkategorisasian insiden *(incident categorization)*	Dalam membuat kategori insiden dibutuhkan sebuah proses khusus antara pegawai pengelola Tl Dinas Kependudukan dan Pencatatan Sipil dan DITJEN DUKCAPIL.
Prioritas insiden *(incident priorization)*	Prioritas penanganan insiden dapat dilakukan berdasarkan besarnya implikasi insiden terhadap kegiatan layanan Dinas Kependudukan dan Pencatatan Sipil, ataupun berdasarkan lamanya penanganan insiden.
Diagnosa awal *(initial diagnosis)*	Diagnosa awal terhadap insiden wajib dilakukan oleh setiap pihak yang pertama kali berhubungan dengan insiden baik itu *service desk,* staf teknis, maupun perangkat otomatis.
Eskalasi insiden *(incident escalation)*	Eskalasi insiden adalah tindakan menaikkan level penanganan insiden.
Investigasi *(investigation and diagnosis)*	Tindakan investigasi dilakukan untuk menemukan sumber masalah dari insiden.
Resolusi *(resolution and recovery)*	Langkah ini merupakan tindakan yang diambil untuk menyelesaikan suatu insiden.

2. Klasifikasi Gangguan / Insiden

Klasifikasi	Insiden / Gangguan	Pelaksana *				SLA
		a	b	c	d	
Service Request	*Move/add/change* akun					
	Gagal *login*					
	Lupa *username/password*					
	Tidak dapat memasukkan data					
	Akses *fisik/logical*					
Fault	Sistem *down*					
	Listrik padam					
	Jaringan *error*					
	Kerusakan perangkat utama					
	Kerusakan perangkat pendukung					
	Pencurian/kehilangan aset					
	Penyalahgunaan akses termasuk perubahan tidak sah pada informasi, aplikasi, sistem atau perangkat keras					
	Pelanggaran kebijakan Tl					
	Potensi penyusup					
	Gratifikasi / penyuapan					
Technical Incident	*Automatic warning*					
	Disk usage					
	Application error					
	Cyberattack (malware/akses tidak sah)					
	Lingkungan (kabel digigit tikus, dan lain-lain)					
	Sabotase/pegacauan/penyusupan/gangguan terhadap jaringan					
Help/Asisstant	Permintaan informasi					
	Bantuan penggunaan aplikasi					
	Bantuan peggunaan *hardware*					

Note *:
a : Helpdesk di masing-masing direktorat
b : Administrator sistem/jaringan di masing-masing direktorat
c : Tim Penanggulangan Gangguan/lnsiden
d : Koordinator STKI

Catatan*

Recovery Time Objective (RTO) adalah durasi waktu dimana sebuah layanan harus dipulihkan setelah terjadinya sebuah gangguan atau bencana untuk menghindari terjadinya dampak yang tidak dapat lagi ditanggung oleh perusahaan.

Recovery Point Objective (RPO) adalah waktu yang dibutuhkan untuk mengembalikan sistem ke kondisi normal.

C. DEFINISI

1. **Gangguan** adalah setiap peristiwa yang bukan merupakan bagian dari operasi standar layanan dan menyebabkan atau dapat menyebabkan pengurangan kualitas layanan.
2. **Permasalahan** adalah setiap peristiwa yang bukan merupakan bagian dari operasi standar layanan dan menyebabkan pengurangan kualitas layanan serta berdampak pada penyelenggaraan layanan yang akan datang.
3. **Permintaan Layanan** adalah salah satu bentuk layanan yang diberikan oleh DITJEN DUKCAPIL, dimana masyarakat dapat menyampaikan permintaan akan layanan yang dibutuhkan.

4. **Insiden** adalah sebuah atau serangkaian kejadian baik Tl maupun non-TI yang tidak diinginkan/diharapkan yang dapat mengganggu operasional proses layanan dan mengancam keamanan informasi maupun kualitas layanan.
5. **Resolusi** adalah tindakan yang diambil untuk memperbaiki akar masalah atau insiden sehingga memberikan solusi.
6. **Waktu Respon *{Response Time)*** adalah ukuran waktu yang dibutuhkan untuk menjawab telepon dan email, atau untuk memulai diagnosis dalam insiden.
7. **Dampak** ditentukan oleh beberapa fungsi/layanan yang berpengaruh. Ada 3 (tiga) dampak,

Penentuan Krit **kalitas Gangguan / Insiden**

Klasifikasi	Kemungkinan	Dampak	Jenis Gangguan / Insiden	RTO*& RPO*
Kritikal	Sering terjadi (bisa terjadi >5x setahun)	• Gangguan operasional, dengan hampir SLA tidak tercapai • Mendapatkan keluhan dari setiap *stakeholder*	• *Technical incident (cyber attack/malware/sabotase* yang mengakibatkan sistem *down* lebih dari 3 hari) • *Fault* (kerusakan perangkat utama yang mengakibatkan sistem *down* lebih dari 3 hari)	RTO: Maks 96 Jam RPO: Maks 96 Jam
Sedang	Jarang terjadi atau terjadi sesekali waktu (bisa terjadi 1-5 x setahun)	• Gangguan operasional ada 1-3 SLA tidak tercapai • Mendapatkan keluhan dari beberapa stakeholder	• *Technical incident (cyber attack/malware/sabotase* yang mengakibatkan sistem *down down* 1-3 hari) • *Fault* (kerusakan perangkat utama dan/atau pendukung yang mengakibatkan sistem *down* 1-3 hari)	RTO: Maks 72 Jam RPO: Maks 72 Jam
Rendah	Relatif Kecil dengan kemungkinan lx terjadinya dalam rentang waktu >1 - 3 tahun	• Operasional dan SLA tidak terlalu berdampak • Tidak sampai menerima keluhan dari stakeholder	• *Fault* (Kerusakan perangkat pendukung namun tidak terlalu berdampak terhadap SLA dan adanya potensi penyusup) • *Service request* (akses akun, lupa *user name/password}* • *Assistance*	RTO: Maks 24 Jam RPO: Maks 24 Jam

yaitu:

a. Kritis - sistem tidak berlaku dan ketidakmampuan menggunakan sistem memiliki efek penting pada operasi.
b. **Sedang -** sistem ini dapat digunakan tetapi dengan fungsi terbatas (sistem sebagian tidak berlaku, namun masih dapat digunakan).
c. Rendah - sistem dapat digunakan dan material tidak mempengaruhi operasi atau masalah yang berkaitan dengan sistem bug vendor.

Dampak dari insiden akan digunakan dalam menentukan prioritas untuk resolusi.

8. ***Service Level Agreement*** adalah kesepakatan antara DITJEN DUKCAPIL dan penyedia layanan

D. REFERENSI

1. ISO/IEC 27001:2013, *Clause 10.1 - Nonconformity and Corrective Action.*
2. ISO/IEC 27001:2013, *Annex A. 16- Information Security Incident Management.*
3. ISO/IEC 27001:2013, *Annex A.16.1 - Management of Information Security Incidents and Improvements.*

Nomor Standar Operasional Prosedur	SOP-02/SMKI-PIAK
Tanggal Pembuatan	10 Mei 2022
Tanggal Revisi	-
Tanggal Pengesahan	02 Juni 2022
Disahkan Oleh	Kepala Dinas Kependudukan dan Pencatatan Sipil Kota Yogyakarta Dra. Septi Sri Rejeki NIP. 196809231995032007
Nama Standar Operasional Prosedur	**Pengelolaan Gangguan & Manajemen Insiden**

TUJUAN

1. Prosedur ini bertujuan untuk menjelaskan proses pengelolaan gangguan terkait dengan layanan TIK di Dinas Kependudukan dan Pencatatan Sipil
2. Prosedur ini bertujuan untuk mengembalikan operasi layanan normal secepat mungkin dan meminimalkan dampak merugikan pada operasi layanan, sehingga memastikan bahwa tingkat terbaik dari kualitas layanan sebagaimana didefinisikan sebagai operasi layanan dalam batas SLA *(Service Level Agreement).*
3. Prosedur ini disusun untuk menjamin bahwa setiap insiden dilaporkan, ditindaklanjuti, dan dievaluasi untuk meminimalkan dampak dan mencegah terulangnya insiden

RUANG LINGKUP

1. Penanganan jika terjadi gangguan (insiden)/permasalahan dimulai dari pengklasifikasian (kategorisasi dan penentuan skala prioritas) dan dukungan awal bagi pegawai pada saat terjadi insiden.
2. Pelaporan, tindak lanjut, dan evaluasi insiden keamanan informasi di lingkungan Dinas Kependudukan dan Pencatatan Sipil

DASAR HUKUM

1. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Tahun 2006 Nomor 124 Tambahan Lembaran Negara 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 Tahun 2013 Nomor 232 Tambahan Lembaran Negara Nomor 5475).
2. 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).
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182).
4. Peraturan Menteri Dalam Negeri Nomor 4 Tahun 2011 tentang Standar Operasional Prosedur di Lingkungan Kemendagri (Berita Negara Republik Indonesia Tahun 2011 Nomor 24).

KUALIFIKASI PELAKSANA

1. Pendidikan minimal D-lll atau sederajat.
2. Memahami konsep teknis sistem/aplikasi/perangkat teknologi informasi.
3. Memahami konsep dasar keamanan informasi.

5. Peraturan Menteri Pendayagunaan Aparatur Negera dan Reformasi Birokrasi Nomor 35 Tahun 2012 tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan (Berita Negara Republik Indonesia Tahun 2012 Nomor 649).
6. Peraturan Menteri Dalam Negeri Nomor 43 Tahun 2015 tentang Organisasi dan Tatakerja Kemendagri (Berita Negara Republik Indonesia Tahun 2015 Nomor 564).
7. Peraturan Menteri Dalam Negeri No. 7 Tahun 2019 tentang Pelayanan Administrasi Kependudukan Secara Daring (Berita Negara Republik Indonesia Tahun 2019 Nomor 152).
8. Peraturan Menteri Dalam Negeri Nomor 95 Tahun 2019 tentang Sistem Informasi Administrasi Kependudukan (Berita Negara Republik Indonesia Tahun 2019 Nomor 1478). dan
9. Peraturan Menteri Dalam Negeri Nomor 57 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Administrasi Kependudukan (Berita Negara Republik Indonesia Tahun 2021 Nomor 1272).

KETERKAITAN

1. MN-01/DITJEN-DUKCAPIL - Pedoman Sistem Manajemen Keamanan Informasi.
2. MN-02/DITJEN-DUKCAPIL - Pedoman Kebijakan Keamanan Informasi.
3. SOP Pengelolaan Keluhan dan Kepuasan Pelanggan.

PERINGATAN

1. Jika prosedur ini tidak dilaksanakan, maka setiap insiden/gangguan layanan yang terjadi tidak tercatat dan tidak dapat ditelusuri status penyelesaiannya.
2. Jika prosedur ini tidak dijalankan dengan konsisten, maka informasi insiden tidak dapat dianalisis serta tidak dapat diupayakan pencegahan dini.
3. Koordinasi antar direktorat menentukan kelancaran penanganan insiden.

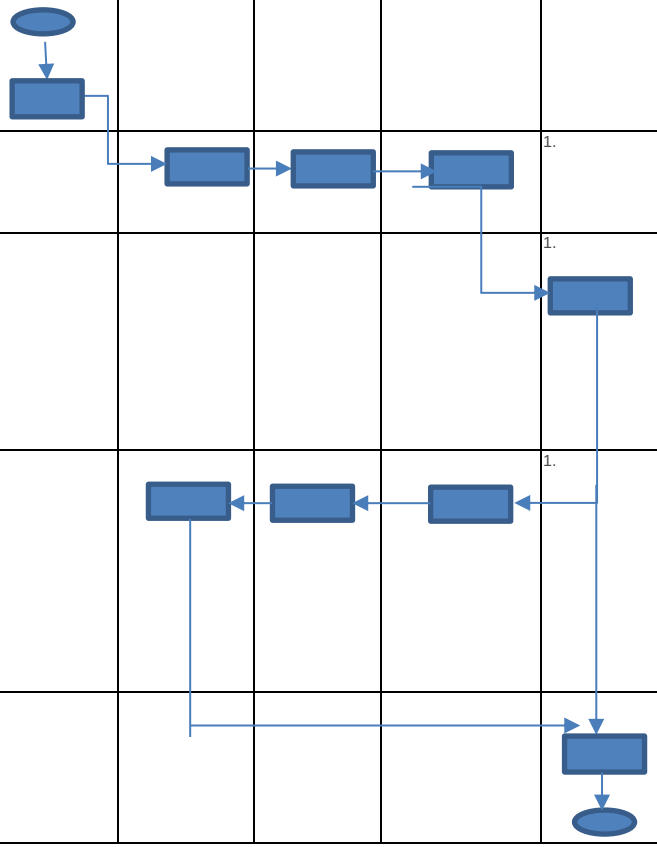
PERALATAN PERLENGKAPAN

1. Komputer kerja.
2. Jaringan komputer.
3. Alat komunikasi.
4. Tools Pengelolaan Insiden.
5. Instruksi Kerja dan Modul Penanganan Insiden.

6

STANDAR OPERASIONAL PROSEDUR PENGELOLAAN GANGGUAN
& MANAJEMEN INSIDEN

No	Uraian Pelaksanaan	Pelaksana					Mutu Baku			Keterangan
		Pelapor	AK PIAK	**Kabid PIAK**	Ka Dinas	**Tim Penanganan Gangguan Ditjen Dukcapil**	**Perlengkapan**	**Waktu**	**Output**	
1	Pelapor/unit kerja terkait menghubungi *Helpdesk* di Bidang PIAK melalui aplikasi, *email*, *message*, dan lain-lain.						Alat Komunikasi	N/A	Laporan	
2	Tim *Helpdesk* mencatat laporan gangguan dari pelapor dan sesegera mungkin memberi tanggapan sebagai tindakan cepat tanggap yang perlu dilakukan sesegera mungkin untuk mengurangi dampak insiden serta me;aporkan ke Ka Dina					1.	1. *Incident Report* 2. Form Pencatatan Gangguan/Permasalahan 3. *Tools*	5 Menit	Tiket Laporan	Contohnya adalah memblokir akses, melaporkan kepada petugas untuk penggeledahan, mengisolasi jaringan untuk mencegah penyebaran virus, dan sebagainya.
3	Ka Dinas melapor ke Tim *Helpdesk* Pusat untuk melakukan pengamanan gangguan dan bukti insiden. Pengamanan bukti gangguan bertujuan untuk memastikan bahwa pihak yang sengaja menyebabkan gangguan tidak menghilangkan bukti-bukti terkait.					1.	1. *Incident Report* 2. Form Pencatatan Gangguan/Permasalahan 3. *Tools* 4. Rekomendasi serta rencana pengujian		Eskalasi Hasil Analisa Rekomendasi serta rencana pengujian	a. Ketua Tim Penanganan Gangguan akan mengkoordinasikan analisis masalah dan *workaround solution* pada unit kerja terkait. b. Analisis problem dilakukan oleh Ketua Tim Penanganan Gangguan dibantu oleh para spesialis dan/ atau *Subject Matter Expert* (SME) yang ada di masing- masing Direktorat terkait. c. Analisis dilakukan dengan metodologi yang baik sehingga ditemukan akar masalahnya.
4	Menunggu rekomendasi perbaikan dan atautindakan perbaikan dari Tim Gangguan di Pusat serta melaksanakan tindakan-tindakan sesuai arahan Ti Gangguan di Pusat					1.	1. *Incident Report* 2. Form Pencatatan Gangguan/Permasalahan 3. *Tools*		Monitoring	d. PHasil/progres analisis dicatatkan dalam *Problem Log.* e. Setiap akar masalah yang ditemukan dalam analisis harus diuji coba oleh tim Penanganan Gangguan terkait *(second/third level support)* di suatu lingkungan f. Setiap masalah yang belum dapat ditemukan solusi permanennya dalam waktu maksimal 1 bulan, maka harus dicarikan *workaround solution* g.
7	Tim Penanganan Gangguan *meng-update* status penanganan gangguan setiap ada progres tindakan perbaikan hingga *closed.*						Monitoring		*Closing* dan log insiden	a. pengujianroblem dapat di-cfose apabila insiden yang disebabkan telah benar-benar terselesaikan. Solusi *workaround* yang pernah dilakukan dan solusi permanen dicatatkan dalam *database* b. Penanganan yang dilakukan dilakukan serta bukti-bukti yang telah diamankan dicatatkan dalam *log* laporan



DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL
KOTA YOGYAKARTA

STANDAR OPERASIONAL PROSEDUR PENGAMANAN INFORMASI UNTUK PEGAWAI DAN PIHAK KETIGA

STANDAR OPERASIONAL PROSEDUR
PENGAMANAN INFORMASI UNTUK PEGAWAI & PIHAK KETIGA

A. PENDAHULUAN

Prosedur ini diperlukan untuk mengatur identifikasi risiko, pemantauan, dan audit terkait pengamanan informasi terhadap seluruh pegawai serta kesesuaian pelayanan pihak ketiga yang melakukan pekerjaan di lingkungan Dinas Kependudukan dan Pencatatan Sipil berdasarkan surat perjanjian kerja pihak ketiga.

B. STANDAR

1. Seluruh pegawai Dinas Kependudukan dan Pencatatan Sipil memahami ketentuan keamanan informasi dan menjamin terjaganya keamanan informasi pada pegawai yang tidak lagi bertugas di DITJEN DUKCAPIL
2. Terjaminnya keamanan informasi dari pihak ketiga yang berada di lingkungan kerja Dinas Kependudukan dan Pencatatan Sipil

C. DEFINISI

1. Informasi adalah satu atau lebih entitas data yang saling berhubungan dan mempunyai makna tertentu.
2. Pihak Ketiga adalah tenaga kerja *outsourcing*, Praktik Kerja Lapangan (PKL), pihak yang terafiliasi, penyedia eksternal dan petugas dinas/lembaga lain yang melakukan kegiatan yang terkait dengan tugas pokok proses pelayanan pengadaan barang/jasa di DITJEN DUKCAPIL.
3. Tenaga Kerja ***Outsourcing*** adalah tenaga kerja yang ditempatkan di unit kerja dalam rangka melaksanakan tugas di unit kerja tersebut.

D. REFERENSI

1. ISO/IEC 27001:2013 - Annex A.7.1.2 - *Terms and Condition of Employment.*
2. ISO/IEC 27001:2013 - Annex A.15.1 - *Information security in supplier relationship.*
3. ISO/IEC 27001:2013 - Annex A.15.2 - *Supplier service delivery management.*

Nomor Standar Operasional Prosedur	S0P-O3/SMKI-PIAK
Tanggal Pembuatan	10 Mei 2022
Tanggal Revisi	-
Tanggal Pengesahan	02 Juni 2022
Disahkan Oleh	Kepala Dinas Kependudukan dan Pencatatan Sipil Kota Yogyakarta Dra. Septi Sri Rejeki NIP. 196809231995032007
Nama Standar Operasional Prosedur	Pengamanan Informasi Untuk Pegawai Dan Pihak Ketiga

TUJUAN

Prosedur ini bertujuan untuk menjamin seluruh pegawai Dinas Kependudukan dan Pencatatan Sipil memahami ketentuan keamanan informasi dan menjamin terjaganya keamanan informasi pada pegawai yang tidak lagi bertugas di Dinas Kependudukan dan Pencatatan Sipil

RUANG LINGKUP

Pelaksanaan sosialisasi dan internalisasi keamanan informasi pada pegawai baru dan proses serah terima asset informasi pada pegawai yang tidak lagi bertugas di Dinas Kependudukan dan Pencatatan Sipil Pelaksanaan sosialisasi keamanan informasi pada pihak ketiga (eksternal) yang akan berkerja atau meminjam asset/informasi di Dinas Kependudukan dan Pencatatan Sipil

DASAR HUKUM

1. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Tahun 2006 Nomor 124 Tambahan Lembaran Negara 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 Tahun 2013 Nomor 232 Tambahan Lembaran Negara Nomor 5475).
2. 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).
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182).
4. Peraturan Menteri Dalam Negeri Nomor 4 Tahun 2011 tentang Standar Operasional Prosedur di Lingkungan Kemendagri (Berita Negara Republik Indonesia Tahun 2011 Nomor 24).

KUALIFIKASI PELAKSANA

1. Pendidikan minimal D-lll atau sederajat.
2. Memahami konsep teknis sistem/aplikasi/perangkat teknologi informasi.
3. Memahami konsep dasar keamanan informasi

5. Peraturan Menteri Pendayagunaan Aparatur Negera dan Reformasi Birokrasi Nomor 35 Tahun 2012 tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan (Berita Negara Republik Indonesia Tahun 2012 Nomor 649).
6. Peraturan Menteri Dalam Negeri Nomor 43 Tahun 2015 tentang Organisasi dan Tatakerja Kemendagri (Berita Negara Republik Indonesia Tahun 2015 Nomor 564).
7. Peraturan Menteri Dalam Negeri No. 7 Tahun 2019 tentang Pelayanan Administrasi Kependudukan Secara Daring (Berita Negara Republik Indonesia Tahun 2019 Nomor 152).
8. Peraturan Menteri Dalam Negeri Nomor 95 Tahun 2019 tentang Sistem Informasi Administrasi Kependudukan (Berita Negara Republik Indonesia Tahun 2019 Nomor 1478). dan
9. Peraturan Menteri Dalam Negeri Nomor 57 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Administrasi Kependudukan (Berita Negara Republik Indonesia Tahun 2021 Nomor 1272).

KETERKAITAN

1. MN-01/DITJEN-DUKCAPIL - Pedoman Sistem Manajemen Keamanan Informasi.
2. MN-02/DITJEN-DUKCAPIL - Pedoman Kebijakan Keamanan Informasi.
3. SOP Manajemen Aset.
4. SOP Pengadaan dan Evaluasi Kinerja Penyedia Eksternal
5. SOP Pengelolaan SDM.

PERALATAN PERLENGKAPAN

1. Komputer kerja.
2. Alat komunikasi.

PERINGATAN

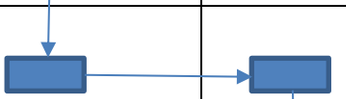
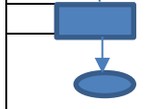
1. Jika prosedur ini tidak dilaksanakan, maka ada potensi kebocoran informasi dikarenakan tidak adanya jaminan untuk menjaga kerahasiaan informasi.
2. Jika prosedur ini tidak dijalankan dengan konsisten, maka tidak dapat diupayakan pencegahan dini untuk mencegah bocornya informasi penting perusahaan.
3. Koordinasi antar direktorat menentukan kelancaran pengelolaan keamanan sumber daya manusia.

PENCATATAN DAN PENDATAAN

1. Perjanjian Kerahasiaan *(Non Disclosure Agreement/NDA)*, dimana memastikan setiap pegawai atau pihak ketiga yang bekerja di lingkungan Dinas Kependudukan dan Pencatatan Sipil dapat menjaga informasi penting yang sifatnya terbatas/rahasia.
2. Kuisioner Keamanan Informasi.

STANDAR OPERASIONAL PROSEDUR
PENGAMANAN INFORMASI UNTUK PEGAWAI DAN PIHAK KE TIGA

Alur Proses Pengamanan Informasi Pada Pegawai

No	Uraian Pelaksanaan	Pelaksana		Mutu Baku			Keterangan
		Seluruh Pegawai DITJEN DUKCAPIL	Koordinador STKI	Perlengkapan	Waktu	Output	
1	Setiap pegawai wajib menandatangani Pakta Integritas *(Non-Disclosure Agreement)*			Perjanjian kerahasiaan *(nondisclosure agreement)*	5 Menit	Perjanjian kerahasiaan *(nondisclosure agreement)* yang sudah diisi	
2	Setiap pegawai baru harus dilakukan proses sosialisasi keamanan informasi oleh Koordinator STKI			Kebijakan Keamanan Informasi	1 Hari Kerja	Bukti Sosialisasi	a. internalisasi keamanan informasi kepada seluruh pegawai
3	Tim STKI Bidang PIAK harus memastikan bahwa pegawai baru mendapatkan aset Tl, hak akses (fisik dan logikal) agar dapat mengakses informasi yang dibutuhkannya untuk kebutuhan pekerjaan			Access *Control Matrix*	N/A	Bukti Serah Terima	
4	Koordinator STKI memastikan setiap perubahan tugas dan kewenangan pada pegawai harus dilakukan serah terima pengembalian informasi dan aset lainnya			Daftar Aset	N/A	Bukti Serah Terima	Serah terima asset meliputi: a. Serah terima asset fisik b. Serah terima aset informasi c. Serah terima tanggung jawab d. Serah terima akses
5	Proses serah terima ini didokumentasikan dalam Berita Acara Serah Terima sesuai SOP Manajemen Aset			Bukti Serah Terima	1 Hari Kerja	Bukti Serah Terima	