SALINAN

BADAN KEPENDUDUKAN DAN
KELUARGA BERENCANA NASIONAL
REPUBLIK INDONESIA

PERATURAN BADAN KEPENDUDUKAN
DAN KELUARGA BERENCANA NASIONAL
REPUBLIK INDONESIA
NOMOR 17 TAHUN 2023
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
BADAN KEPENDUDUKAN DAN KELUARGA BERENCANA NASIONAL

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN KEPENDUDUKAN DAN KELUARGA BERENCANA NASIONAL
REPUBLIK INDONESIA,

Menimbang :

a. bahwa untuk melindungi dan menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi di lingkungan Badan Kependudukan dan Keluarga Berencana Nasional, perlu dibangun sistem manajemen keamanan informasi;
b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan untuk melaksanakan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, perlu menetapkan Peraturan Badan Kependudukan dan Keluarga Berencana Nasional tentang Sistem Manajemen Keamanan Informasi Badan Kependudukan dan Keluarga Berencana Nasional;

Mengingat :

1. Undang-Undang Nomor 52 Tahun 2009 tentang Perkembangan Kependudukan dan Pembangunan Keluarga (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 161, Tambahan Lembaran Negara Republik Indonesia Nomor 5080);
2. 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);
3. Peraturan Pemerintah Nomor 87 Tahun 2014 tentang Perkembangan Kependudukan dan Pembangunan Keluarga, Keluarga Berencana, dan Sistem Informasi Keluarga (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 319, Tambahan Lembaran Negara Republik Indonesia Nomor 5614);
4. Keputusan Presiden Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non

Departemen sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Presiden Nomor 145 Tahun 2015 tentang Perubahan Kedelapan atas Keputusan Presiden Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non Kementerian (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 322);

5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
6. Peraturan Kepala Badan Kependudukan dan Keluarga Berencana Nasional Nomor 82/PER/B5/2011 tentang Organisasi dan Tata Kerja Perwakilan Badan Kependudukan dan Keluarga Berencana Nasional Provinsi;
7. Peraturan Badan Kependudukan dan Keluarga Berencana Nasional Nomor 11 Tahun 2020 tentang Organisasi dan Tata Kerja Badan Kependudukan dan Keluarga Berencana Nasional (Berita Negara Republik Indonesia Tahun 2020 Nomor 703);
8. Peraturan Badan Kependudukan dan Keluarga Berencana Nasional Nomor 12 Tahun 2020 tentang Organisasi dan Tata Kerja Unit Pelaksana Teknis Balai Pendidikan, dan Pelatihan Kependudukan, dan Keluarga Berencana (Berita Negara Republik Indonesia Tahun 2020 Nomor 779);
9. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
10. Peraturan Badan Kependudukan dan Keluarga Berencana Nasional Nomor 9 Tahun 2022 tentang Tata Kelola Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Kependudukan dan Keluarga Berencana Nasional (Berita Negara Republik Indonesia Tahun 2022 Nomor 640);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN KEPENDUDUKAN DAN KELUARGA BERENCANA NASIONAL TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI BADAN KEPENDUDUKAN DAN KELUARGA BERENCANA NASIONAL.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Badan ini yang dimaksud dengan:

1. Ancaman adalah potensi penyebab insiden yang tidak diinginkan, yang dapat mengakibatkan bahaya pada sistem atau organisasi.

2. Informasi adalah data dalam segala bentuknya (*input*, *output*, dan data terproses) yang digunakan oleh aktivitas bisnis.
3. Keamanan Informasi adalah proteksi perlindungan Informasi dari Ancaman yang relevan untuk memastikan keberlangsungan bisnis, dan meminimalkan risiko bisnis.
4. Kendali adalah tindakan yang memelihara dan/atau memodifikasi risiko.
5. Risiko adalah segala kejadian dalam setiap aktivitas organisasi yang timbul karena faktor eksternal maupun internal, yang mengandung potensi menghambat pencapaian tujuan organisasi atau mengoptimalkan peluang bisnis.
6. Manajemen Risiko adalah aktivitas terkoordinasi untuk identifikasi, penilaian, dan penentuan prioritas Risiko yang kemudian akan dikelola, dipantau, dan dikontrol untuk mengurangi dampak dan/atau kemungkinan terjadinya Risiko tersebut.
7. Rencana Tindak Lanjut Risiko yang selanjutnya disebut RTL adalah respon yang direncanakan manajemen untuk menindaklanjuti hasil evaluasi Risiko.
8. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah pendekatan sistem manajemen keamanan Aset Informasi terutama dalam konteks *confidentiality* (kerahasiaan), *integrity* (keutuhan), dan *availability* (ketersediaan).
9. *Statement of Applicability* yang selanjutnya disingkat SoA adalah dokumen komprehensif yang menguraikan Kendali Keamanan Informasi sesuai hasil penilaian Risiko.
10. Pemangku Kepentingan adalah orang atau organisasi yang dapat memengaruhi, dipengaruhi, atau menganggap dirinya dipengaruhi oleh suatu keputusan atau aktivitas.
11. Badan Kependudukan dan Keluarga Berencana Nasional yang selanjutnya disingkat BKKBN adalah Instansi Pemerintah yang melaksanakan tugas pemerintahan di bidang pengendalian penduduk dan penyelenggaraan keluarga berencana.

Pasal 2

Peraturan Badan ini dimaksudkan sebagai pedoman bagi pimpinan unit kerja di lingkungan BKKBN dalam mengelola Keamanan Informasi.

BAB II
SIKLUS SISTEM MANAJEMEN
KEAMANAN INFORMASI

Bagian Kesatu
Umum

Pasal 3

Siklus SMKI meliputi:
a. penetapan ruang lingkup;
b. penetapan penanggung jawab;
c. perencanaan;
d. dukungan pengoperasian;
e. evaluasi kinerja; dan
f. perbaikan berkelanjutan,

terhadap keamanan informasi dalam sistem pemerintahan berbasis elektronik.

Bagian Kedua
Penetapan Ruang Lingkup

Pasal 4

(1) Penetapan ruang lingkup SMKI BKKBN dilakukan melalui tahapan:
    a. identifikasi isu;
    b. identifikasi kebutuhan; dan
    c. penetapan lingkup SMKI.
(2) Identifikasi isu sebagaimana dimaksud pada ayat (1) huruf a dilakukan dengan cara mengidentifikasi isu internal maupun eksternal yang berpengaruh dalam pencapaian *outcome* SMKI.
(3) Identifikasi kebutuhan sebagaimana dimaksud pada ayat (1) huruf b dilakukan dengan cara mengidentifikasi Pemangku Kepentingan terkait SMKI dan kebutuhan serta ekspektasi masing-masing Pemangku Kepentingan tersebut.
(4) Penetapan lingkup SMKI sebagaimana dimaksud pada ayat (1) huruf c dilakukan dengan cara analisis lingkup dan batasan SMKI dengan mempertimbangkan isu dan kebutuhan yang telah diidentifikasi.

Bagian Ketiga
Penetapan Penanggung Jawab

Pasal 5

(1) Penanggung jawab SMKI dijabat oleh Sekretaris Utama BKKBN.
(2) Penanggung jawab SMKI memiliki tugas:
    a. memastikan tujuan dan kebijakan SMKI yang selaras dengan arahan strategis BKKBN;
    b. memastikan terjadinya integrasi antara SMKI dengan proses bisnis BKKBN;
    c. memastikan ketersediaan sumber daya SMKI;
    d. mengkomunikasikan pentingnya SMKI dan pemenuhan persyaratannya kepada Pemangku

Kepentingan;
e. memberikan arahan dan dukungan kepada manajemen dan pelaksana SMKI; dan
f. memastikan tercapainya tujuan SMKI.

(3) Dalam melaksanakan tugas, penanggung jawab SMKI dibantu oleh tim SMKI.

(4) Tim SMKI sebagaimama dimaksud pada ayat (3) ditetapkan oleh Kepala BKKBN.

Bagian Keempat
Perencanaan SMKI

Pasal 6

(1) Perencanaan SMKI dilakukan melalui tahapan:
a. penilaian Risiko Keamanan Informasi;
b. penetapan SoA; dan
c. perencanaan sasaran Keamanan Informasi.

(2) Tim SMKI melakukan penilaian Risiko Keamanan Informasi sebagaimana dimaksud pada ayat (1) huruf a dengan tahapan:
a. penetapan pendekatan penilaian Risiko Keamanan Informasi yang akan digunakan oleh BKKBN;
b. identifikasi, analisis, evaluasi, dan penanganan Risiko yang akan menghasilkan analisis Risiko dan RTL;
c. RTL memuat Kendali yang dibutuhkan untuk memitigasi Risiko;
d. Pelaksanaan Kendali diarahkan pada upaya mengurangi Risiko Keamanan Informasi sampai batas yang dapat diterima oleh BKKBN; dan
e. Persetujuan dari Kepala BKKBN atas hasil analisis Risiko Keamanan Informasi dan RTL BKKBN.

(3) Sekretaris Utama BKKBN selaku penanggung jawab SMKI menetapkan SoA sebagaimana dimaksud pada ayat (1) huruf b dengan memilih Kendali Keamanan Informasi sesuai dengan hasil penilaian Risiko.

(4) Tim SMKI melakukan perencanaan sasaran Keamanan Informasi sebagaimana dimaksud pada ayat (1) huruf c dengan berdasarkan pada kebijakan SMKI dan kebutuhan Keamanan Informasi.

(5) Perencanaan sasaran Keamanaan Informasi sebagaimana dimaksud pada ayat (4) dapat dilakukan perubahan.

(6) Perubahan sebagaimana dimaksud pada ayat (5) dilaksanakan sesuai dengan Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Bagian Kelima
Dukungan Pengoperasian

Pasal 7

(1) Dalam melaksanakan SMKI BKKBN diperlukan

dukungan:
a. sumber daya;
b. penyampaian komunikasi dan dokumentasi SMKI; dan
c. pengendalian dokumen.

(2) Dukungan sumber daya sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui:
a. persetujuan rencana kerja anggaran terkait dan realisasi pengadaannya untuk keberjalanan SMKI; dan
b. alokasi sumber daya manusia Keamanan Informasi yang memadai untuk keberjalanan SMKI, yang memenuhi aspek kuantitas dan kualitas yang disyaratkan.

(3) Dukungan penyampaian komunikasi dan dokumentasi SMKI sebagaimana dimaksud pada ayat (1) huruf b dilakukan melalui:
a. penyampaian komunikasi Keamanan Informasi oleh Kepala BKKBN kepada Pemangku Kepentingan; dan
b. pengelolaan dan pengendalian dokumentasi SMKI oleh Tim SMKI yang sesuai dengan prosedur Keamanan Informasi yang berlaku dan memenuhi aspek ketersediaan, keutuhan, kerahasiaan dalam hal akses, distribusi, penyimpanan, perubahan/Kendali versi, retensi serta disposisi.

(4) Dukungan pengendalian dokumen sebagaimana dimaksud pada ayat (1) huruf c dilakukan melalui:
a. pengendalian distribusi dokumen sesuai dengan klasifikasi Keamanan Informasi dokumen;
b. pengendalian dokumen yang digunakan merupakan dokumen yang terbaru;
c. kebijakan, prosedur, dan pedoman dipublikasikan secara terpusat; dan
d. dokumen yang sudah tidak digunakan, sudah digantikan oleh dokumen versi terbaru, atau ditarik karena alasan tertentu, ditandai sebagai dokumen kadaluarsa atau tidak digunakan sejak tanggal tertentu.

Pasal 8

(1) Pengoperasian SMKI dilakukan dengan tahapan:
a. formulasi rencana penanganan Risiko;
b. implementasi rencana pengendalian Risiko;
c. pengendalian perubahan tahap operasional; dan
d. penilaian Risiko Keamanan Informasi tahap operasional.

(2) Formulasi rencana penanganan Risiko sebagaimana dimaksud pada ayat (1) huruf a meliputi rencana tindakan, sumber daya, tanggung jawab, serta prioritas yang memadai untuk mengelola Risiko Keamanan Informasi di BKKBN.

(3) Implementasi rencana pengendalian Risiko sebagaimana dimaksud pada ayat (1) huruf b dilakukan dalam rangka mencapai tujuan pengendalian dengan mempertimbangkan aspek pendanaan dan alokasi

peran serta tanggung jawab Keamanan Informasi di BKKBN.

(4) Pengendalian perubahan tahap operasional sebagaimana dimaksud pada ayat (1) huruf c dilakukan dengan mereviu dampak perubahan dan melakukan tindakan untuk memitigasi Risiko perubahan tersebut.

(5) Penilaian Risiko Keamanan Informasi tahap operasional sebagaimana dimaksud pada ayat (1) huruf d dilakukan secara rutin atau pada saat perubahan sesuai dengan Kebijakan Manajemen Risiko yang berlaku.

Bagian Keenam
Evaluasi Kinerja SMKI

Pasal 9

(1) Evaluasi kinerja SMKI dilakukan melalui tahapan:
   a. evaluasi pencapaian sasaran SMKI;
   b. audit internal; dan
   c. tinjauan manajemen.

(2) Tim SMKI melakukan evaluasi pencapaian sasaran SMKI sebagaimana dimaksud pada ayat (1) huruf a melalui evaluasi pencapaian kinerja Keamanan Informasi sesuai dengan sasaran yang telah ditetapkan sebelumnya.

(3) Unit kerja yang melaksanakan fungsi pengawasan internal melakukan audit internal sebagaimana dimaksud pada ayat (1) huruf b untuk memastikan persyaratan SMKI telah dipenuhi dan terimplementasi serta terpelihara secara efektif.

(4) Penanggung jawab SMKI melakukan tinjauan manajemen sebagaimana dimaksud pada ayat (1) huruf c terhadap:
   a. status tinjauan manajemen sebelumnya;
   b. perubahan isu Keamanan Informasi;
   c. perubahan pihak berkepentingan dan kebutuhannya;
   d. *feedback* kinerja Keamanan Informasi;
   e. *feedback* dari pihak terkait;
   f. hasil asesmen Risiko dan status *risk treatment*; dan
   g. peluang peningkatan kematangan SMKI BKKBN.

(5) Evaluasi Kinerja SMKI sebagaimana dimaksud pada ayat (1) dilaksanakan secara rutin paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Bagian Ketujuh
Perbaikan Berkelanjutan

Pasal 10

(1) Tim SMKI melakukan upaya tindak lanjut berdasarkan hasil tinjauan manajemen sebagaimana dimaksud dalam Pasal 9 ayat (4) melalui peningkatan kesesuaian, kecukupan, dan efektivitas SMKI di BKKBN.

(2) Berdasarkan hasil evaluasi kinerja SMKI ditemukan ketidaksesuaian SMKI, tim SMKI melakukan:
   a. peningkatan Kendali dan perbaikan dalam rangka

mitigasi Risiko;
b. mitigasi dampak atas ketidaksesuaian SMKI;
c. mengevaluasi efektivitas tindakan koreksi; dan
d. pendokumentasian hasil tindak lanjut ketidaksesuaian SMKI.

BAB III
PENGENDALIAN SISTEM MANAJEMEN
KEAMANAN INFORMASI

Pasal 11

(1) Kendali sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf c merupakan seperangkat upaya dalam rangka memitigasi Risiko.
(2) Kendali Keamanan Informasi sebagaimana dimaksud pada ayat (1) terbagi atas kategori organisasi, orang, fisik, dan teknologi.
(3) Ketentuan mengenai Kendali Keamanan Informasi sebagaimana dimaksud pada ayat (2) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

BAB IV
KETENTUAN PENUTUP

Pasal 12

Peraturan Badan ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Jakarta
pada tanggal 8 November 2023

KEPALA BADAN KEPENDUDUKAN
DAN KELUARGA BERENCANA NASIONAL
REPUBLIK INDONESIA,

ttd

HASTO WARDOYO

Diundangkan di Jakarta
pada tanggal 20 November 2023

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

ttd

ASEP N. MULYANA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2023 NOMOR 913

Salinan sesuai dengan aslinya
Badan Kependudukan dan Keluarga Berencana Nasional
Kepala Biro Hukum, Organisasi, dan Tata Laksana

Puji Rihatiningsih

LAMPIRAN
PERATURAN BADAN KEPENDUDUKAN
DAN KELUARGA BERENCANA NASIONAL
REPUBLIK INDONESIA
NOMOR 17 TAHUN 2023
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
BADAN KEPENDUDUKAN DAN KELUARGA BERENCANA NASIONAL

A. Latar Belakang

Informasi menjadi Aset penting bagi BKKBN. Oleh karena itu BKKBN harus menjaga Keamanan Informasi yang dimiliki termasuk Informasi berbentuk fisik maupun elektronik. Penjagaan Informasi termasuk menjaga sistem yang mengolah, menyimpan maupun mentransmisikan Informasi. Penjagaan sistem termasuk sistem yang dikelola oleh internal maupun eksternal BKKBN. Sistem tersebut sudah digunakan setiap pegawai bahkan terdapat ketergantungan pada sistem. Oleh karena itu, pengamanan terhadap sistem menjadi penting bagi BKKBN.

Ancaman terhadap sistem Teknologi Informasi (TI) semakin banyak. Sehingga pengamanan Informasi dan maupun sistem TI harus semakin kuat. Oleh karena itu, pengamanan Informasi termasuk TI tidak bisa dilakukan parsial maupun hanya dilakukan hanya pada aspek teknis perangat lunak maupun keras. Tetapi pengamanan dilakukan lebih komprehensif pada semua aspek terkait.

Implementasi SMKI menjadi jawaban atas pengamanan Informasi yang lebih komprehensif. Implementasi SMKI akan mempertimbangkan regulasi relevan, isu yang berkembang, kebutuhan Pemangku Kepentingan maupun semua Risiko yang relevan. Implementasi SKMI juga memuat semua aspek relevan seperti organisasi, orang, fisik maupun teknologi yang digunakan.

SMKI memastikan beberapa hal berikut ini:

1. Kerahasiaan (*confidentiality*): memastikan bahwa Informasi hanya dapat diakses oleh pihak yang memiliki wewenang;
2. Keutuhan (*integrity*): memastikan bahwa Informasi tetap akurat dan lengkap, serta Informasi tersebut tidak dimodifikasi tanpa otorisasi yang jelas; dan
3. Ketersediaan (*availability*): memastikan bahwa Informasi dapat diakses oleh pihak yang memiliki wewenang ketika dibutuhkan.

Keberhasilan penerapan SMKI akan memberikan beberapa manfaat bagi BKKBN, antara lain:

a. meningkatkan *assurance* akan proteksi Aset Informasi terhadap setiap Ancaman;
b. memiliki *framework* yang terstruktur, komprehensif untuk: (i) mengidentifikasi, menilai Risiko Keamanan Informasi; (ii) memilih dan menerapkan Kendali terkait; dan (iii) mengukur, memperbaiki efektivitas Kendali tersebut;
c. perbaikan secara kontinyu atas lingkungan Kendali; dan
d. pemenuhan kepatuhan terhadap regulasi/hukum secara efektif.

B. Tujuan

Peraturan Badan ini digunakan sebagai pedoman pengelolaan Keamanan Informasi BKKBN dalam rangka melindungi Informasi ataupun Aset Informasi BKKBN terutama aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

C. Pengertian Umum

1. Autentikasi adalah pemberian keyakinan bahwa sebuah karakteristik yang diklaim dari suatu Entitas adalah benar.
2. Aset adalah segala hal yang memiliki nilai bagi organisasi.
3. Pengguna adalah pihak berkepentingan dengan akses ke sistem Informasi organisasi.
4. *Business Continuity Management* adalah kemampuan suatu organisasi untuk melanjutkan penyampaian produk dan layanan dalam jangka waktu yang dapat diterima pada kapasitas yang telah ditentukan selama terjadi gangguan.
5. *Business Continuity Plan* adalah Informasi terdokumentasi yang memandu organisasi untuk merespon gangguan dan memulihkan penyampaian produk dan layanan agar konsisten dengan kelangsungan tujuan bisnisnya.
6. *Business Impact Analysis* yang selanjutnya disingkat BIA adalah proses menganalisis dampak gangguan bisnis organisasi dari waktu ke waktu.
7. *Disaster Recovery Plan* yang selanjutnya disingkat DRP adalah rencana pemulihan yang dapat diambil jika terjadi suatu insiden yang berdampak pada sistem Keamanan Informasi suatu organisasi.
8. *Disposal* adalah suatu proses pemusnahan atau penghapusan Aset yang tidak lagi digunakan.
9. Disrupsi adalah insiden, baik yang terantisipasi maupun takterantisipasi, yang menyebabkan deviasi negatif takterencana terhadap penyampaian produk dan layanan yang diharapkan sesuai dengan sasaran organisasi.
10. Entitas adalah item yang relevan untuk tujuan pengoperasian suatu domain yang memiliki keberadaan khusus yang dapat dikenali. Suatu Entitas dapat berwujud fisik atau logikal.
11. Fasilitas Pemrosesan Informasi adalah setiap sistem pemrosesan Informasi, layanan, atau infrastruktur, atau lokasi fisik yang menaunginya.
12. Informasi Sensitif adalah Informasi yang perlu diproteksi dari ketaktersediaan, akses yang takterotorisasi, modifikasi, atau pengungkapan publik karena potensi efek buruk terhadap individu, organisasi, keamanan nasional, atau keselamatan publik.
13. Insiden Keamanan Informasi adalah satu atau beberapa peristiwa keamanan Informasi terkait dan teridentifikasi yang dapat membahayakan Aset organisasi atau membobol operasinya.
14. *IT Master Plan* adalah strategi organisasi dalam memanfaatkan teknologi Informasi sebagai *enabler* dan menambah keunggulan yang kompetitif guna mendukung visi dan misi organisasi.
15. *IT Service Desk* adalah titik kontak terpusat (*central point of contact*) antara Unit Pengelola TI dengan Pelanggan atau Pengguna atau Pengguna pada kegiatan operasional harian.
16. Kerentanan adalah kelemahan suatu Aset atau kontrol yang dapat dieksploitasi oleh satu atau lebih Ancaman.

17. Kontrol adalah tindakan yang memelihara dan/atau memodifikasi Risiko.
18. Kontrol Akses adalah cara untuk memastikan bahwa akses fisik dan logikal ke Aset terotorisasi dan dibatasi berdasarkan persyaratan keamanan bisnis dan Informasi.
19. Manajemen Insiden Keamanan Informasi adalah penerapan pendekatan yang konsisten dan efektif untuk penanganan Insiden Keamanan Informasi.
20. Mitra Kerja adalah penyedia yang menyalurkan layanan (barang dan/atau jasa) kepada Entitas bisnis di lingkungan BKKBN.
21. Pelanggaran Keamanan Informasi adalah pembobolan Keamanan Informasi yang mengarah pada kerusakan, kerugian, perubahan, pengungkapan, atau akses yang tidak diinginkan terhadap Informasi terlindungi yang dikirimkan, disimpan, atau diproses.
22. Perangkat Titik Akhir Pengguna adalah perangkat titik akhir (dapat merujuk ke komputer *desktop*, laptop, ponsel pintar, tablet, *thin client*, dsb) yang digunakan oleh Pengguna untuk mengakses layanan pemrosesan Informasi.
23. Perimeter adalah batas luar dari tempat tertutup atau terlindungi dan digunakan untuk memproteksi area yang berisi Informasi dan Aset terkait lainnya.
24. Peristiwa Keamanan Informasi adalah peristiwa yang mengindikasikan suatu kemungkinan Pelanggaran Keamanan Informasi atau kegagalan Kontrol.
25. *Personally Identifiable Information* yang selanjutnya disingkat PII adalah segala Informasi yang (a) dapat digunakan untuk membangun hubungan antara Informasi tersebut dengan orang perorangan yang terkait dengan Informasi semacam itu, atau (b) terkait atau dapat dikaitkan secara langsung atau tidak langsung dengan orang perorangan.
26. Proses adalah seperangkat aktivitas yang saling terkait atau berinteraksi yang menggunakan atau mentransformasi input untuk memberikan hasil.
27. Rekaman adalah Informasi yang dibuat, diterima, dan dipelihara sebagai bukti dan sebagai Aset oleh organisasi atau orang, dalam rangka obligasi legal (mencakup semua persyaratan hukum, statutori, regulatori, dan kontrak) atau dalam transaksi bisnis.
28. Rencana Jangka Panjang yang selanjutnya disebut RJPP BKKBN adalah dokumen terperinci yang menguraikan tujuan dan sasaran BKKBN selama periode waktu tertentu.
29. *Recovery Point Objective* yang selanjutnya disingkat RPO adalah titik waktu saat data dipulihkan setelah Disrupsi terjadi.
30. *Recovery Time Objective* yang selanjutnya disingkat RTO adalah jangka waktu saat level minimum layanan dan/atau produk serta sistem, aplikasi, atau fungsi pendukung dipulihkan setelah terjadinya suatu Disrupsi.
31. Serangan adalah upaya takterotorisasi yang berhasil atau takberhasil untuk menghancurkan, mengubah, melumpuhkan, mendapatkan akses ke suatu Aset atau upaya apapun untuk mengekspos, mencuri, atau menggunakan Aset secara takterotorisasi.
32. *Service Level Agreement* yang selanjutnya disingkat SLA adalah kontrak pengalihdayaan yang menguraikan tingkat layanan yang dijanjikan Mitra Kerja untuk diberikan kepada Pelanggan.
33. Sistem Informasi adalah seperangkat aplikasi, layanan, Aset teknologi Informasi, atau komponen lain penanganan Informasi.

D. Kendali Organisasi

1. Kebijakan Keamanan Informasi
   a. Kebijakan Keamanan Informasi terdiri dari 2 (dua) jenis yaitu Kebijakan umum Keamanan Informasi dan Kebijakan khusus Keamanan Informasi. Kebijakan umum Keamanan Informasi memuat arahan umum dan komitmen dalam mengelola keamanan infomasi. Sedangkan Kebijakan khusus Keamanan Informasi memuat Kendali Keamanan Informasi.
   b. Kebijakan Keamanan Informasi dan perubahan atas Kebijakan tersebut harus ditetapkan oleh Pimpinan.
   c. Reviu Kebijakan Keamanan Informasi harus dilakukan apabila terdapat perubahan:
      1) Strategi bisnis termasuk yang tertuang dalam RJPP BKKBN dan *IT Master Plan*;
      2) Lingkungan teknis di BKKBN;
      3) Regulasi, peraturan internal maupun kontrak yang relevan;
      4) Profil Risiko Keamanan Informasi;
      5) Lingkungan Ancaman Keamanan Informasi; dan
      6) *Lesson learned* atas kejadian maupun Insiden Keamanan Informasi.
   d. Kebijakan Keamanan Informasi harus dikomunikasikan ke seluruh pegawai, Mitra Kerja, dan Pemangku Kepentingan lainnya melalui media komunikasi yang tepat. Kebijakan Keamanan Informasi tersebut juga mudah diakses oleh Pemangku Kepentingan terkait.
   e. Kebijakan Keamanan Informasi yang dikomunikasikan ke pihak luar BKKBN dipastikan tidak melanggar peraturan kerahasian Informasi BKKBN.
2. Peran dan Tanggung Jawab dalam Keamanan Informasi
   a. Alokasi peran dan tanggung jawab dalam Keamanan Informasi harus dilakukan sesuai dengan Kebijakan Keamanan Informasi dan Kebijakan khusus. BKKBN harus menetapkan dan mengelola tanggung jawab untuk:
      1) Perlindungan Informasi dan Aset terkait lainnya;
      2) Melaksanakan Proses Keamanan Informasi tertentu;
      3) Aktivitas Manajemen Risiko Keamanan Informasi dan khususnya penerimaan Risiko residual (misalnya kepada pemilik Risiko); dan
      4) Semua personil yang menggunakan Informasi BKKBN dan Aset terkait lainnya.
   b. Tanggung jawab ini harus dilengkapi, jika perlu, dengan panduan yang lebih rinci untuk lokasi tertentu dan Fasilitas Pemrosesan Informasi. Individu dengan tanggung jawab Keamanan Informasi yang dialokasikan dapat memberikan tugas keamanan kepada orang lain. Namun, mereka tetap bertanggung jawab dan harus menentukan bahwa setiap tugas yang didelegasikan telah dilakukan dengan benar.
   c. Setiap area keamanan yang menjadi tanggung jawab individu harus ditetapkan, didokumentasikan, dan dikomunikasikan. Tingkat otorisasi harus ditetapkan dan didokumentasikan. Individu yang mengambil peran Keamanan Informasi tertentu harus kompeten dalam pengetahuan dan keterampilan yang dibutuhkan oleh peran tersebut dan harus didukung untuk mengikuti perkembangan terkait peran tersebut dan

diperlukan untuk memenuhi tanggung jawab peran tersebut.

3. Segregasi Tugas
   a. Pemisahan tugas dan bidang tanggung jawab bertujuan untuk memisahkan tugas-tugas yang saling bertentangan antara individu yang berbeda untuk mencegah satu individu melaksanakan sendiri tugas-tugas yang berpotensi menimbulkan konflik.
   b. BKKBN harus menentukan tugas dan bidang tanggung jawab mana yang perlu dipisahkan.
   c. Perhatian harus diambil ketika menggunakan sistem Kendali akses berbasis peran untuk memastikan bahwa orang tidak diberikan peran yang bertentangan. Peran harus didefinisikan dan disediakan dengan hati-hati untuk meminimalkan masalah akses jika peran dihapus atau ditugaskan kembali.
4. Tanggung Jawab Manajemen
   a. Manajemen harus menunjukkan dukungan terhadap kebijakan Keamanan Informasi, kebijakan khusus, prosedur, dan Kendali Keamanan Informasi.
   b. Tanggung jawab manajemen harus mencakup memastikan bahwa personil:
      1) Diberi pengarahan dengan benar tentang peran dan tanggung jawab Keamanan Informasi mereka sebelum diberi akses ke Informasi BKKBN dan Aset terkait lainnya;
      2) Diberi mandat untuk memenuhi Kebijakan Keamanan Informasi dan Kebijakan khusus topik BKKBN;
      3) Mencapai tingkat *awareness* Keamanan Informasi yang relevan dengan peran dan tanggung jawab mereka dalam BKKBN;
      4) Kepatuhan terhadap syarat dan ketentuan kerja, kontrak atau perjanjian, termasuk Kebijakan Keamanan Informasi BKKBN dan metode kerja yang sesuai;
      5) Terus meningkatkan keterampilan dan kualifikasi Keamanan Informasi yang sesuai melalui pendidikan profesional berkelanjutan;
      6) Jika memungkinkan, disediakan saluran khusus untuk melaporkan pelanggaran Kebijakan Keamanan Informasi, Kebijakan atau prosedur khusus topik untuk Keamanan Informasi (*whistleblowing*). Hal ini memungkinkan pelaporan anonim, atau memiliki ketentuan untuk memastikan bahwa pengetahuan tentang identitas pelapor hanya diketahui oleh mereka yang perlu menangani laporan tersebut; dan
      7) Disediakan sumber daya dan waktu yang memadai untuk menerapkan Proses dan Kendali terkait keamanan BKKBN.
5. Kontak dengan Otoritas
   a. BKKBN harus membangun dan memelihara kontak dengan pihak berwenang terkait untuk memastikan aliran Informasi yang tepat sehubungan dengan Keamanan Informasi.
   b. Untuk menerapkan Kebijakan terkait Kontak dengan Pihak Berwenang, maka BKKBN harus:
      1) Menentukan kapan dan oleh siapa otoritas (misalnya penegak hukum, badan pengawas, otoritas pengawas) harus dihubungi dan bagaimana Insiden Keamanan Informasi yang teridentifikasi harus dilaporkan secara

tepat waktu;

2) Kontak dengan pihak berwenang juga harus digunakan untuk memfasilitasi pemahaman tentang ekspektasi saat ini dan yang akan datang dari pihak berwenang tersebut (misalnya peraturan Keamanan Informasi yang berlaku); dan
3) Menyusun daftar kontak pihak berwenang, dan secara berkala diperbaharui sesuai dengan kondisi terbaru dari kontak pihak berwenang.

6. Kontak dengan Kelompok Kepentingan Khusus
   a. BKKBN harus menjalin dan memelihara kontak dengan kelompok minat khusus atau forum keamanan khusus lainnya dan asosiasi profesional untuk memastikan Informasi yang tepat terjadi sehubungan dengan Keamanan Informasi.
   b. Untuk menerapkan Kebijakan terkait Kontak dengan Kelompok Khusus, maka BKKBN harus:
      1) Menyusun dan memperbaharui daftar kontak dengan kelompok khusus. Pembaharuan dilakukan minimal satu tahun sekali atau jika ada perubahan; dan
      2) Kelompok khusus tersebut terkait dengan peningkatan pengetahuan, keterampilan maupun isu terkini Keamanan Informasi.
7. Intelijen Ancaman
   a. Informasi yang berkaitan dengan Ancaman Keamanan Informasi harus dikumpulkan dan dianalisis untuk menghasilkan intelijen terhadap Ancaman sehingga tindakan mitigasi yang tepat dapat diambil.
   b. Informasi tentang Ancaman dikumpulkan dan dianalisis untuk:
      1) Memfasilitasi tindakan untuk mencegah Ancaman yang menyebabkan kerugian bagi BKKBN; dan
      2) Mengurangi dampak Ancaman tersebut.
   c. Intelijen Ancaman dapat dibagi menjadi tiga lapisan, yang semuanya harus dipertimbangkan:
      1) Intelijen Ancaman strategis: pertukaran Informasi tingkat tinggi tentang lanskap Ancaman yang berubah (misalnya jenis penyerang atau jenis Serangan);
      2) Intelijen Ancaman taktis: Informasi tentang metodologi, alat, dan teknologi penyerang yang terlibat; dan
      3) Intelijen Ancaman operasional: perincian tentang Serangan spesifik, termasuk indikator teknis.
   d. Intelijen terhadap Ancaman harus:
      1) Relevan (yaitu terkait dengan perlindungan BKKBN);
      2) Berwawasan luas (yaitu memberikan BKKBN pemahaman yang akurat dan terperinci tentang lanskap Ancaman);
      3) Kontekstual, untuk memberikan *awareness* situasional (yaitu menambahkan konteks pada Informasi berdasarkan waktu peristiwa, di mana peristiwa itu terjadi, pengalaman sebelumnya dan prevalensi di BKKBN serupa); dan
      4) Dapat ditindaklanjuti (yaitu BKKBN dapat bertindak berdasarkan Informasi dengan cepat dan efektif).

e. Kegiatan Intelijen terhadap Ancaman harus mencakup:
   1) Penetapan tujuan untuk intelijen Ancaman;
   2) Identifikasi, pemeriksaan dan pemilihan sumber Informasi internal dan eksternal yang diperlukan;
   3) Pengumpulan Informasi dari sumber yang dipilih, baik internal maupun eksternal;
   4) Pemrosesan Informasi yang dikumpulkan (misalnya dengan menerjemahkan, memformat, atau menguatkan Informasi);
   5) Analisis Informasi untuk memahami bagaimana hal itu berhubungan dan berarti bagi BKKBN; dan
   6) Komunikasi kepada individu yang relevan dalam format yang dapat dipahami.

f. Intelijen terhadap Ancaman harus dianalisis dan kemudian digunakan:
   1) Untuk memasukkan Informasi yang dikumpulkan dari sumber intelijen Ancaman ke dalam Proses Manajemen Risiko Keamanan Informasi BKKBN;
   2) Sebagai masukan tambahan untuk Kendali pencegahan dan deteksi teknis seperti *firewall*, sistem deteksi intrusi, atau solusi anti *malware*; dan
   3) Sebagai masukan untuk proses dan teknik pengujian Keamanan Informasi.

g. BKKBN harus berbagi Intelijen terhadap Ancaman dengan organisasi lain secara bersama untuk meningkatkan Intelijen Ancaman secara keseluruhan.

8. Keamanan Informasi dalam Manajemen Proyek
   a. Keamanan Informasi harus diintegrasikan ke dalam manajemen proyek untuk memastikan Risiko Keamanan Informasi yang terkait dengan proyek dan hasil kerja ditangani secara efektif dalam manajemen proyek sepanjang siklus hidup proyek.
   b. Keamanan Informasi harus diintegrasikan ke dalam manajemen proyek untuk memastikan Risiko Keamanan Informasi ditangani sebagai bagian dari manajemen proyek. Ini dapat diterapkan untuk semua jenis.
   c. Manajemen proyek yang digunakan harus mensyaratkan bahwa:
      1) Risiko Keamanan Informasi dinilai dan ditangani pada tahap awal dan secara berkala sebagai bagian dari Risiko proyek sepanjang siklus hidup proyek;
      2) Persyaratan Keamanan Informasi (misalnya seperti persyaratan Keamanan aplikasi, persyaratan untuk mematuhi hak kekayaan intelektual dan sebagainya) dibahas pada tahap awal proyek;
      3) Risiko Keamanan Informasi yang terkait dengan pelaksanaan proyek, seperti keamanan aspek komunikasi internal dan eksternal dipertimbangkan dan ditangani selama siklus hidup proyek; dan
      4) Kemajuan perlakuan Risiko Keamanan Informasi ditinjau dan efektivitas perlakuan dievaluasi serta diuji.
   d. Kesesuaian pertimbangan dan kegiatan Keamanan Informasi harus ditindaklanjuti pada tahap yang telah ditentukan oleh

orang atau badan tata kelola yang sesuai, seperti komite pengarah proyek.

e. Tanggung jawab dan wewenang untuk Keamanan Informasi yang relevan dengan proyek harus didefinisikan dan dialokasikan untuk peran tertentu.

f. Persyaratan Keamanan Informasi untuk produk atau layanan yang akan disampaikan oleh proyek harus ditentukan dengan menggunakan berbagai metode, termasuk persyaratan kepatuhan yang diturunkan dari Kebijakan Keamanan Informasi, Kebijakan dan peraturan topik khusus. Persyaratan Keamanan Informasi lebih lanjut dapat diperoleh dari aktivitas seperti pemodelan Ancaman, tinjauan insiden, penggunaan ambang Kerentanan atau perencanaan darurat, sehingga memastikan bahwa arsitektur dan desain Sistem Informasi terlindungi dari Ancaman yang diketahui berdasarkan lingkungan operasional.

g. Persyaratan Keamanan Informasi harus ditentukan untuk semua jenis proyek, tidak hanya proyek pengembangan TI.

9. Inventori Informasi dan Aset Terkait Lainnya

a. Inventarisasi Informasi dan Aset terkait lainnya, termasuk pemilik, harus disusun dan dipelihara untuk mengidentifikasi Informasi BKKBN dan Aset terkait lainnya dalam rangka menjaga Keamanan Informasi dan menetapkan kepemilikan yang sesuai.

b. BKKBN harus mengidentifikasi Informasi dan Aset terkait lainnya dan menentukan kepentingannya dalam hal Keamanan Informasi. Dokumentasi harus dipelihara dalam inventaris khusus.

c. Inventarisasi Informasi dan Aset terkait lainnya harus akurat, terkini, konsisten, dan selaras dengan inventaris lainnya. Keakuratan inventaris Informasi dan Aset terkait lainnya dilakukan melalui:

1) Tinjauan rutin atas Informasi yang teridentifikasi dan Aset terkait lainnya terhadap inventaris Aset; dan

2) Pembaruan inventaris secara otomatis dalam Proses pemasangan, perubahan, atau penghapusan Aset.

d. Lokasi Aset harus dimasukkan dalam inventaris sebagaimana mestinya.

e. Setiap Aset harus diklasifikasikan sesuai dengan klasifikasi Informasi yang terkait dengan Aset tersebut.

f. Setiap Aset harus dilakukan pemeliharaan secara berkala dan melindungi dari gangguan, Ancaman atau bencana serta melakukan penghapusan/pemusnahan Aset jika sudah tidak digunakan/rusak berat/*expired* (kadaluarsa).

10. Penggunaan yang Akseptabel dari Informasi dan Aset Terkait Lainnya

a. Aturan penggunaan Informasi dan Aset terkait lainnya harus diidentifikasi, didokumentasikan, dan diimplementasikan untuk memastikan Informasi dan Aset terkait lainnya dilindungi, digunakan, dan ditangani dengan tepat.

b. Untuk menerapkan Kebijakan terkait Penerimaan Penggunaan Informasi dan Aset, maka BKKBN harus:

1) Memastikan pegawai dan Mitra Kerja yang mengakses Informasi maupun Aset terkait, memahami persyaratan Keamanan Informasi pada Informasi dan Aset tersebut; dan
2) Pegawai dan Mitra Kerja bertanggung jawab terhadap Informasi maupun Aset terkait yang digunakan; dan
3) Penggunaan Aset Informasi diluar area kantor BKKBN harus memperoleh ijin dari pejabat yang berwenang.

11. Pengembalian Aset
    a. Personil dan pihak berkepentingan lainnya harus mengembalikan semua Aset BKKBN yang mereka gunakan setelah perubahan atau pemutusan hubungan kerja, kontrak, atau perjanjian.
    b. Untuk menerapkan Kebijakan Pengembalian Aset, maka:
        1) Seluruh pegawai yang berhenti maupun mutasi harus mengembalikan Aset milik BKKBN melalui prosedur yang berlaku; dan
        2) Seluruh pegawai yang berhenti maupun mutasi yang menggunakan Aset pribadi dalam bekerja maka dipastikan Informasi dalam Aset tersebut harus dihapus secara aman.
12. Klasifikasi Informasi
    a. Informasi diklasifikasikan menurut kebutuhan Keamanan Informasi BKKBN berdasarkan kerahasiaan, keutuhan, ketersediaan, dan persyaratan pihak berkepentingan yang relevan.
    b. Seluruh Aset Informasi BKKBN dinilai dan diklasifikasikan sesuai dengan konten Aset tersebut.
    c. Kriteria utama dalam klasifikasi yaitu ketentuan hukum, nilai Informasi terhadap BKKBN, kritikalitas Informasi, dan sensitivitas terhadap modifikasi dan kebocoran Informasi.
    d. Terdapat empat tingkat klasifikasi Informasi, yaitu Informasi publik (*public*/*unclassified*), Informasi terbatas (*protected*), Informasi rahasia (*restricted*), dan Informasi sangat rahasia (*classified*).
    e. Lingkup Informasi dalam setiap kategori klasifikasi Informasi ditetapkan dalam Surat Keputusan Pimpinan terpisah.
    f. Pengklasifikasian ulang secara berkala dibutuhkan, mengingat sensitivitas Aset bisa berubah dari waktu ke waktu.
    g. BKKBN harus menetapkan Kebijakan khusus topik tentang klasifikasi Informasi dan mengkomunikasikannya kepada semua pihak terkait yang berkepentingan.
13. Pelabelan Informasi
    a. Prosedur pelabelan Informasi harus dikembangkan dan diterapkan sesuai dengan skema klasifikasi Informasi yang diadopsi oleh BKKBN.
    b. Prosedur pelabelan Informasi harus mencakup Informasi dan Aset terkait lainnya dalam semua format. Label harus mudah dikenali. Prosedur harus memberikan panduan tentang di mana dan bagaimana label dilampirkan dengan mempertimbangkan bagaimana Informasi diakses atau Aset ditangani tergantung pada jenis media penyimpanan.
    c. Informasi digital harus menggunakan metadata untuk mengidentifikasi, mengelola dan mengontrol Informasi, terutama yang berkaitan dengan Kerahasiaan. Metadata juga

harus memungkinkan pencarian Informasi yang efisien dan benar. Metadata harus memfasilitasi sistem untuk berinteraksi dan mengambil keputusan berdasarkan yang terkait label klasifikasi.

d. Prosedur harus menjelaskan cara melampirkan metadata ke Informasi, label apa yang digunakan dan bagaimana data harus ditangani, sejalan dengan model Informasi BKKBN dan arsitektur TIK.

e. Personil dan pihak berkepentingan lainnya harus diberi tahu tentang prosedur pelabelan. Semua personil harus diberi pelatihan yang diperlukan untuk memastikan bahwa Informasi diberi label dengan benar dan ditangani dengan tepat.

f. Keluaran dari sistem yang berisi Informasi yang diklasifikasikan sebagai sensitif atau kritis harus memiliki label klasifikasi yang sesuai.

14. Transfer Informasi

a. Prosedur, atau perjanjian transfer Informasi berlaku untuk semua jenis fasilitas transfer dalam BKKBN dan antara BKKBN dengan pihak lain untuk menjaga Keamanan Informasi.

b. Terkait Transfer Informasi, BKKBN menetapkan:

1) Informasi yang dipertukarkan dengan pihak luar harus diproteksi sesuai dengan klasifikasi Informasi;

2) Pertukaran Informasi dengan pihak luar diharuskan membuat perjanjian pertukaran Informasi sesuai dengan Risiko Informasi yang dipertukarkan;

3) Dalam transfer Informasi secara elektronik ke pihak luar, BKKBN menerapkan:

a) Perlindungan terhadap *malware*;

b) Persetujuan atas Informasi yang dipertukarkan;

c) Pelarangan *automatic forwarder*; dan

d) Pelarangan transfer Informasi Sensitif menggunakan layanan *instant messaging*.

4) Dalam transfer Informasi secara fisik ke pihak luar, BKKBN menerapkan:

a) Penanggung jawab dalam pengendalian, transmisi dan penerimaan Informasi fisik;

b) Pengecekan alamat penerima;

c) Perlindungan kemasan untuk menjaga infomasi rusak atau terbuka ke pihak yang tidak berwenang sesuai dengab klasifikasi Informasi;

d) Daftar kurir terpercaya; dan

e) Pembuatan *logs* untuk Informasi yang dipertukarkan.

5) Dalam transfer Informasi verbal ke pihak luar, BKKBN menerapkan:

a) Pelarangan penyampaian Informasi Sensitif secara verbal di tempat umum;

b) Seleksi penerima Informasi Sensitif yang disampaikan secara verbal; dan

c) Kendali ruangan agar Informasi Sensitif tidak terdengar di luar ruangan.

15. Kontrol Akses
    a. Seperangkat kaidah atau nilai yang dipatuhi untuk mengontrol akses fisik dan logis ke Informasi dan Aset terkait lainnya harus ditetapkan dan diterapkan berdasarkan kebutuhan bisnis dan Keamanan Informasi untuk memastikan akses yang sah dan untuk mencegah akses yang tidak sah ke Informasi dan Aset terkait lainnya.
    b. Untuk menerapkan Kebijakan terkait Kendali Akses, maka BKKBN menetapkan:
        1) Pemilik Informasi dan Aset terkait menentukan persyaratan akses Informasi yang menjadi tanggung jawabnya;
        2) BKKBN menerapkan matriks akses yang digunakan sebagai acuan dalam pengaturan hak akses. Akses tersebut dilakukan oleh orang maupun sistem;
        3) BKKBN memastikan konsistensi matriks akses dengan klasifikasi Informasi BKKBN;
        4) BKKBN memberikan akses kepada Entitas sesuai dengan kebutuhan untuk mendukung pekerjaan (*need-to-know*); dan
        5) Pemberian akses melalui prosedur yang ditetapkan dan pihak yang sudah ditetapkan oleh BKKBN.
16. Manajemen Identitas
    a. Siklus hidup identitas dikelola dengan melakukan identifikasi unik individu dan sistem yang mengakses Informasi BKKBN dan Aset terkait lainnya dan untuk memungkinkan pemberian hak akses yang sesuai.
    b. Manajemen identitas memastikan bahwa:
        1) Identitas yang diberikan kepada orang, identitas hanya terkait dengan satu orang sehingga dapat meminta pertanggungjawaban orang tersebut atas tindakan yang dilakukan;
        2) Tidak memberikan akses pribadi ke orang lain;
        3) Identitas yang diberikan kepada beberapa orang (misalnya identitas bersama) hanya diizinkan jika diperlukan untuk alasan bisnis atau operasional dan tunduk pada persetujuan khusus;
        4) Identitas yang ditetapkan untuk Entitas non-manusia tunduk pada persetujuan dan pengawasan independen yang berkelanjutan;
        5) Identitas dinonaktifkan atau dihapus tepat waktu jika tidak lagi diperlukan; dan
        6) Rekaman semua peristiwa penting terkait penggunaan dan pengelolaan identitas Pengguna harus disimpan.
    c. BKKBN memiliki Proses pendukung untuk menangani perubahan Informasi yang terkait dengan identitas pengguna. Proses ini dapat mencakup verifikasi ulang dokumen yang terkait identitas seseorang.
    d. Saat menggunakan identitas yang diberikan atau dikeluarkan oleh Mitra Kerja (misalnya kredensial media sosial), BKKBN harus memastikan bahwa identitas Mitra Kerja memberikan tingkat kepercayaan yang diperlukan dan setiap Risiko ditangani secara memadai. Ini dapat mencakup Kendali yang terkait dengan Mitra Kerja serta Kendali yang terkait dengan Informasi Autentikasi terkait.

17. Informasi Autentikasi
    a. Pengelolaan Informasi otentikasi dikendalikan oleh Proses manajemen, termasuk menyampaikan kepada personil untuk memperlakukan penanganan Informasi otentikasi dengan benar.
    b. Proses alokasi dan manajemen Informasi otentikasi memastikan bahwa:
        1) Kata sandi pribadi atau nomor identifikasi pribadi (PIN) dihasilkan secara otomatis selama Proses pendaftaran karena Informasi Autentikasi bersifat rahasia dan Pengguna harus mengubahnya setelah penggunaan pertama;
        2) Prosedur verifikasi identitas Pengguna sebelum memberikan Informasi otentikasi baru, pengganti, atau sementara;
        3) Informasi Autentikasi, termasuk Informasi Autentikasi sementara, dikirimkan kepada Pengguna dengan cara yang aman;
        4) Informasi Autentikasi *default* harus diubah setelah pemasangan sistem atau perangkat lunak; dan
        5) Catatan peristiwa penting mengenai alokasi dan pengelolaan Informasi otentikasi disimpan dan dipastikan Kerahasiaannya.
    c. Setiap orang yang memiliki akses atau menggunakan Informasi otentikasi memastikan bahwa:
        1) Informasi otentikasi rahasia seperti kata sandi dijaga Kerahasiaannya. Informasi otentikasi rahasia pribadi tidak boleh dibagikan kepada siapa pun.
        2) Informasi otentikasi yang sudah tidak aman, diubah segera setelah pemberitahuan atau indikasi lain.
            a) Kualitas kata sandi diterapkan di semua jaringan dan sistem dengan menggunakan parameter berikut:
                (1) Panjang Minimum 8 (delapan) karakter;
                (2) Panjang Maximum 16 (enam belas) karakter;
                (3) Karakter yang diisi:
                    (a) Sekurang - kurangnya satu huruf kapital;
                    (b) Setidaknya satu simbol; dan
                    (c) Setidaknya satu nomor.
                (4) Kata sandi baru tidak dapat memiliki lebih dari tiga karakter dalam posisi yang sama seperti password lama;
                (5) Kata sandi tidak dapat berisi nama Pengguna atau Informasi terkait dengan pengguna;
                (6) Perubahan dilakukan setidaknya 90 (sembilan puluh) hari sekali;
                (7) Pemblokiran setelah 5 (lima) kali kesalahan percobaan; dan
                (8) Akun hanya bisa diaktifkan kembali oleh *IT Service Desk*.
            b) Kata sandi yang sama tidak digunakan di seluruh layanan dan sistem yang berbeda.
        3) Ketika kata sandi digunakan sebagai Informasi Autentikasi, sistem manajemen kata sandi harus:
            a) Mengizinkan Pengguna untuk memilih dan mengubah kata sandi mereka sendiri dan

menyertakan prosedur konfirmasi untuk mengatasi kesalahan input;

b) Memberlakukan kata sandi yang kuat sesuai dengan rekomendasi praktik baik;

c) Memaksa Pengguna untuk mengubah kata sandi mereka saat pertama kali masuk;

d) Menerapkan perubahan kata sandi seperlunya, misalnya setelah insiden keamanan, atau setelah pemutusan hubungan kerja atau perubahan pekerjaan;

e) Mencegah penggunaan kembali kata sandi sebelumnya minimal 5 (lima) kali ganti kata sanadi sebelum ke kata sandi lama;

f) Mencegah penggunaan kata sandi yang umum digunakan dan nama Pengguna yang disusupi, kombinasi kata sandi dari sistem yang diretas;

g) Tidak menampilkan kata sandi di layar saat dimasukkan; dan

h) Menyimpan dan mengirimkan kata sandi dalam bentuk yang dilindungi.

4) Enkripsi kata sandi dan *hashing* harus dilakukan sesuai dengan teknik kriptografi yang disetujui untuk kata sandi.

18. Hak Akses

a. Hak akses ke Informasi dan Aset terkait lainnya harus disediakan, ditinjau, dimodifikasi, dan dihapus sesuai dengan kebijakan. Aturan Kendali akses digunakan untuk memastikan akses ke Informasi dan Aset terkait lainnya sesuai dengan persyaratan bisnis.

b. Dalam menerapkan kebijakan Hak Akses, BKKBN menetapkan:

1) Pemberian maupun pencabutan akses pada Informasi fisik maupun elektronik melalui persetujuan pihak yang berwenang;

2) Kewenangan persetujuan hak akses dipisah dari kewenangan implementasi hak akses;

3) Pencabutan maupun perubahan hak akses secara tepat waktu untuk personil yang berhenti atau mutasi;

4) Pencabutan hak akses untuk Pengguna sementara sesuai dengan *expiration date*;

5) BKKBN memelihara catatan perubahan akses fisik maupun elektronik pengguna; dan

6) Reviu hak akses fisik maupun elektronik secara reguler maupun insidental ketika terdapat perubahan personil di BKKBN.

19. Keamanan Informasi dalam Hubungan Mitra Kerja

a. Prosedur pengelolaan Risiko Keamanan Informasi yang terkait dengan penggunaan produk atau layanan Mitra Kerja ditujukan untuk menjaga tingkat Keamanan Informasi yang disepakati dalam hubungan dengan Mitra Kerja.

b. Dalam menerapkan Keamanan Informasi dalam hubungan dengan Mitra Kerja, BKKBN melakukan:

1) Identifikasi tipe Mitra Kerja yang berpotensi mempengaruhi kerahasiaan, keutuhan, dan ketersediaan Informasi BKKBN;

2) Penyusunan Proses evaluasi dan pemilihan Mitra Kerja

sesuai dengan sensitivitas Informasi produk atau layanan;
3) Evaluasi dan pemilihan produk atau layanan yang memenuhi Kendali keamanan yang dibutuhkan;
4) Penentuan Informasi, layanan TI, infrastruktur fisik yang bisa diakses Mitra Kerja;
5) Identifikasi layanan TI yang diberikan Mitra Kerja dan berpengaruh terhadap Keamanan Informasi BKKBN;
6) *Assessment* Mitra Kerja maupun produk/layanan yang diberikan Mitra Kerja termasuk Kerentanannya;
7) Monitoring kepatuhan persyaratan Keamanan Informasi Mitra Kerja dan mitigasi ketidakpatuhan;
8) Penanganan insiden dan kontingensi terkait produk/layanan Mitra Kerja dan tanggung jawab masing-masing;
9) *Awareness* dan training personil Mitra Kerja yang mengakses Informasi maupun layanan BKKBN;
10) Pengelolaan transfer Informasi ataupun Aset terkait lainnya dengan Mitra Kerja yang perlu dijaga Kerahasiaan Informasinya; dan
11) Pengelolaan terminasi Mitra Kerja.

20. Manangani Keamanan Informasi dalam Perjanjian Mitra Kerja
    a. Perjanjian disepakati dengan Mitra Kerja untuk memastikan pemahaman kesepemahaman terkait dengan kepatuhan terhadap persyaratan Keamanan Informasi.
    b. Dalam melakukan perjanjian dengan Mitra Kerja Keamanan Informasi, BKKBN mempertimbangkan beberapa klausul berikut:
        1) Deskripsi Informasi yang diakses Mitra Kerja dan metode aksesnya;
        2) Klasifikasi Informasi berdasarkan klasifikasi Informasi BKKBN;
        3) Pemetaan klasifikasi Informasi BKKBN dengan Mitra Kerja;
        4) Persyaratan hukum, legal maupun kontraktual yang harus dipatuhi;
        5) Kepatuhan semua pihak terhadap Kendali Keamanan Informasi relevan;
        6) Otorisasi penggunaan Informasi atau Aset terkait oleh personil Mitra Kerja;
        7) Persyaratan Keamanan Informasi terhadap layanan TIK yang diberikan oleh Mitra Kerja;
        8) Ganti rugi atau remediasi atas kegagalan Mitra Kerja;
        9) Persyaratan dan prosedur manajemen insiden;
        10) Persyaratan *awareness* dan *training*;
        11) Ketentuan mengenai subkontrak;
        12) Persyaratan skrining personil Mitra Kerja;
        13) Bukti maupun mekanisme *assurance* Mitra Kerja atas efektivitas Kendali Keamanan Informasi; dan
        14) Hak audit Mitra Kerja atas Proses atau Kendali tertentu yang relevan.

21. Memanajemeni Keamanan Informasi dalam Rantai Pasokan TIK
    a. Proses BKKBN diterapkan untuk mengelola Risiko Keamanan Informasi terkait dengan rantai pasok produk dan layanan TI.
    b. Dalam menerapkan Kebijakan Keamanan Informasi rantai

pasok TI, maka BKKBN:

1) Menetapkan persyaratan keamanan pada pengadaan produk atau layanan TI;
2) Memastikan Mitra Kerja mempersyaratkan Keamanan Informasi pada rantai pasoknya;
3) Memastikan Mitra Kerja memberikan Informasi fitur keamanan pada produknya; dan
4) Melakukan validasi produk dan layanan TI telah memenuhi persyaratan Keamanan Informasi.

22. Pemonitoran, Reviu, dan Manajemen Perubahan Layanan Mitra Kerja
    a. BKKBN secara teratur memantau, meninjau, mengevaluasi, dan mengelola perubahan pemberian layanan maupun praktik Keamanan Informasi Mitra Kerja.
    b. Pemantauan, peninjauan, dan manajemen perubahan layanan Mitra Kerja meliputi:
        1) Pemantauan tingkat layanan yang sesuai dengan perjanjian;
        2) Pemantauan perubahan yang dilakukan Mitra Kerja;
        3) Reviu laporan layanan Mitra Kerja;
        4) Audit Mitra Kerja; dan
        5) Reviu *security event/incident*.
    c. Tanggung jawab untuk mengelola hubungan Mitra Kerja harus diberikan kepada individu atau tim yang ditunjuk. Keterampilan teknis dan sumber daya yang memadai harus tersedia untuk memantau bahwa persyaratan perjanjian, khususnya persyaratan Keamanan Informasi, dipenuhi.
    d. Tindakan yang tepat harus diambil ketika terjadi kekurangan dalam penyampaian layanan.
23. Keamanan Informasi untuk Penggunaan Layanan *Cloud*
    a. Proses untuk akuisisi, penggunaan, pengelolaan, dan keluar dari layanan *cloud* harus ditetapkan sesuai dengan persyaratan Keamanan Informasi BKKBN.
    b. BKKBN mendefinisikan dan mengkomunikasikan cara mengelola Risiko Keamanan Informasi yang terkait dengan penggunaan layanan *cloud*.
    c. Penggunaan layanan *cloud* dapat melibatkan tanggung jawab bersama dalam Keamanan Informasi antara penyedia layanan *cloud* dan BKKBN yang bertindak sebagai pelanggan.
    d. Perjanjian layanan *cloud* harus membahas persyaratan kerahasiaan, keutuhan, ketersediaan, dan penanganan Informasi BKKBN.
    e. BKKBN melakukan penilaian Risiko untuk mengidentifikasi Risiko yang terkait dengan penggunaan layanan *cloud*.
    f. Tanggung jawab untuk peran Keamanan Informasi bersama dalam penggunaan layanan cloud harus dialokasikan kepada pihak-pihak yang teridentifikasi, didokumentasikan, dikomunikasikan, dan diimplementasikan oleh pelanggan layanan *cloud* dan penyedia layanan *cloud* untuk memperjelas hubungan mengenai peran dan tanggung jawab bersama antara pelanggan layanan *cloud* dan penyedia layanan *cloud* untuk manajemen Keamanan Informasi.
    g. Pelanggan layanan *cloud* harus menetapkan atau memperluas Kebijakan dan prosedur yang ada sesuai dengan penggunaan layanan *cloud*, dan membuat Pengguna layanan *cloud*

menyadari peran dan tanggung jawab mereka dalam penggunaan layanan *cloud*.

h. Penyedia layanan *cloud* harus mendokumentasikan dan mengkomunikasikan kemampuan, peran, dan tanggung jawab Keamanan Informasinya untuk penggunaan layanan *cloud*nya, bersama dengan peran dan tanggung jawab Keamanan Informasi yang perlu diimplementasikan dan dikelola oleh pelanggan layanan cloud sebagai bagian dari penggunaannya dari layanan *cloud*.

i. Aset pelanggan layanan *cloud* yang berada di tempat penyedia layanan *cloud* harus dihapus, dan dikembalikan jika perlu, pada waktu yang tepat setelah pengakhiran perjanjian layanan *cloud* untuk memastikan Aset pelanggan *cloud* bila terjadi perubahan Aset *cloud* harus segera dihapus bila terjadi pengakhiran perjanjian layanan *cloud*.

j. Pelanggan layanan *cloud* harus meminta deskripsi terdokumentasi tentang penghentian Proses layanan yang mencakup pengembalian dan penghapusan Aset pelanggan layanan *cloud* diikuti dengan penghapusan semua salinan Aset tersebut dari sistem penyedia layanan *cloud*.

k. Deskripsi harus mencantumkan semua Aset dan mendokumentasikan jadwal penghentian layanan, yang harus terjadi tepat waktu.

l. Penyedia layanan *cloud* harus memberikan Informasi tentang pengaturan pengembalian dan penghapusan Aset pelanggan layanan cloud mana pun setelah penghentian perjanjian untuk penggunaan layanan *cloud*.

m. Pengaturan pengembalian dan pemindahan Aset harus didokumentasikan dalam perjanjian dan harus dilakukan tepat waktu. Pengaturan harus menentukan Aset yang akan dikembalikan dan dihapus.

n. Memastikan lingkungan virtual pelanggan layanan *cloud* yang berjalan pada layanan *cloud* harus dilindungi dari pelanggan layanan *cloud* lain dan orang yang tidak berwenang untuk mengurangi Risiko Keamanan Informasi saat menggunakan lingkungan virtual bersama komputasi awan.

o. Penyedia layanan *cloud* harus menerapkan pemisahan logis yang sesuai dari data pelanggan layanan *cloud*, aplikasi virtual, sistem operasi, penyimpanan, dan jaringan untuk:
   1) Pemisahan sumber daya yang digunakan oleh pelanggan layanan *cloud* di lingkungan multi-penyewa; dan
   2) Pemisahan administrasi internal penyedia layanan *cloud* dari sumber daya yang digunakan oleh pelanggan layanan *cloud*.

p. Jika layanan *cloud* melibatkan *multi-tenancy*, penyedia layanan *cloud* harus menerapkan Kendali Keamanan Informasi untuk memastikan isolasi yang tepat dari sumber daya yang digunakan oleh tenant yang berbeda.

q. Penyedia layanan *cloud* harus mempertimbangkan Risiko yang terkait dengan menjalankan perangkat lunak yang disediakan pelanggan layanan *cloud* dalam layanan *cloud* yang ditawarkan oleh penyedia layanan cloud.

r. Mesin virtual dalam lingkungan *cloud* harus diperkuat untuk memenuhi kebutuhan bisnis untuk memastikan mesin virtual aman digunakan untuk kebutuhan bisnis.

s. Saat mengonfigurasi mesin virtual untuk *cloud*, pelanggan

layanan *cloud* dan penyedia layanan *cloud* harus memastikan bahwa aspek-aspek yang sesuai telah diperkuat (misalnya, hanya port, protokol, dan layanan yang diperlukan).

t. Bahwa langkah-langkah teknis yang sesuai sudah tersedia (mis., anti-*malware*, *logging*) untuk setiap mesin virtual yang digunakan.

u. Prosedur untuk operasi administratif lingkungan *cloud* harus ditetapkan, didokumentasikan, dan dipantau untuk memastikan prosedur operasi administratif tersedia.

v. Pelanggan layanan *cloud* harus mendokumentasikan prosedur untuk operasi kritis di mana kegagalan dapat menyebabkan kerusakan Aset yang tidak dapat dipulihkan di lingkungan komputasi *cloud*.

w. Dokumen tersebut harus menentukan bahwa supervisor harus memantau operasi ini.

x. Pelanggan layanan *cloud* harus memiliki kemampuan untuk memantau aspek tertentu dari pengoperasian layanan *cloud* yang digunakan oleh pelanggan layanan *cloud* untuk memastikan adanya pemantauan layanan *cloud* yang digunakan.

y. Pelanggan layanan *cloud* harus meminta Informasi dari penyedia layanan *cloud* tentang kemampuan pemantauan layanan yang tersedia untuk setiap layanan *cloud*.

z. Penyedia layanan *cloud* harus menyediakan kemampuan yang memungkinkan pelanggan layanan *cloud* untuk memantau aspek-aspek tertentu, yang relevan dengan pelanggan layanan *cloud*, dari pengoperasian layanan *cloud*. Kendali akses yang tepat harus mengamankan penggunaan kemampuan pemantauan. Kemampuan tersebut harus menyediakan akses hanya ke Informasi tentang instans layanan *cloud* milik pelanggan layanan *cloud* itu sendiri.

aa. Penyedia layanan *cloud* harus memberikan dokumentasi kemampuan pemantauan layanan kepada pelanggan layanan *cloud*.

bb. Pemantauan harus menyediakan data yang konsisten dengan log peristiwa dan membantu persyaratan SLA.

cc. Konfigurasi jaringan virtual, konsistensi konfigurasi antara jaringan virtual dan fisik harus diverifikasi berdasarkan Kebijakan keamanan jaringan penyedia layanan *cloud* untuk memastikan adanya Pedoman konfigurasi *cloud* tersedia dan telah diverifikasi.

dd. Penyedia layanan *cloud* harus menetapkan dan mendokumentasikan Kebijakan Keamanan Informasi untuk konfigurasi jaringan virtual yang konsisten dengan Kebijakan Keamanan Informasi untuk jaringan fisik.

ee. Penyedia layanan *cloud* harus memastikan bahwa konfigurasi jaringan virtual sesuai dengan Kebijakan Keamanan Informasi terlepas dari sarana yang digunakan untuk membuat konfigurasi.

24. Perencanaan dan Persiapan Manajemen Insiden Keamanan Informasi

a. BKKBN merencanakan dan mempersiapkan pengelolaan Insiden Keamanan Informasi dengan mendefinisikan, menetapkan, dan mengkomunikasikan proses, peran, dan tanggung jawab Manajemen Insiden Keamanan Informasi.

b. Dalam menerapkan Kebijakan terkait Perencanaan dan

Persiapan Manajemen Insiden Keamanan Informasi, maka BKKBN menetapkan:

1) Pengelolaan Insiden Keamanan Informasi diatur dalam prosedur manajemen insiden;
2) Fungsi *service desk* bertanggung jawab mengelola insiden termasuk Insiden Keamanan Informasi. Semua Insiden Keamanan Informasi dilaporkan melalui *service desk*;
3) BKKBN menetapkan prioritas penanganan insiden termasuk *resolution time* untuk setiap kategori Insiden Keamanan Informasi;
4) BKKBN menyediakan formulir pelaporan Insiden Keamanan Informasi untuk memastikan Informasi insiden lengkap;
5) BKKBN melakukan monitoring, deteksi, klasifikasi, analisis, dan pelaporan insiden kemananan Informasi;
6) BKKBN menyediakan mekanisme eskalasi insiden yang memungkinkan aktivasi *Business Continuity Plan*;
7) Fungsi *service desk* melakukan pencatatan aktivitas manajemen insiden;
8) Fungsi *service desk* memberikan *feedback* kepada pelapor Insiden Keamanan Informasi setelah insiden ditindaklanjuti dan ditutup.

25. Asesmen dan Keputusan tentang Peristiwa Keamanan Informasi
    a. BKKBN menilai Peristiwa Keamanan Informasi dan memutuskan apakah peristiwa itu akan dikategorikan sebagai Insiden Keamanan Informasi.
    b. Dalam menerapkan Kebijakan terkait Penilaian dan Keputusan tentang Peristiwa Keamanan Informasi, maka BKKBN menetapkan:
        1) Fungsi *Service Desk* yang melakukan kategorisasi dan klasifikasi *security event*;
        2) Kategori *security event* berdasarkan Ancaman Keamanan Informasi;
        3) Klasifikasi *security event* berdasarkan dampak dan urgensi *security event* tersebut;
        4) Dampak *security event* dibagi menjadi:
            a) Tinggi yaitu gangguan dengan akibat atau cakupan luas, seperti:
                (1) Gangguan terhadap kegiatan BKKBN secara luas; dan
                (2) Gangguan yang terkait dengan layanan/aplikasi yang berdasarkan BIA tergolong sebagai layanan/aplikasi kritis.
            b) Sedang yaitu gangguan dengan akibat atau cakupan sedang, seperti:
                (1) Gangguan terhadap kegiatan satu atau beberapa Direktorat/Biro; dan
                (2) Gangguan yang terkait dengan layanan/aplikasi yang berdasar BIA tergolong sebagai layanan/aplikasi sedang.
            c) Rendah yaitu gangguan dengan akibat atau cakupan rendah, seperti:
                (1) Gangguan terhadap personil tetapi tidak sampai satu Direktorat/Biro; dan
                (2) Gangguan yang terkait dengan layanan/aplikasi yang berdasar BIA tergolong

sebagai layanan atau aplikasi rendah.

5) Urgensi *security event* dibagi menjadi:
   a) Tinggi: Pengguna atau Kelompok Pengguna tidak dapat melaksanakan kegiatannya atau dampak akan semakin luas jika gangguan tidak diselesaikan dalam waktu sesegera mungkin dikarenakan berakibat pada berhentinya Proses bisnis.
   b) Sedang: Pengguna atau Kelompok Pengguna tidak dapat melaksanakan kegiatannya atau dampak akan semakin luas jika gangguan tidak diselesaikan dalam waktu 5 (lima) hari kerja.
   c) Rendah: Pengguna atau Kelompok Pengguna tidak masalah apabila gangguan tidak dapat diselesaikan lebih dari 5 (lima) hari kerja.
6) Fungsi *Service Desk* melakukan klasifikasi *event*. *Security event* diklasifikasikan sebagai insiden apabila masuk dalam klasifikasi *minor event* atau *major event*;
7) *Major event* untuk *event* prioritas kritikal sedangkan *minor event* prioritas non kritikal; dan
8) Hasil klasifikasi *event* dicatat untuk menjadi referensi dan bahan verifikasi *event* berikutnya.

26. Respons terhadap Insiden Keamanan Informasi
    a. Insiden Keamanan Informasi ditanggapi sesuai dengan prosedur yang berlaku.
    b. BKKBN menetapkan dan mengkomunikasikan prosedur Insiden Keamanan Informasi kepada semua pihak berkepentingan.
    c. Insiden Keamanan Informasi dikelola oleh tim resmi dengan kompetensi yang sesuai ketentuan peraturan perundang-undangan.
27. Belajar dari Insiden Keamanan Informasi
    a. Pengetahuan yang diperoleh dari Insiden Keamanan Informasi digunakan untuk memperkuat dan meningkatkan Kendali Keamanan Informasi.
    b. BKKBN menetapkan prosedur untuk memantau jenis, volume Insiden Keamanan Informasi.
    c. Informasi yang diperoleh dari evaluasi Insiden Keamanan Informasi digunakan untuk:
       1) Meningkatkan rencana pengelolaan insiden termasuk skenario dan prosedur insiden;
       2) Mengidentifikasi insiden yang berulang dan penyebabnya; dan
       3) Meningkatkan *awareness* Pengguna dengan memberikan contoh tentang apa yang dapat terjadi, bagaimana menanggapi insiden tersebut dan bagaimana menghindarinya.
28. Pengumpulan Bukti
    a. BKKBN menetapkan dan menerapkan prosedur untuk identifikasi, pengumpulan, perolehan, dan penyimpanan bukti yang terkait dengan Peristiwa Keamanan Informasi.
    b. Prosedur tersebut untuk mengelola bukti yang berkaitan dengan Peristiwa Keamanan Informasi untuk tujuan tindakan pendisiplinan maupun tindakan hukum.
    c. Secara umum, prosedur pengelolaan barang bukti memuat identifikasi, pengumpulan, perolehan dan penyimpanan

barang bukti. Bukti dikumpulkan dengan cara yang dapat diterima oleh pengadilan.

29. Keamanan Informasi Selama Disrupsi
    a. BKKBN merencanakan untuk menjaga Keamanan Informasi selama gangguan.
    b. Dalam menerapkan Kebijakan Keamanan Informasi Selama Gangguan, maka BKKBN menetapkan:
        1) Persyaratan Keamanan Informasi yang menjadi bagian Proses *Business Continuity Management*;
        2) Rencana pemulihan Keamanan Informasi pada Proses bisnis kritikal sesuai dengan persyaratan waktu yang disepakati;
        3) Implementasi Kendali Keamanan Informasi dalam DRP*;*
        4) Penjagaan Kendali Keamanan infomasi selama gangguan; dan
        5) C*ompensating control* untuk Kendali keamanan yang tidak bisa diterapkan saat gangguan.
30. Kesiapan TIK untuk Kontinuitas Bisnis
    a. Kesiapan TIK untuk kontinuitas bisnis harus direncanakan, diterapkan, dipelihara dan diuji untuk memastikan Ketersediaan Informasi BKKBN dan Aset terkait lainnya selama gangguan.
    b. Kesiapan TIK untuk kontinuitas bisnis merupakan komponen penting dalam manajemen kelangsungan bisnis dan manajemen Keamanan Informasi untuk memastikan bahwa tujuan BKKBN dapat terus terpenuhi selama gangguan.
    c. Persyaratan kontinuitas TI merupakan hasil dari BIA. Proses BIA menggunakan kriteria dampak untuk menilai dampak gangguan aktivitas bisnis. Besaran dan durasi dampak digunakan untuk mengidentifikasi kegiatan prioritas yang ditetapkan dalam RTO.
    d. BIA yang melibatkan layanan TI dapat diperluas untuk menentukan persyaratan RPO.
    e. Berdasarkan keluaran BIA dan penilaian Risiko yang melibatkan layanan TI, BKKBN mengidentifikasi dan memilih strategi kontinuitas TI.
    f. Strategi kontinuitas bisnis dapat terdiri dari satu atau lebih solusi. Berdasarkan strategi tersebut, rencana kontinuitas dikembangkan, diterapkan, dan diuji untuk memenuhi tingkat Ketersediaan layanan TI.
31. Persyaratan Legal, Statutori, Regulatori, dan Kontraktual
    a. Persyaratan hukum, undang-undang, peraturan, dan kontrak yang relevan dengan Keamanan Informasi dan pendekatan BKKBN untuk memenuhi persyaratan tersebut harus diidentifikasi, didokumentasikan, dan diperbarui.
    b. Untuk menerapkan Kebijakan terkait persyaratan hukum, undang-undang, peraturan, dan kontrak, maka BKKBN memastikan:
        1) Persyaratan hukum, regulasi, kontrak dijadikan pertimbangan dalam penyusunan Kebijakan, prosedur, Kendali keamanan, klasifikasi Informasi, *risk assessment*, *job description*, kontrak Mitra Kerja;
        2) BKKBN mengidentifikasi, mereviu regulasi yang relevan untuk Keamanan Informasi.
        3) BKKBN mematuhi regulasi, peraturan hukum mengenai

kriptografi; dan

4) BKKBN memasukan persyaratan Keamanan Informasi dalam kontrak dengan klien, Mitra Kerja, dan asuransi.

32. Hak Kekayaan Intelektual

a. BKKBN menerapkan prosedur untuk melindungi hak kekayaan intelektual.

b. Untuk melindungi materi apa pun yang dapat dianggap kekayaan intelektual, dapat dipertimbangkan:

1) Mendefinisikan dan mengkomunikasikan Kebijakan khusus mengenai perlindungan hak kekayaan intelektual;

2) Menerbitkan prosedur untuk kepatuhan hak kekayaan intelektual pada penggunaan perangkat lunak dan produk Informasi;

3) Memperoleh perangkat lunak hanya melalui sumber yang dikenal dan bereputasi baik, untuk memastikan tidak ada pelanggaran hak cipta;

4) Memelihara daftar Aset untuk melindungi hak kekayaan intelektual;

5) Memelihara bukti dan bukti kepemilikan lisensi;

6) Memastikan jumlah maksimum Pengguna atau sumber daya (misalnya unit pemrosesan pusat (*central processing unit*/CPU)) yang diizinkan dalam lisensi;

7) Melakukan tinjauan untuk memastikan perangkat lunak resmi dan produk berlisensi yang dipasang;

8) Menyediakan prosedur untuk mempertahankan kondisi lisensi yang sesuai;

9) Menyediakan prosedur untuk membuang atau mentransfer perangkat lunak kepada orang lain;

10) Mematuhi syarat dan ketentuan untuk perangkat lunak dan Informasi yang diperoleh dari jaringan publik dan sumber luar;

11) Tidak menggandakan, mengonversi ke format lain atau mengekstrak dari Rekaman komersial (video, audio) selain yang diizinkan oleh undang-undang hak cipta atau lisensi yang berlaku; dan

12) Tidak menyalin, secara penuh atau sebagian, standar (misalnya Standar Internasional ISO/IEC), buku, artikel, laporan atau dokumen lain, selain yang diizinkan oleh undang-undang hak cipta atau lisensi yang berlaku.

33. Proteksi Rekaman

a. Rekaman harus dilindungi dari kehilangan, perusakan, pemalsuan, akses tidak sah, dan pelepasan tanpa izin untuk memastikan kepatuhan dengan persyaratan hukum, undang-undang, peraturan dan kontrak, serta harapan masyarakat atau masyarakat terkait dengan untuk perlindungan dan Ketersediaan arsip.

b. Untuk menerapkan Kebijakan terkait Perlindungan Rekaman, maka BKKBN harus menetapkan:

1) Melindungi otentikasi, reliabilitas, integrasi, dan kegunaan Rekaman. Rekaman bisa berupa Rekaman fisik maupun elektronik;

2) Perlindungan Rekaman dengan mengatur retensi, *Disposal*, dan melarang manipulasi Rekaman;

3) Ketentuan retensi Rekaman mengikuti ketentuan retensi

dokumen di BKKBN; dan

4) Pengelola Rekaman membuat metadata Rekaman yang memuat Konteks, konten dan struktur Rekaman.

34. Privasi dan Proteksi PII

a. BKKBN harus mengidentifikasi dan memenuhi persyaratan mengenai privasi dan perlindungan PII sesuai dengan undang-undang dan peraturan yang berlaku serta persyaratan kontrak untuk memastikan kepatuhan terhadap persyaratan hukum, undang-undang, peraturan dan kontrak yang terkait dengan aspek Keamanan Informasi perlindungan PII.

b. BKKBN harus menetapkan dan mengkomunikasikan Kebijakan khusus topik tentang privasi dan perlindungan PII kepada semua pihak terkait yang berkepentingan.

c. BKKBN harus mengembangkan dan menerapkan prosedur untuk menjaga privasi dan perlindungan PII. Prosedur ini harus dikomunikasikan kepada semua pihak terkait yang berkepentingan yang terlibat dalam pemrosesan Informasi identitas pribadi.

d. Kepatuhan terhadap prosedur ini dan semua undang-undang dan peraturan yang relevan mengenai pelestarian privasi dan perlindungan PII memerlukan peran, tanggung jawab, dan Kendali yang sesuai. Seringkali hal ini paling baik dicapai dengan penunjukan orang yang bertanggung jawab, seperti petugas privasi, yang harus memberikan panduan kepada personil, penyedia layanan, dan pihak berkepentingan lainnya tentang tanggung jawab masing-masing dan prosedur khusus yang harus diikuti.

e. Tanggung jawab untuk menangani PII harus ditangani dengan mempertimbangkan undang-undang dan peraturan yang relevan.

f. Langkah-langkah teknis dan organisasi yang tepat untuk melindungi PII harus dilaksanakan.

35. Pelindungan Data Pribadi

a. Jenis Data Pribadi

Jenis Data Pribadi yang dikelola oleh BKKBN diklasifikasikan sebagai berikut:

1) Data Pribadi yang bersifat spesifik yang meliputi:
   a) Data dan Informasi kesehatan;
   b) Data biometrik;
   c) Data genetika;
   d) Catatan kejahatan;
   e) Data anak;
   f) Data keuangan pribadi; dan/atau
   g) Data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

2) Data Pribadi yang bersifat umum yang meliputi:
   a) Nama lengkap;
   b) Jenis kelamin;
   c) Kewarganegaraan;
   d) Agama;
   e) Status perkawinan; dan/atau
   f) Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

b. Hak Subjek Data Pribadi

1) Subjek Data Pribadi berhak untuk:

a) Mendapatkan Informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi.
b) Melengkapi, memperbarui atau memperbaiki kesalahan atau ketidakakuratan Data Pribadi tentang dirinya sesuai dengan tujuan pemrosesan Data Pribadi.
c) Mendapatkan akses dan memperoleh salinan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.
d) Mengakhiri pemrosesan, menghapus, dan/atau memusnahkan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.
e) Menarik kembali persetujuan pemrosesan Data Pribadi tentang dirinya yang telah diberikan kepada BKKBN.
f) Mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis, termasuk pemrofilan, yang menimbulkan akibat hukum atau berdampak signifikan pada Subjek Data Pribadi.
g) Menunda atau membatasi pemrosesan Data Pribadi secara proporsional sesuai dengan tujuan pemrosesan Data Pribadi.
h) Menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.
i) Mendapatkan dan/atau menggunakan Data Pribadi tentang dirinya dari BKKBN dalam bentuk yang sesuai dengan struktur dan/atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik.
j) Menggunakan dan mengirimkan Data Pribadi tentang dirinya ke pihak lainnya, sepanjang sistem yang digunakan dapat saling berkomunikasi secara aman sesuai dengan prinsip Pelindungan Data Pribadi.

2) Hak-hak Subjek Data Pribadi sebagaimana dimaksud dikecualikan untuk:
a) Kepentingan pertahanan dan keamanan nasional;
b) Kepentingan Proses penegakan hukum;
c) Kepentingan umum dalam rangka penyelenggaraan negara;
d) Kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara; atau
e) Kepentingan statistik dan penelitian ilmiah;

c. Pemrosesan Data Pribadi
1) Pemrosesan data pribadi antara lain meliputi:
a) Pemerolehan dan pengumpulan;
b) Pengolahan dan analisis;
c) Penyimpanan;
d) Perbaikan dan pembaruan;
e) Penampilan, pengumuman, transfer, penyebarluasan,

atau pengungkapan; dan/atau
f) Penghapusan atau pemusnahan.

2) Pemrosesan Data Pribadi dilakukan sesuai dengan Prinsip Pelindungan Data Pribadi yang meliputi:
a) Pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, dan transparan;
b) Pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya;
c) Pemrosesan Data Pribadi dilakukan dengan menjamin hak Subjek Data Pribadi dengan;
d) Pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan;
e) Pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, penyalahgunaan, perusakan, dan/atau penghilangan Data Pribadi;
f) Pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan Pelindungan Data Pribadi;
g) Data Pribadi dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan Subjek Data Pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan; dan
h) Pemrosesan Data Pribadi dilakukan secara bertanggung jawab dan dapat dibuktikan secara jelas.

3) Dasar Pemrosesan Data Pribadi antara lain meliputi:
a) Persetujuan yang sah secara eksplisit dari Subjek Data Pribadi untuk 1 (satu) atau beberapa tujuan tertentu;
b) Pemenuhan kewajiban perjanjian dalam hal Subjek Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan Subjek Data Pribadi pada saat akan melakukan perjanjian;
c) Pemenuhan kewajiban hukum sesuai dengan ketentuan peraturan perundang-undangan;
d) Pemenuhan perlindungan kepentingan vital Subjek Data Pribadi;
e) Pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan BKKBN berdasarkan peraturan perundang-undangan; dan/atau
f) Pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan BKKBN dan hak Subjek Data Pribadi.

d. Kewajiban BKKBN dalam Pemrosesan Data Pribadi

1) Kewajiban BKKBN dalam pemrosesan data pribadi sebagai berikut:
a) Melakukan pemrosesan Data Pribadi secara terbatas dan spesifik, sah secara hukum, dan transparan;
b) Melakukan pemrosesan Data Pribadi sesuai dengan

tujuan pemrosesan Data Pribadi;

c) Memastikan akurasi, kelengkapan, dan konsistensi Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan;

d) Melakukan verifikasi atas akurasi, kelengkapan, dan konsistensi Data Pribadi;

e) Memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak menerima permintaan pembaruan dan/atau perbaikan Data Pribadi;

f) Memberitahukan hasil pembaruan dan/atau perbaikan Data Pribadi kepada Subjek Data Pribadi;

g) Melakukan perekaman terhadap seluruh kegiatan pemrosesan Data Pribadi;

h) Memberikan akses kepada Subjek Data Pribadi terhadap Data Pribadi yang diproses beserta rekam jejak pemrosesan Data Pribadi sesuai dengan jangka waktu penyimpanan Data Pribadi. Akses yang diberikan pada subjek data pribadi paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak menerima permintaan akses;

i) Menolak memberikan akses perubahan terhadap Data Pribadi kepada Subjek Data Pribadi dalam hal:
   (1) Membahayakan keamanan, kesehatan fisik, atau kesehatan mental Subjek Data Pribadi dan/atau orang lain;
   (2) Berdampak pada pengungkapan Data Pribadi milik orang lain; dan/ atau
   (3) Bertentangan dengan kepentingan pertahanan dan keamanan nasional;

j) Melakukan penilaian dampak Pelindungan Data Pribadi dalam hal pemrosesan Data Pribadi memiliki potensi Risiko tinggi terhadap Subjek Data Pribadi. Pemrosesan Data Pribadi memiliki potensi Risiko tinggi sebagaimana dimaksud antara lain meliputi:
   (1) Pengambilan keputusan secara otomatis yang memiliki akibat hukum atau dampak yang signifikan terhadap Subjek Data Pribadi;
   (2) Pemrosesan atas Data Pribadi yang bersifat spesifik;
   (3) Pemrosesan Data Pribadi dalam skala besar;
   (4) Pemrosesan Data Pribadi untuk kegiatan evaluasi, penskoran, atau pemantauan yang sistematis terhadap Subjek Data Pribadi;
   (5) Pemrosesan Data Pribadi untuk kegiatan pencocokan atau penggabungan sekelompok data;
   (6) Penggunaan teknologi baru dalam pemrosesan Data Pribadi; dan/atau
   (7) Pemrosesan Data Pribadi yang membatasi pelaksanaan hak Subjek Data Pribadi.

k) Melindungi dan memastikan keamanan Data Pribadi yang diprosesnya, dengan melakukan:
   (1) Penyusunan dan penerapan langkah teknis

operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan; dan

(2) Penentuan tingkat keamanan Data Pribadi dengan memperhatikan sifat dan Risiko dari Data Pribadi yang harus dilindungi dalam pemrosesan Data Pribadi.

l) Menjaga Kerahasiaan Data Pribadi.

m) Melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan Data Pribadi.

n) Melindungi Data Pribadi dari pemrosesan yang tidak sah dan mencegah Data Pribadi diakses secara tidak sah dengan menggunakan sistem keamanan terhadap Data Pribadi yang diproses dan/atau memproses Data Pribadi menggunakan sistem elektronik secara andal, aman, dan bertanggung jawab.

o) Menghentikan pemrosesan Data Pribadi dalam hal Subjek Data Pribadi menarik kembali persetujuan pemrosesan Data Pribadi. Menghentikan pemrosesan Data Pribadi dilakukan paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak menerima permintaan penarikan kembali persetujuan pemrosesan Data Pribadi.

p) Melakukan penundaan dan pembatasan pemrosesan Data Pribadi baik sebagian maupun seluruhnya paling lambat 3 x 24 (tiga kali dalam puluh empat) jam terhitung sejak menerima permintaan penundaan dan pembatasan pemrosesan Data Pribadi. Penundaan tersebut diberitahukan kepada Subjek Data Pribadi. Penundaan dan pembatasan pemrosesan Data Pribadi dikecualikan dalam hal:

(1) Terdapat ketentuan peraturan perundang-undangan yang tidak memungkinkan dilakukan penundaan dan pembatasan pemrosesan Data Pribadi;

(2) Dapat membahayakan keselamatan pihak lain; dan

(3) Subjek Data Pribadi terikat perjanjian tertulis dengan pihak tertentu yang tidak memungkinkan dilakukan penundaan dan pembatasan pemrosesan Data Pribadi.

q) Mengakhiri pemrosesan Data Pribadi dalam hal:

(1) Telah mencapai masa retensi;

(2) Tujuan pemrosesan Data Pribadi telah tercapai; dan

(3) Terdapat permintaan dari Subjek Data Pribadi.

r) Menghapus Data Pribadi dalam hal:

(1) Data Pribadi tidak lagi diperlukan untuk pencapaian tujuan pemrosesan Data Pribadi;

(2) Subjek Data Pribadi telah melakukan penarikan kembali persetujuan pemrosesan Data Pribadi;

(3) Terdapat permintaan dari Subjek Data Pribadi; atau

(4) Data Pribadi diperoleh dan/atau diproses

dengan cara melawan hukum.

s) Memusnahkan Data Pribadi dalam hal:
   (1) Telah habis masa retensinya dan berketerangan dimusnahkan berdasarkari jadwal retensi arsip;
   (2) Terdapat permintaan dari Subjek Data Pribadi;
   (3) Tidak berkaitan dengan penyelesaian Proses hukum suatu perkara; dan/atau
   (4) Data Pribadi diperoleh dan/atau diproses dengan cara melawan hukum.

t) Memberitahukan penghapusan dan/atau pemusnahan Data Pribadi kepada Subjek Data Pribadi.

u) Dalam hal terjadi kegagalan Pelindungan Data Pribadi, menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 (tiga kali dua puluh empat) jam kepada:
   (1) Subjek Data Pribadi; dan
   (2) Lembaga terkait.

v) Pemberitahuan tertulis tentang kegagalan Pelindungan Data Pribadi minimal memuat:
   (1) Data Pribadi yang terungkap;
   (2) Kapan dan bagaimana Data Pribadi terungkap; dan
   (3) Upaya penanganan dan pemulihan atas terungkapnya Data Pribadi.

w) Dalam hal tertentu, melakukan pemberitahuan kepada masyarakat mengenai kegagalan Pelindungan Data Pribadi.

x) Kewajiban BKKBN dikecualikan untuk:
   (1) Kepentingan pertahanan dan keamanan nasional;
   (2) Kepentingan Proses penegakan hukum;
   (3) Kepentingan umum dalam rangka penyelenggaraan negara; atau
   (4) Kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara.

e. Transfer Data Pribadi
   1) Transfer Data Pribadi Dalam Wilayah Hukum Negara Republik Indonesia
      a) BKKBN dapat melakukan transfer Data Pribadi kepada pihak lainnya dalam wilayah hukum Negara Republik Indonesia;
      b) BKKBN melakukan Pelindungan Data Pribadi dalam melakukan transfer tersebut;
   2) Transfer Data Pribadi ke Luar Wilayah Hukum Negara Republik Indonesia
      a) BKKBN dapat melakukan transfer Data Pribadi kepada pihak lain di luar wilayah hukum Negara Republik Indonesia sesuai dengan ketentuan yang diatur dalam peraturan perundang-undangan;
      b) Dalam melakukan transfer Data Pribadi sebagaimana dimaksud, BKKBN memastikan negara tempat kedudukan pihak yang menerima transfer Data Pribadi memiliki tingkat Pelindungan Data

Pribadi yang setara atau lebih tinggi dari yang diatur dalam peraturan perundang-undangan;

c) Jika penerima transfer Data Pribadi tidak memiliki tingkat Pelindungan Data Pribadi yang setara atau lebih tinggi, maka BKKBN wajib memastikan terdapat Pelindungan Data Pribadi yang memadai dan bersifat mengikat; dan

d) Pada saat melakukan transfer Data Pribadi ke Luar Wilayah Hukum Negara Republik Indonesia Organisasi Pribadi wajib mendapatkan persetujuan Subjek Data Pribadi.

36. Reviu Independen terhadap Keamanan Informasi

a. Pendekatan BKKBN untuk mengelola Keamanan Informasi dan implementasinya termasuk orang, proses, dan teknologi harus ditinjau secara independen pada interval yang direncanakan, atau ketika terjadi perubahan signifikan untuk memastikan kesesuaian, kecukupan, dan efektivitas pendekatan BKKBN untuk mengelola Keamanan Informasi secara berkelanjutan.

b. Untuk menerapkan Kebijakan terkait Tinjauan Independen terhadap Keamanan Informasi, maka BKKBN harus menetapkan:

1) Reviu independen Keamanan Informasi dilakukan minimal satu tahun sekali. Reviu dilakukan terhadap Kebijakan dan Kendali Keamanan Informasi lainnya;

2) Reviu dilakukan oleh pihak independen yang bukan pelaksana tugas maupun penanggung jawab pekerjaan. Reviu bisa dilakukan oleh fungsi internal audit, *independent manager*, maupun Mitra Kerja;

3) Personil yang melakukan reviu harus memiliki kompetensi yang memadai dalam melakukan asesmen;

4) Hasil reviu dilaporkan ke Pimpinan. Apabila terdapat ketidaksesuaian maka dilakukan *corrective action*;

5) Selain reviu reguler, reviu dilakukan apabila terdapat perubahan regulasi, terdapat insiden besar, perubahan bisnis, perubahan produk/layanan dan perubahan Kendali Keamanan Informasi.

37. Kepatuhan terhadap Kebijakan, Aturan, dan Standar Keamanan Informasi

a. Kepatuhan terhadap Kebijakan Keamanan Informasi BKKBN, Kebijakan topik khusus, aturan dan standar harus ditinjau secara berkala untuk memastikan bahwa Keamanan Informasi diterapkan dan dioperasikan sesuai dengan Kebijakan Keamanan Informasi BKKBN, Kebijakan, aturan, dan standar topik tertentu.

b. Pemilik layanan, produk, atau Informasi harus mengidentifikasi cara meninjau bahwa persyaratan Keamanan Informasi yang ditentukan dalam Kebijakan Keamanan Informasi, Kebijakan topik khusus, aturan, standar, dan peraturan lain yang berlaku terpenuhi. Alat pengukuran dan pelaporan otomatis harus dipertimbangkan untuk tinjauan rutin yang efisien.

c. Jika ditemukan ketidakpatuhan sebagai hasil dari tinjauan, manajer harus:

1) Mengidentifikasi penyebab ketidakpatuhan;

2) Mengevaluasi perlunya tindakan korektif untuk mencapai kepatuhan;
3) Menerapkan tindakan korektif yang sesuai; dan
4) Meninjau tindakan korektif yang diambil untuk memverifikasi keefektifannya dan mengidentifikasi setiap kekurangan atau kelemahan.

d. Hasil tinjauan dan tindakan korektif yang dilakukan oleh manajer, pemilik layanan, produk atau Informasi harus dicatat dan catatan ini harus dipelihara. Manajer harus melaporkan hasilnya kepada orang yang melakukan tinjauan independen ketika tinjauan independen dilakukan di area tanggung jawab mereka.

e. Tindakan korektif harus diselesaikan tepat waktu sesuai dengan Risikonya. Jika tidak diselesaikan pada tinjauan terjadwal berikutnya, kemajuan setidaknya harus ditangani pada tinjauan itu.

38. Prosedur Operasi Terdokumentasi

a. Prosedur operasi untuk Fasilitas Pemrosesan Informasi hendaklah didokumentasikan dan tersedia bagi personil yang membutuhkannya untuk memastikan pengoperasian Fasilitas Pemrosesan Informasi yang benar dan aman.

b. Untuk menerapkan Kebijakan terkait Dokumen Prosedur Operasi, maka BKKBN harus:

1) Menyusun prosedur operasi yang antara lain meliputi prosedur: 1) instalasi dan konfigurasi, 2) *backup*, 3) *schedulling*, 4) *handling error*, 5) eskalasi dukungan pihak eksternal, 6) *recovery*, 7) manajemen *audit trail*, 8) monitoring kapasitas, kinerja, dan keamanan, 9) pemeliharaan; dan
2) Prosedur direviu dan diupdate sesuai kebutuhan melalui mekanisme persetujuan yang telah ditetapkan.

E. Kendali Orang

1. Skrining

a. Pemeriksaan verifikasi latar belakang terhadap semua calon pegawai harus dilakukan sebelum bergabung dengan BKKBN dengan memperhatikan persyaratan hukum, peraturan, etika yang berlaku, kebutuhan BKKBN, klasifikasi Informasi yang akan diakses, dan Risiko relevan.

b. Proses skrining harus dilakukan untuk semua jenis pegawai termasuk tetap maupun tidak tetap termasuk personil Mitra Kerja, persyaratan skrining disertakan dalam perjanjian kontrak dengan Mitra Kerja.

c. Informasi tentang calon pegawai ditangani dengan mempertimbangkan Peraturan Pelindungan Data Pribadi.

d. Verifikasi calon pegawai mencakup beberapa hal berikut:

1) Ketersediaan referensi yang memadai (misalnya referensi kerja);
2) Kelengkapan dan kebenaran riwayat hidup pelamar;
3) Kualifikasi akademik dan profesional;
4) Identitas (misalnya paspor atau dokumen lain yang dapat diterima); dan
5) Catatan kriminal jika kandidat mengambil peran penting.

e. Ketika seseorang dipekerjakan untuk peran Keamanan Informasi tertentu, BKKBN harus memastikan kandidat tersebut:
   1) Memiliki kompetensi yang diperlukan untuk menjalankan peran keamanan;
   2) Dapat dipercaya untuk mengambil peran tersebut, terutama jika peran tersebut sangat penting bagi BKKBN; dan
   3) Jika suatu pekerjaan melibatkan orang yang memiliki akses ke Fasilitas Pemrosesan Informasi Sensitif maka mempertimbangkan diperlukan verifikasi lebih rinci.

2. Syarat dan Ketentuan Ketenagakerjaan
   a. Perjanjian kontrak kerja harus menyatakan tanggung jawab pegawai dan BKKBN untuk Keamanan Informasi dan sesuai dengan peraturan BKKBN yang berlaku.
   b. Kewajiban kontrak pegawai mempertimbangkan Kebijakan Keamanan Informasi BKKBN. Selain itu, mempertimbangkan hal berikut:
      1) Perjanjian Kerahasiaan Informasi ditandatangani oleh pegawai sebelum diberi akses ke Informasi Sensitif;
      2) Tanggung jawab untuk klasifikasi Informasi dan pengelolaan Informasi sesuai klasifikasi Informasi tersebut;
      3) Tanggung jawab untuk menangani Informasi yang diterima dari pihak yang berkepentingan; dan
      4) Tindakan yang harus dilakukan jika pegawai melanggar persyaratan keamanan BKKBN.
   c. Peran dan tanggung jawab Keamanan Informasi harus dikomunikasikan kepada kandidat selama rekrutmen.
   d. BKKBN harus memastikan bahwa pegawai menyetujui syarat dan ketentuan terkait Keamanan Informasi.

3. *Awareness*, Pendidikan, dan Pelatihan Keamanan Informasi
   a. Pegawai dan pihak terkait BKKBN menerima program *awareness*, pendidikan, dan pelatihan Keamanan Informasi yang sesuai termasuk pembaruan Kebijakan Keamanan Informasi BKKBN.
   b. *Awareness* Keamanan Informasi, program pendidikan, dan pelatihan harus ditetapkan sejalan dengan Kebijakan Keamanan Informasi BKKBN dengan mempertimbangkan Informasi BKKBN yang akan dilindungi dan Kendali Keamanan Informasi yang telah diterapkan.
   c. *Awareness* Keamanan Informasi, pendidikan, dan pelatihan harus dilakukan secara berkala.
   d. Pemahaman personil harus dinilai pada akhir program *awareness*, pendidikan, atau pelatihan untuk menguji efektivitas kegiatan.
   e. *Awareness*
      1) Program *awareness* Keamanan Informasi ditujukan untuk membuat personil sadar akan tanggung jawab mereka terkait Keamanan Informasi dan memahami cara melaksanakan tanggung jawab masing-masing;
      2) Program *awareness* direncanakan dengan mempertimbangkan peran personil dalam BKKBN, termasuk personil internal dan eksternal; dan

3) Kegiatan program *awareness* dilaksanakan rutin dan untuk personil baru serta mempertimbangkan Insiden Keamanan Informasi.

f. Pendidikan dan Pelatihan
   1) BKKBN mengidentifikasi, menyiapkan, dan menerapkan rencana pelatihan untuk tim teknis yang perannya memerlukan keahlian dan keahlian khusus; dan
   2) Program pendidikan dan pelatihan harus mempertimbangkan berbagai bentuk kegiatan dan merotasi anggota staf untuk mengikuti berbagai kegiatan tersebut.

4. Proses Kedisiplinan
   a. Pendisiplinan melalui Proses formal dan Proses tersebut dikomunikasikan ke pihak relevan.
   b. Proses pendisiplinan tidak boleh dimulai tanpa verifikasi bahwa telah terjadi pelanggaran Kebijakan Keamanan Informasi.
   c. Proses pendisiplinan formal memberikan tanggapan secara bertahap dengan mempertimbangkan faktor-faktor seperti:
      1) Sifat (siapa, apa, kapan, bagaimana) dan beratnya pelanggaran dan konsekuensinya;
      2) Apakah tindak pidana itu disengaja (*malicious*) atau tidak disengaja (*accidental*); dan
      3) Apakah ini merupakan pelanggaran pertama atau berulang.
   d. Tanggapan mempertimbangkan persyaratan hukum, undang-undang, peraturan kontrak yang relevan serta faktor-faktor lain yang diperlukan.
   e. Proses pendisiplinan juga harus digunakan untuk mencegah personil dan pihak terkait lainnya yang berkepentingan melanggar Kebijakan Keamanan Informasi.
   f. Pelanggaran Kebijakan Keamanan Informasi yang disengaja maka diperlukan tindakan segera.

5. Tanggung Jawab Setelah Terminasi atau Perubahan Pekerjaan
   a. Tanggung jawab Keamanan Informasi tetap berlaku setelah pemutusan hubungan kerja atau perubahan pekerjaan. Tanggung jawab tersebut dikomunikasikan kepada personil terkait dan pihak berkepentingan.
   b. Proses untuk mengelola pemutusan hubungan kerja atau perubahan pekerjaan mengatur tanggung jawab dan tugas Keamanan Informasi yang tetap berlaku setelah pemutusan atau perubahan tersebut.
   c. Proses pemutusan hubungan kerja atau perubahan pekerjaan juga harus diterapkan pada personil Mitra Kerja ketika terjadi pemutusan hubungan kerja terhadap personil atau ketika ada perubahan pekerjaan di dalam BKKBN.

6. Perjanjian Konfidensialitas atau nirungkap (*non-disclosure*)
   a. Perjanjian konfidensialitas atau *non-disclosure* yang mencerminkan kebutuhan BKKBN untuk perlindungan Informasi harus diidentifikasi, didokumentasikan, ditinjau secara berkala dan ditandatangani oleh personil dan pihak berkepentingan terkait lainnya serta sesuai dengan regulasi BKKBN yang berlaku untuk menjaga Kerahasiaan Informasi yang dapat diakses oleh personil atau pihak eksternal.

b. Perjanjian konfidensialitas atau *non-disclosure* harus membahas persyaratan untuk melindungi Informasi rahasia menggunakan persyaratan yang dapat ditegakkan secara hukum.
c. Dalam perjanjian konfidensialitas atau nirungkap, beberapa hal berikut dipertimbangkan:
   1) Definisi Informasi yang akan dilindungi (misalnya Informasi rahasia);
   2) Jangka waktu yang diharapkan dari suatu perjanjian, termasuk kasus-kasus di mana diperlukan untuk menjaga Kerahasiaan tanpa batas waktu atau sampai Informasi tersebut tersedia untuk umum;
   3) Tindakan yang diperlukan ketika perjanjian diakhiri;
   4) Tanggung jawab untuk menghindari pengungkapan Informasi yang tidak sah; dan
   5) Hak mengaudit dan memantau kegiatan yang melibatkan Informasi rahasia untuk keadaan yang sangat sensitif.
d. BKKBN mempertimbangkan kepatuhan terhadap perjanjian konfidensialitas dan *non-disclosure*;
e. Persyaratan untuk perjanjian Kerahasiaan dan *non-disclosure* ditinjau secara berkala dan bila terjadi perubahan yang memengaruhi persyaratan ini.

7. Telekarya (*Remote working*)
   a. Langkah-langkah keamanan diterapkan ketika personil bekerja jarak jauh dalam rangka melindungi Informasi yang diakses, diproses, atau disimpan di luar lokasi BKKBN dan sesuai dengan regulasi relevan.
   b. BKKBN mengeluarkan Kebijakan khusus topik tentang kerja jarak jauh yang menetapkan ketentuan dan batasan yang relevan.
8. Pelaporan Peristiwa Keamanan Informasi
   a. BKKBN menyediakan mekanisme bagi personil untuk melaporkan kejadian Keamanan Informasi.
   b. Semua personil dan Pengguna diberikan *awareness* akan tanggung jawab mereka dalam melaporkan kejadian Keamanan Informasi secepat mungkin untuk mencegah atau meminimalkan dampak Insiden Keamanan Informasi.
   c. Mekanisme pelaporan mudah diakses. Peristiwa Keamanan Informasi meliputi insiden, pelanggaran, dan Kerentanan.
   d. Personil dan Pengguna disarankan untuk tidak berusaha membuktikan dugaan Kerentanan Keamanan Informasi.

F. Kendali Fisik
1. Perimeter Keamanan Fisik
   a. Perimeter digunakan untuk mencegah akses fisik yang tidak sah, kerusakan, dan gangguan terhadap Informasi dan Aset terkait Informasi.
   b. Menentukan Perimeter keamanan dan kekuatan setiap Perimeter sesuai dengan persyaratan Keamanan Informasi yang sesuai dengan Aset di dalam Perimeter.
   c. Memantau dan menguji pintu pada Perimeter untuk menetapkan tingkat ketahanan yang diperlukan sesuai dengan standar yang sesuai.

2. Entri Fisik
    1) Area aman harus dilindungi oleh Kendali masuk dan titik akses yang sesuai untuk memastikan hanya akses fisik yang berwenang ke Informasi BKKBN dan Aset terkait lainnya yang terjadi.
    2) Membatasi akses ke lokasi dan bangunan hanya untuk personil yang berwenang. Akses ke wilayah fisik dilakukan tinjauan secara berkala.
    3) Menerapkan mekanisme teknis pengelolaan akses ke tempat pemrosesan atau penyimpanan Informasi.
    4) Memeriksa barang-barang personil dan pihak yang berkepentingan pada saat masuk dan keluar area;
    5) Mewajibkan semua personil dan pihak-pihak yang berkepentingan untuk menggunakan identifikasi yang mudah terlihat.
    6) Memberikan akses terbatas kepada personil Mitra Kerja ke area aman atau Fasilitas Pemrosesan Informasi hanya jika diperlukan. Akses ini harus diotorisasi dan dipantau.
    7) Mengamankan titik masuk lainnya seperti pintu keluar darurat dari akses yang tidak sah.
    8) Mengelola kunci untuk memastikan keamanan kunci fisik atau Informasi Autentikasi dan buku log akses.
3. Mengamankan Kantor, Ruangan, dan Fasilitas
    a. Keamanan fisik untuk kantor, ruangan, dan fasilitas harus dirancang dan diterapkan untuk mencegah akses fisik yang tidak sah, kerusakan, dan gangguan terhadap Informasi BKKBN dan Aset terkait lainnya di kantor, ruangan, dan fasilitas.
    b. Menempatkan fasilitas penting untuk menghindari akses publik.
    c. Jika dapat diterapkan, memastikan bangunan tidak mengganggu dan memberikan petunjuk minimum tentang tujuannya, tanpa tanda yang jelas, di luar atau di dalam gedung, yang mengidentifikasi keberadaan aktivitas pemrosesan Informasi.
    d. Mengonfigurasi fasilitas untuk mencegah Informasi atau aktivitas rahasia terlihat dan terdengar dari luar. Perisai elektromagnetik juga harus dianggap sesuai.
    e. Tidak membuat direktori, buku telepon internal dan peta online yang dapat diakses yang mengidentifikasi lokasi Fasilitas Pemrosesan Informasi rahasia tersedia untuk setiap orang yang tidak berwenang.
4. Pemonitoran Keamanan Fisik
    a. Gedung, ruangan maupun fasilitas dipantau untuk mendeteksi dan mencegah akses fisik yang tidak sah.
    b. Area aman terletak di lokasi yang terhindar dari akses atau visibilitas publik, terpisah secara fisik dari tempat umum, dan tidak berbagi dengan Mitra Kerja.
    c. Seluruh *entry point* dinilai Risikonya dan diterapkan Kendali yang memadai.
    d. Terdapat penjaga pada area pintu masuk area aman.
    e. Terdapat pintu darurat yang memenuhi persyaratan.
    f. Terdapat sistem pemantauan CCTV di area-area penting.
    g. Seluruh personil yang masuk direkam identitas dan waktu keluar masuknya.

h. Ruang server memiliki akses Kendali dua faktor, seperti kunci dan nomor pin.
i. Peralatan Rekaman seperti kamera, video, dan semacamnya tidak diizinkan memasuki area aman tanpa izin khusus sebelumnya.
j. Direktori telepon area aman tidak boleh tersedia secara umum.
k. Area aman terjamin kerahasiaan, keutuhan, dan ketersediaan data terhadap Ancaman eksternal seperti banjir, kebakaran, gempa bumi, gangguan listrik, bahan kimia, petir, dan Ancaman lainnya.
l. Keluar masuk material ke area aman diperiksa sebelum material memasuki area aman, dan staf pengiriman tidak memiliki akses memasuki area aman.
m. Perangkat dalam area aman seperti server dan monitor tidak boleh terlihat dari tempat umum atau dari luar area aman (misalnya melalui jendela).
n. Makan, minum, dan merokok tidak diperbolehkan dilakukan di area aman.
o. Fasilitas pendukung seperti AC, listrik, gas, air, ventilasi, dan jaringan komunikasi tersedia dalam area aman, terdapat backup dari fasilitas tersebut, serta terdapat alarm jika fasilitas pendukung mengalami gangguan.

5. Memproteksi dari Ancaman Fisik dan Lingkungan
   a. Perlindungan dirancang dan dilakukan terhadap Ancaman fisik dan lingkungan, seperti bencana alam dan Ancaman fisik yang disengaja atau tidak disengaja lainnya.
   b. Penilaian Risiko untuk mengidentifikasi konsekuensi potensial Ancaman fisik dan lingkungan dilakukan sebelum memulai operasi kritis di lokasi fisik, dan secara berkala.
6. Bekerja di Area Aman
   a. Tindakan keamanan untuk bekerja di area aman diterapkan untuk melindungi Informasi dan Aset terkait lainnya dari kerusakan dan gangguan tidak sah oleh personil yang bekerja di area ini.
   b. Personil mengetahui keberadaan area aman dan aktivitas di dalamnya hanya sesuai dengan kebutuhan masing-masing.
   c. Menghindari kegiatan tanpa pengawasan di area aman untuk mengurangi kemungkinan aktivitas berbahaya.
   d. Mengunci area aman dan secara berkala memeriksa area aman yang kosong.
   e. Tidak mengizinkan peralatan fotografi, video, audio, atau Rekaman lainnya, seperti kamera di Perangkat Titik Akhir Pengguna, kecuali diizinkan.
   f. Mengendalikan penggunaan perangkat Pengguna di area aman.
7. Meja Bersih dan Layar Bersih
   a. Aturan kebersihan meja dari kertas dan media penyimpanan serta aturan kebersihan layar untuk Fasilitas Pemrosesan Informasi dijalankan untuk mengurangi Risiko akses yang tidak sah maupun kehilangan/kerusakan Informasi.
   b. Menyimpan dengan aman dokumen maupun media penyimpanan yang memuat Informasi Sensitif ketika tidak digunakan.

c. Melindungi Perangkat Titik Akhir Pengguna saat tidak digunakan atau tanpa pengawasan, misalnya dengan mengunci layar otomatis.
d. Membuat pemilik dokumen segera mengumpulkan *output* dari printer atau perangkat multifungsi lainnya.
e. Menyimpan dokumen dan media penyimpanan yang berisi Informasi Sensitif dengan aman serta membuangnya dengan mekanisme pembuangan yang aman.
f. Pengguna mematikan pop-up email/*messaging* lainnya selama presentasi, berbagi layar atau di termpat umum.
g. Menghapus Informasi Sensitif atau penting di papan tulis dan jenis tampilan lainnya saat tidak diperlukan lagi.

8. Penempatan dan Proteksi Peralatan
   a. Peralatan ditempatkan dengan aman untuk mengurangi Risiko Ancaman fisik, lingkungan, maupun akses yang tidak sah.
   b. Fasilitas Pemrosesan Informasi yang menangani data sensitif ditempatkan dengan aman sehingga tidak bisa dilihat oleh pihak yang tidak berwenang selama penggunaannya.
   c. Menerapkan Kendali untuk meminimalkan Risiko potensi Ancaman fisik dan lingkungan berupa pencurian, kebakaran, gangguan pasokan listrik ataupun vandalisme.
   d. Menetapkan Pedoman untuk makan, minum, dan merokok di dekat Fasilitas Pemrosesan Informasi.
   e. Memantau kondisi lingkungan, seperti suhu dan kelembapan yang dapat berdampak negatif terhadap pengoperasian Fasilitas Pemrosesan Informasi.
9. Keamanan Aset di luar Premis
   a. Aset di luar lokasi harus dilindungi untuk mencegah dari kehilangan, kerusakan, pencurian maupun akses yang tidak berwenang.
   b. Tidak meninggalkan peralatan dan media penyimpanan di tempat umum tanpa pengawasan.
   c. Melakukan otorisasi pada pemindahan peralatan dan media dari lokasi BKKBN yang disimpan di luar lokasi BKKBN.
   d. Melindungi pihak lain bisa melihat Informasi di perangkat *mobile* Pengguna ketika berada di tempat umum.
   e. Menerapkan pelacakan lokasi perangkat dan aktivasi fitur penghapusan data perangkat dari jarak jauh.
10. Media Penyimpanan
   a. Siklus hidup media penyimpanan yang meliputi pengadaan, penggunaan, pengangkutan, dan pembuangannya kelola sesuai dengan skema klasifikasi dan persyaratan penanganan BKKBN.
   b. Melakukan otorisasi untuk media penyimpanan yang dipindahkan dari BKKBN dan pencatatan atas pemindahan tersebut.
   c. Menyimpan media penyimpanan di tempat yang aman sesuai dengan klasifikasi Informasinya dan melindunginya dari Ancaman lingkungan.
   d. Mempertimbangkan kriptografi untuk melindungi Informasi pada media penyimpanan yang memuat Informasi Sensitif.
   e. Menyimpan beberapa salinan Informasi berharga pada media penyimpanan terpisah untuk mengurangi Risiko kerusakan atau kehilangan Informasi yang tidak disengaja.

11. Utilitas Pendukung
    a. Fasilitas Pemrosesan Informasi dilindungi dari kegagalan termasuk kegagalan utilitas pendukung.
    b. Memastikan peralatan pendukung utilitas dikonfigurasi, dioperasikan dan dipelihara sesuai dengan spesifikasi pabrikan.
    c. Memastikan utilitas pendukung dilakukan pengujian secara rutin.
12. Keamanan Perkabelan
    a. Kabel yang membawa daya, data atau layanan Informasi pendukung dilindungi dari intersepsi, interferensi, atau kerusakan.
    b. Memisahkan kabel listrik dari kabel komunikasi untuk mencegah interferensi.
    c. Untuk sistem yang sensitif atau kritis, pengendalian lebih lanjut yang perlu dipertimbangkan meliputi:
        1) Penggunaan pelindung elektromagnetik untuk melindungi kabel; dan
        2) Pemeriksaan teknis dan fisik berkala untuk mendeteksi perangkat yang tidak sah yang terpasang pada kabel.
    d. Memberi label kabel pada setiap ujung dengan perincian sumber dan tujuan yang memadai untuk identifikasi fisik dan pemeriksaan kabel.
13. Pemeliharaan Peralatan
    1) Peralatan harus dipelihara dengan benar untuk memastikan kerahasiaan, keutuhan, dan ketersediaan Informasi.
    2) Memelihara peralatan sesuai dengan spesifikasi dan frekuensi yang direkomendasikan Mitra Kerja.
    3) Penerapan dan pemantauan program pemeliharaan oleh BKKBN.
    4) Hanya personil pemeliharaan resmi yang melakukan perbaikan dan pemeliharaan peralatan.
    5) Menyimpan catatan pemeliharaan preventif dan korektif.
    6) Menerapkan pengendalian yang tepat dalam pemeliharaan peralatan termasuk pemeliharaan di lokasi atau di luar BKKBN.
    7) Mengawasi personil pemeliharaan saat melakukan pemeliharaan di lokasi.
    8) Mengizinkan dan mengendalikan akses untuk pemeliharaan jarak jauh.
14. Pemusnahan atau Penggunaan Kembali Peralatan dengan Aman
    a. Sebelum dilakukan pemusnahan atau penggunaan kembali, peralatan yang berisi media penyimpanan dilakukan verifikasi untuk memastikan semua data sensitif dan lisensi telah dihapus dengan aman.
    b. Peralatan harus diverifikasi untuk memastikan apakah media penyimpanan masih menyimpan data atau tidak sebelum dibuang atau digunakan kembali.
    c. Media penyimpanan yang berisi Informasi rahasia atau memiliki hak cipta harus dimusnahkan secara fisik atau Informasi dalam media penyimpanan dimusnahkan menggunakan teknik tertentu sehingga Informasi tidak dapat diperoleh kembali.

d. Label yang mengidentifikasi BKKBN atau menunjukkan klasifikasi, pemilik, sistem atau jaringan, harus dihilangkan sebelum dibuang.
e. BKKBN harus mempertimbangkan penghapusan Kendali keamanan seperti Kendali akses atau peralatan pengawasan pada akhir masa sewa atau ketika pindah tempat. Beberapa hal yang bisa dilakukan:
   1) Mengembalikan fasilitas ke kondisi semula;
   2) Meminimalkan Risiko meninggalkan sistem dengan Informasi Sensitif untuk penyewa berikutnya (misalnya daftar akses pengguna, file video atau gambar); dan
   3) Menggunakan kembali Kendali di fasilitas yang lain.

G. Kendali Teknologi
1. Perangkat Titik Akhir Pengguna
   a. Informasi yang disimpan, diproses oleh, atau dapat diakses melalui Perangkat Titik Akhir Pengguna dilindungi dengan Kendali yang sesuai.
   b. Kendali terkait Penggunaan Perangkat Titik Akhir Pengguna, antara lain:
      1) Pengguna tidak boleh menyimpan Informasi Sensitif di perangkat titik akhir, kecuali disimpan menggunakan enkripsi;
      2) Perangkat Titik Akhir Pengguna yang digunakan untuk menjalankan aktivitas bisnis adalah perangkat milik BKKBN yang sudah teregistrasi, atau perangkat milik sendiri atau yang telah mendapatkan persetujuan;
      3) Pengguna perangkat memastikan perangkatnya hanya digunakan oleh dirinya sendiri, dan tidak digunakan oleh orang lain yang tidak berhak;
      4) Instalasi *software* pada Perangkat Titik Akhir Pengguna dilakukan terpusat. Pengguna tidak diperbolehkan menginstal *software* tanpa persetujuan dari Tim *Service Desk* yang berwenang;
      5) Pengguna perangkat memastikan perangkat *mobile* yang berada pada lokasi yang aman;
      6) Pengguna perangkat memastikan fitur keamanan seperti *screen lock*, *password*, dan sebagainya, dalam keadaan aktif;
      7) Pengguna perangkat melakukan *backup* secara berkala pada perangkat *mobile* yang digunakan;
      8) Pengguna perangkat memasang antivirus pada perangkat titik akhir-nya; dan
      9) Apabila terjadi kerusakan atau kehilangan pada perangkat titik akhir, Pengguna melaporkannya pada Tim *Service Desk*.
2. Hak Akses Istimewa (*Privilege*)
   a. Penggunaan hak akses istimewa dibatasi untuk memastikan hanya pengguna/sistem yang berwenang yang diberikan hak akses istimewa.
   b. Kebijakan terkait Hak Akses Istimewa, antara lain:
      1) Fungsi TI mengidentifikasi kebutuhan hak akses istimewa pada setiap sistem atau proses;

2) Hak akses istimewa hanya diberikan kepada personil yang bewenang sesuai dengan tugas pokok dan fungsi masing-masing;
3) Hak akses istimewa hanya diberikan oleh pimpinan fungsi TI dalam jangka waktu yang ditentukan;
4) Hak akses istimewa tidak diperbolehkan menggunakan generik ID;
5) Hak akses istimewa hanya digunakan untuk pekerjaan administrasi/konfigurasi sistem dan tidak diperbolehkan untuk pekerjaan umum sehari-hari Pengguna biasa;
6) Penggunaan hak akses istimewa dilakukan *logging* dan *monitoring*; dan
7) Hak akses istimewa direviu secara berkala minimal setahun sekali dan setiap terjadi perubahan organisasi.

3. Pembatasan Akses Informasi
   a. Akses ke Informasi dan Aset terkait lainnya harus dibatasi sesuai dengan Kebijakan akses untuk mencegah akses tidak sah ke Informasi dan Aset terkait lainnya.
   b. Kebijakan akses BKKBN antara lain:
      1) Pengguna publik atau anonim tidak diperbolehkan mengakses Informasi Sensitif; dan
      2) Setiap sistem, aplikasi maupun layanan diterapkan mekanisme Kendali akses sesuai dengan Kebijakan Kendali akses termasuk matriks akses.
4. Akses ke Kode Sumber (*Source Code*)
   a. Akses ke *source code*, *tools* pengembangan, dan *library* perangkat lunak dikelola dengan tepat untuk mencegah akses tidak sah, menghindari perubahan yang tidak disengaja dan untuk menjaga kekayaan intelektual.
   b. Kebijakan terkait pembatasan akses ke *source code*, sebagai berikut:
      1) *Source code* dan dokumen pengembangan disimpan dalam *repository* yang aman;
      2) Akses terhadap *source code repository* dibatasi untuk pihak yang mempunyai kewenangan;
      3) Pemberian akses terhadap *source code* didasarkan kepada kebutuhan bisnis dan asesmen Risiko;
      4) *Developer* tidak diberikan akses langsung ke *source code repository*, tetapi melalui *developer tools;* dan
      5) *Log* akses terhadap *source code repository* diaktifkan dan dijaga.
5. Autentikasi Aman
   a. Teknologi dan prosedur otentikasi yang aman diterapkan berdasarkan pembatasan akses Informasi untuk memastikan Pengguna atau Entitas diautentikasi dengan aman, ketika mengakses ke sistem, aplikasi, dan layanan diberikan.
   b. Kebijakan terkait Otentikasi Keamanan, sebagai berikut:
      1) Otentikasi sistem, aplikasi atau layanan disesuaikan dengan klasifikasi Informasi pada sistem, aplikasi atau layanan tersebut;
      2) Prosedur *login* mengimplementasikan beberapa hal sebagai berikut:
         a) Tidak menampilkan Informasi Sensitif sebelum *login*;
         b) Menginformasikan peringatan bahwa sistem hanya bisa diakses oleh pihak yang berwenang;

c) Tidak memberikan Informasi bantuan selama *login*;
d) Proteksi terhadap *brute force log-in* dengan *automated public turing test* (CAPTCHA);
e) Tidak menampilkan *password* dalam *clear text* ketika sedang diinput;
f) Tidak mentransmisikan *password* melalui jaringan dalam bentuk *clear text*; dan
g) *Setting* sistem agar ketika *inactive session* dalam periode tertentu.

6. Manajemen Kapasitas
   a. Penggunaan sumber daya harus dipantau dan disesuaikan sesuai dengan kebutuhan kapasitas.
   b. Kebijakan terkait Manajemen Kapasitas, sebagai berikut:
      1) Setiap sistem, fasilitas dan SDM ditentukan kebutuhan kapasitas dengan mempertimbangkan kritikalitas bisnis;
      2) Fungsi TI bertanggung jawab melakukan Proses monitoring dan perencanaan kapasitas yang dilakukan secara berkala;
      3) *System tuning* dan *monitoring* dilaksanakan untuk memastikan efisiensi dan Ketersediaan sistem;
      4) BKKBN melakukan *stress-test* terhadap sistem yang akan diimplementasikan untuk mengukur kecukupan kapasitas dibandingkan dengan kebutuhan;
      5) Fungsi TI melakukan monitoring untuk mendeteksi permasalahan kapasitas;
      6) Proyeksi kapasitas TI mempertimbangkan pengembangan bisnis dan sistem kedepan termasuk tren yang berkembang;
      7) Fungsi TI bertanggung jawab memastikan sistem saat ini masih berada di ambang batas yang telah direncanakan.
7. Proteksi terhadap Perangkat Perusak (*malware*)
   a. Perlindungan terhadap *malware* menggunakan perangkat lunak pendeteksi, perbaikan *malware*, *awareness* Keamanan Informasi, akses sistem yang sesuai, dan Kendali manajemen perubahan dengan mempertimbangkan:
      1) Daftar *software* yang boleh diinstal untuk mencegah *unauthorized software* yang berpotensi menyebarkan *malware*; dan
      2) Pembatasan akses pada *malicious website* yang berpotensi menyebarkan *malware*.
   b. BKKBN melakukan pertahanan terhadap *malware* dengan menerapkan:
      1) *Firewall*;
      2) *Anti-Virus*;
      3) *Penyaring Spam*;
      4) *Instalasi* Perangkat Lunak dan *Scanning*;
      5) *Manajemen* Kerentanan;
      6) *Pelatihan Awareness* Pengguna;
      7) *Monitoring* dan Notifikasi Terhadap Ancaman;
      8) *Peninjauan* Teknis Berkala;
      9) *Manajemen* Insiden *Malware*;
   c. Perangkat lunak *anti-malware* diinstal dan dikonfigurasi pada semua Sistem Informasi dan perangkat yang dimiliki oleh BKKBN.

d. Perangkat lunak *anti-malware* melakukan Proses *scan* otomatis pada semua *attachment* dan menghapus atau melakukan Proses *quarantine* pada *file-file* yang dicurigai.
e. Perangkat lunak *anti-malware* melakukan Proses pemeriksaan pada *web page* untuk mendeteksi adanya kemungkinan *malicious code.*
f. *Firewall* dikonfigurasi untuk melakukan *filter* terhadap hasil *download* perangkat lunak dari Internet.
g. Perangkat lunak dari eksternal diinspeksi dan dilakukan Proses otorisasi oleh Fungsi TI apakah sudah bebas dari virus dan sesuai dengan kebutuhan.

8. Manajemen Kerentanan Teknis
   a. Informasi tentang Kerentanan teknis TI dievaluasi dan dilakukan tindakan yang tepat untuk mencegah eksploitasi Kerentanan.
   b. Kebijakan terkait Otentikasi Keamanan, sebagai berikut:
      1) Asesmen Kerentanan TI minimal satu kali dalam setahun;
      2) Inventarisasi Aset TI sebagai persyaratan awal melakukan asesmen Kerentanan TI;
      3) Penentuan ruang lingkup asesmen Kerentanan pada Aset TI di inventaris Aset TI;
      4) Asesmen Kerentanan dilakukan oleh personil yang kompeten;
      5) Asesmen Kerentanan menggunakan *tool scanning* yang relevan sesuai dengan ruang lingkup Aset;
      6) Kerentanan teknis yang telah diidentifikasi dilakukan asesmen Risiko dan dilakukan tindakan perbaikan yang perlu dilakukan;
      7) Tindakan perbaikan dilakukan berdasarkan prioritas Risiko yang telah dianalisis sebelumnya; dan
      8) Asesmen Kerentanan pada layanan *cloud* dilakukan oleh internal TI, penyedia layanan *cloud* atau Mitra Kerja.

9. Manajemen Konfigurasi
   a. Konfigurasi, termasuk konfigurasi keamanan, perangkat keras, perangkat lunak, layanan, dan jaringan ditetapkan, didokumentasikan, diimplementasikan, dipantau, dan ditinjau untuk memastikan perangkat keras, perangkat lunak, layanan, dan jaringan berfungsi dengan benar dengan pengaturan keamanan yang diperlukan, dan konfigurasi tidak diubah oleh perubahan yang tidak sah atau salah.
   b. Kebijakan terkait Manajemen Konfigurasi, sebagai berikut:
      1) Manajemen konfigurasi dilakukan untuk *hardware, software, service*, jaringan TI;
      2) Pendataan konfigurasi tersebut menggunakan *template* atau tools yang relevan;
      3) Data konfigurasi harus mempertimbangkan keamanan data dan data-data yang tidak diperlukan;
      4) Data konfigurasi meliputi:
         1) Pemilik Aset terkini;
         2) Tanggal terakhir perubahan konfigurasi;
         3) Konfigurasi Aset;
         4) Relasi konfigurasi.
      5) Data konfigurasi disimpan dalam tempat penyimpanan ataupun *repository* yang aman; dan

6) Data konfigurasi dilakukan *monitoring* dan reviu secara berkala.

10. Penghapusan Informasi
    a. Informasi yang disimpan dalam sistem Informasi, perangkat, atau media penyimpanan lainnya dihapus jika tidak diperlukan lagi atau disesuaikan dengan regulasi yang berlaku untuk mencegah penyebaran Informasi Sensitif yang tidak perlu dan untuk mematuhi persyaratan hukum, undang-undang, peraturan, dan kontrak.
    b. Kebijakan terkait Penghapusan Informasi, sebagai berikut:
        1) Informasi Sensitif tidak disimpan lebih lama dari yang diperlukan untuk mengurangi Risiko pembukaan Informasi;
        2) Penghapusan Informasi pada sistem, aplikasi, layanan mempertimbangkan metode penghapusan;
        3) Metode penghapusan mempertimbangkan penghapusan Informasi kadaluarsa, penggunaan *software* terpercaya dan menggunakan mekanisme *Disposal* untuk menghapus Informasi secara permanen;
        4) Perjanjian penggunaan Informasi oleh Mitra Kerja mengharuskan perjanjian penghapusan Informasi setelah selesai perjanjian kerjasama;
        5) Penggunaan layanan *cloud* memasukan perjanjian penghapusan Informasi dengan metode yang disepakati bersama;
        6) Penggunaan perangkat milik Mitra Kerja dipertimbangkan untuk mengambil media penyimpanan Informasi sebelum dikembalikan ke Mitra Kerja;
        7) Permintaan *Disposal* media diajukan pada *IT Service Desk*, disertai dengan pemilik, jenis media, nomor seri, serta klasifikasi Informasi yang ada.
11. Penyamaran (*Masking*) Data
    a. *Data masking* digunakan sesuai dengan Kebijakan BKKBN, persyaratan bisnis, maupun ketentuan peraturan perundang-undangan.
    b. Kebijakan *Data Masking* sebagai berikut:
        1) Dalam rangka melindungi data sensitif, perusahan mempertimbangkan penyembunyian data dengan menggunakan beberapa teknis seperti data *masking*, *pseudonymization* atau *anonymization*;
        2) Teknik *data masking* antara lain melalui enskripsi, penghapusan karakter, variasi nomor-tanggal, substitusi nilai, penggantian nilai dengan *hash*;
        3) *Data masking* mempertimbangan beberapa hal berikut:
            a) Tidak memberikan akses semua Pengguna ke semua data tetapi sesuai seminimal mungkin sesuai kebutuhan pengguna;
            b) Tingkat penyembunyian data tergantung pada tingkat penggunaan data;
            c) Kendali akses data;
            d) Perjanjian atau pembatasan penggunaan data;
            e) Larangan menggabungkan data yang telah disembunyikan dengan data lain; dan
            f) *Tracking* data yang telah disembunyikan.

12. Pencegahan Kebocoran Data
    a. Pencegahan kebocoran data diterapkan untuk mendeteksi dan mencegah pengungkapan dan ekstraksi Informasi yang tidak sah oleh individu atau sistem.
    b. Kebijakan terkait Pencegahan Kebocoran Data sebagai berikut:
        1) Kebocoran data dimitigasi dengan beberapa cara berikut:
            a) BKKBN melakukan identifikasi dan klasifikasi data yang akan dilindungi dari kebocoran;
            b) *Monitoring* jalur kebocoran data; dan
            c) Pencegahan kebocoran data.
        2) *Tools data leakage prevention* digunakan untuk:
            a) Identifikasi dan *monitor* Informasi Sensitif atas Risiko pembukaan;
            b) Deteksi pembukaan Informasi Sensitif; dan
            c) Memblokir tindakan Pengguna atau pengiriman data sensitif.
        3) BKKBN membatasi Pengguna untuk menggandakan, *upload* data keluar organisasi; dan
        4) Apabila diperlukan data keluar dari BKKBN maka harus melalui mekanisme persetujuan.
13. Pencadangan (*backup*) Informasi
    a. Salinan *backup* Informasi, perangkat lunak, dan sistem dipelihara dan diuji secara teratur sesuai dengan Kebijakan BKKBN.
    b. Kebijakan *Backup* Informasi sebagai berikut:
        1) BKKBN memastikan Informasi dan *software* bisa dipulihkan ketika terjadi insiden;
        2) BKKBN menentukan persyaratan *backup* dalam bentuk RPO yang menjadi acuan dalam menentukan frekuensi *backup*;
        3) Fungsi TI melakukan *backup* sesuai dengan frekuensi *backup* yang telah ditentukan;
        4) Tempat penyimpanan *backup* dilakukan di tempat yang aman dan relatif jauh dari lokasi Data Center;
        5) Fungsi TI secara rutin melakukan pengujian *backup* minimal satu tahun sekali melalui *restore* ke sistem *testing* terutama untuk aplikasi *core business*;
        6) Berdasarkan klasifikasi Informasinya, Proses *backup* dapat dilakukan dengan cara:
            a) Untuk Informasi yang mempunyai klasifikasi Informasi sangat rahasia, rahasia, dan terbatas, Proses *backup* data dilakukan *differential backup* setiap satu hari sekali dan *full backup* setiap satu minggu sekali; dan
            b) Untuk Informasi yang mempunyai klasifikasi Informasi publik, maka Proses *backup* data bisa dilakukan *differential backup* setiap satu bulan sekali dan *full backup* setiap tiga bulan sekali.
14. Redudansi Fasilitas Pemrosesan Informasi
    a. Fasilitas Pemrosesan Informasi diimplementasikan dengan redundansi yang memadai untuk memenuhi persyaratan Ketersediaan Informasi.
    b. Kebijakan Redundansi Fasilitas Pemrosesan Informasi sebagai berikut:

1) BKKBN mengidentifikasi persyaratan *availability* layanan TI;
2) Fungsi TI membuat desain dan implementasi arsitektur sistem untuk memenuhi persyaratan *availability* tersebut, salah satunya dengan redundansi;
3) Redundasi berupa duplikasi Fasilitas Pemrosesan Informasi termasuk prosedur aktivasi komponen redundan;
4) Fungsi TI memastikan tingkat keamanan sistem redundan sama dengan sistem utama;
5) Redundansi dilakukan pada beberapa hal berikut:
   a) Kontrak dengan dua atau lebih penyedia jaringan dan Fasilitas Pemrosesan Informasi;
   b) Jaringan redundan;
   c) Data center yang terpisah secara geografis;
   d) *Power supply* redundan;
   e) Paralel *instances* komponen *software* dengan *load balancing* otomatis; dan
   f) Duplikasi komponen jaringan (misal: *firewall,router, switch*).
6) Sistem redundan dilakukan pengujian untuk memastikan kegagalan satu sistem dibackup oleh sistem lainnya.

15. Membuat *Log*
    a. *Log* merekam aktivitas, *exception*, *fault*, dan kejadian relevan lainnya. *Log* tersebut disimpan, dilindungi, dan dianalisis dan dipastikan integrasinya.
    b. Kebijakan *logging* sebagai berikut:
       1) BKKBN menentukan tujuan aktivasi *log*, data yang dikumpulkan, dan persyaratan pengamanan *log*; dan
       2) *Event log* mencatat setiap *event* termasuk:
          a) ID pengguna;
          b) Aktivitas sistem;
          c) Waktu, tanggal, detil *event* relevan;
          d) Identitas perangkat, sistem dan lokasi; dan
          e) Alamat dan protokol jaringan.
       3) *Event* yang harus di-*log* yaitu:
          a) Usaha akses sistem, baik gagal maupun berhasil;
          b) Usaha akses data atau *resource* yang lain, baik gagal maupun berhasil;
          c) Perubahan konfigurasi sistem;
          d) Penggunaan *privileges*;
          e) Penggunaan program utilitas;
          f) File yang diakses dan tipe akses;
          g) Alarm sistem Kendali akses aktif;
          h) Aktivasi dan deaktivasi sistem keamanan;
          i) Pembuatan, modifikasi, dan penghapusan identitas; dan
          j) Transaksi Pengguna di aplikasi.
       4) Pengguna dengan hak akses istimewa dilarang menghapus aktivitasnya dan menonaktifkan *log* aktivitas bersangkutan;
       5) Hal-hal berikut ini adalah perubahan-perubahan yang tidak diizinkan pada fasilitas *logging* dan perlu diberlakukan Kendali:
          a) Perubahan pada tipe pesan yang direkam;
          b) *File log* dilakukan Proses *editing* atau dihapus; dan

c) Kegagalan merekam kejadian atau menimpa Rekaman kejadian sebelumnya.

6) *Log* yang dikirim ke pihak luar harus dilakukan de-identifikasi, misal menggunakan *data masking*;
7) *Event log* bisa memuat data sensitif sehingga diperlukan proteksi privasi;
8) Analisis *log* dilakukan dengan menginterpretasikan kejadian keamanan untuk mengidentifikasi aktivitas yang tidak biasa, perilaku anomali;
9) Analisis log harus didukung kegiatan *monitoring* untuk mengidentifikasi dan menganalisis perilaku anomali.

16. Pemonitoran Aktivitas
    a. Jaringan, sistem dan aplikasi dipantau untuk mengidentifikasi perilaku anomali dan tindakan yang tepat diambil dalam menindaklanjuti potensi Insiden Keamanan Informasi;
    b. Kebijakan monitoring sebagai berikut:
        1) Ruang lingkup dan tingkat *monitoring* ditentukan berdasarkan kebutuhan bisnis dan mempertimbangkan kepatuhan pada regulasi;
        2) Rekaman *monitoring* harus dijaga sesuai dengan ketentuan retensi;
        3) Beberapa yang dipertimbangkan untuk di*monitor* yaitu:
            a) Trafik aplikasi, sistem dan *inbound-outbond network*;
            b) Akses sistem, server, jaringan, sistem *monitoring*, dan aplikasi kritikal;
            c) Admin level sistem dan konfigurasi jaringan;
            d) *Log* dari *security tools*;
            e) *Event log* sistem dan aktivitas jaringan;
            f) Pengecekan keabsahan *code* yang dijalankan di lingkungan produksi; dan
            g) Penggunaan sumber daya dan kinerjanya.
        4) BKKBN menetapkan *baseline* perilaku yang normal dan memantau perubahan anomali *baseline* tersebut;
        5) Perilaku anomali seperti:
            a) Terminasi aplikasi atau Proses yang tidak terencana;
            b) Aktivitas yang berhubungan dengan *malware* atau *malicious IP address*;
            c) Karakteristik Serangan yang sudah diketahui;
            d) Perilaku sistem yang tidak biasa;
            e) *Bottleneck* dan *overload*;
            f) Akses tidak berwenang ke sistem atau Informasi;
            g) *Scanning* tidak berwenang ke aplikasi, sistem atau jaringan;
            h) Usaha akses ke sistem yang diproteksi; dan
            i) Perilaku sistem dan Pengguna yang tidak biasa.
        6) *Software monitoring* dikonfigurasi menghasilkan *alert* berdasarkan *threshold* yang ditentukan;
        7) Fungsi TI menyusun prosedur untuk merespon hasil *monitoring* sehingga bisa mengurangi dampak negatif kejadian keamanan.

17. Sinkronisasi Jam
    a. Jam sistem pemrosesan Informasi yang digunakan oleh BKKBN disinkronkan dengan sumber waktu yang disetujui untuk mendukung analisis kejadian keamanan dan mendukung investigasi Insiden Keamanan Informasi.

b. Kebijakan Sinkronisasi jam sebagai berikut:
   1) Jam semua Sistem Informasi didalam BKKBN disinkronisasi dengan standar yang telah disepakati untuk memastikan akurasi dari *log* audit;
   2) Format tanggal yang digunakan oleh BKKBN adalah dd/mm/yy;
   3) Format waktu yang digunakan oleh BKKBN adalah hh:mm, yang memberlakukan sistem 24 jam;
   4) Jam pada semua server dan perangkat pemrosesan Informasi BKKBN diperiksa secara reguler dan dikoreksi jika dibutuhkan; dan
   5) Jam pada layanan *cloud* harus di*monitor* dan dilakukan mitigasi Risiko apabila terdapat ketidaksesuaian.

18. Penggunaan Program Utilitas *Privilege*
    a. Penggunaan program utilitas yang mampu mengesampingkan Kendali sistem dan aplikasi dikendali dengan ketat untuk memastikan penggunaan program utilitas tidak membahayakan sistem dan aplikasi.
    b. Penggunaan program utilitas yang dapat mengesampingkan Kendali sistem dan aplikasi harus mempertimbangkan:
       1) Pembatasan penggunaan program utilitas hanya untuk Pengguna yang terpercaya dan berwenang;
       2) Penggunaan prosedur identifikasi, otentikasi dan otorisasi untuk program utilitas, termasuk identifikasi unik atas orang yang menggunakan program utilitas;
       3) Mendefinisikan dan mendokumentasikan tingkat otorisasi untuk program utilitas;
       4) Otorisasi untuk penggunaan *ad hoc program* utilitas;
       5) Tidak membuat program utilitas tersedia bagi Pengguna yang memiliki akses ke aplikasi pada sistem yang memerlukan pemisahan tugas;
       6) Menghapus atau menonaktifkan semua program utilitas yang tidak perlu;
       7) Memisahkan program utilitas dari perangkat lunak aplikasi;
       8) Pembatasan Ketersediaan program utilitas (misalnya selama perubahan resmi); dan
       9) Mencatat semua penggunaan program utilitas.

19. Instalasi Perangkat Lunak pada Sistem Operasional
    a. Prosedur diterapkan dalam mengelola instalasi perangkat lunak secara aman pada sistem operasional untuk memastikan integrasi sistem operasional dan mencegah eksploitasi Kerentanan teknis.
    b. Kebijakan perubahan dan pemasangan perangkat lunak dengan aman pada sistem operasional sebagai berikut:
       1) Melakukan pembaruan perangkat lunak operasional hanya oleh administrator terlatih dengan otorisasi manajemen yang sesuai;
       2) Memastikan bahwa hanya kode yang disetujui dan tidak ada kode pengembangan atau kompiler yang diinstal pada sistem operasional;
       3) Hanya menginstal dan memperbarui perangkat lunak setelah pengujian berhasil;
       4) Memperbarui semua *source library* program yang sesuai;

5) Menggunakan sistem Kendali konfigurasi untuk tetap mengontrol semua perangkat lunak operasional serta dokumentasi sistem;
6) Menentukan strategi *rollback* sebelum perubahan diterapkan;
7) Memelihara *log* audit dari semua pembaruan perangkat lunak operasional; dan
8) Pengarsipan perangkat lunak versi lama, bersama dengan semua Informasi dan parameter yang diperlukan, prosedur, detail konfigurasi, dan perangkat lunak pendukung.

c. Setiap keputusan untuk memutakhirkan ke rilis baru harus mempertimbangkan persyaratan bisnis.
d. Perangkat lunak yang mengunakan perangkat lunak dan paket pihak eksternal dipantau dan dikendalikan untuk menghindari perubahan yang tidak sah, karena dapat menimbulkan Kerentanan Keamanan Informasi.
e. Perangkat lunak yang disediakan Mitra Kerja dipelihara sesuai dengan tingkat pemeliharaan yang disepakati. yang didukung oleh Mitra Kerja.
f. Ketika Mitra Kerja terlibat dalam penginstalan atau pemutakhiran perangkat lunak, akses fisik atau logis hanya boleh diberikan jika diperlukan dan dengan otorisasi yang sesuai.
g. BKKBN menetapkan dan menegakkan aturan ketat tentang jenis perangkat lunak yang dapat diinstal oleh pengguna.

20. Keamanan Jaringan
a. Jaringan dan perangkat jaringan harus diamankan, dikelola, dan dikendalikan untuk melindungi Informasi dalam sistem dan aplikasi tehadap kompromi melalui jaringan.
b. Kendali Keamanan Informasi dalam jaringan mempertimbangkan:
1) Jenis dan tingkat klasifikasi Informasi yang dapat didukung jaringan;
2) Menetapkan tanggung jawab dan prosedur untuk pengelolaan peralatan dan perangkat jaringan;
3) Memelihara dokumentasi terkini termasuk diagram jaringan dan file konfigurasi perangkat (mis. *router*, *switch*);
4) Memisahkan tanggung jawab operasional untuk jaringan dari operasi sistem TIK jika perlu;
5) Menetapkan Kendali untuk menjaga kerahasiaan, keutuhan, dan ketersediaan data yang melewati jaringan publik, jaringan Mitra Kerja atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung;
6) Pencatatan dan pemantauan yang dapat melakukan perekaman dan pendeteksian tindakan yang dapat mempengaruhi Keamanan Informasi;
7) Mengoordinasikan pengelolaan jaringan untuk memastikan bahwa Kendali diterapkan secara konsisten di seluruh infrastruktur pemrosesan Informasi;
8) Mengotentikasi sistem pada jaringan;
9) Membatasi dan memfilter koneksi sistem ke jaringan (misalnya menggunakan *firewall*);

10) Mendeteksi, membatasi, dan mengautentikasi sambungan peralatan dan perangkat ke jaringan; dan
11) *Hardening* perangkat jaringan.

c. BKKBN memastikan penerepan Kendali keamanan diterapkan pada penggunaan jaringan *virtual*.

21. Keamanan Layanan Jaringan
    a. Mekanisme keamanan, tingkat layanan, dan persyaratan layanan dari layanan jaringan diidentifikasi, diterapkan, dan dipantau untuk menjamin keamanan dalam penggunaan layanan jaringan.
    b. Kemampuan penyedia layanan jaringan untuk mengelola layanan dengan cara yang aman dipantau secara reguler. Hak untuk mengaudit harus disepakati antara BKKBN dan penyedia.
    c. Aturan penggunaan jaringan dan layanan jaringan harus dirumuskan dan dilaksanakan meliputi:
        1) Jaringan dan layanan jaringan yang boleh diakses;
        2) Persyaratan otentikasi untuk mengakses berbagai layanan jaringan;
        3) Prosedur otorisasi untuk menentukan siapa yang diizinkan mengakses jaringan dan layanan jaringan mana;
        4) Manajemen jaringan dan Kendali teknologi serta prosedur untuk melindungi akses ke koneksi jaringan dan layanan jaringan;
        5) Sarana yang digunakan untuk mengakses jaringan dan layanan jaringan, seperti penggunaan jaringan pribadi *virtual* (*VPN*) atau jaringan nirkabel;
        6) Waktu, lokasi, dan atribut lain dari Pengguna pada saat akses; dan
        7) Pemantauan penggunaan layanan jaringan.
    d. Fitur keamanan layanan jaringan berikut dipertimbangkan:
        1) Teknologi yang diterapkan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi, dan Kendali koneksi jaringan; dan
        2) Parameter teknis yang diperlukan untuk sambungan aman dengan layanan jaringan sesuai dengan aturan keamanan dan sambungan jaringan.

22. Segregasi jaringan
    a. Kelompok layanan Informasi, Pengguna, dan Sistem Informasi dipisahkan melalui segmentasi jaringan untuk membagi jaringan dalam batas keamanan dan mengontrol lalu lintas jaringan sesuai kebutuhan bisnis.
    b. BKKBN mengelola keamanan jaringan dengan membaginya menjadi beberapa domain dan memisahkannya dari jaringan publik (yaitu internet).
    c. Domain dapat dipilih berdasarkan tingkat kepercayaan, kekritisan, dan sensitivitas (misalnya domain akses publik, *domain desktop, domain server*, sistem berisiko rendah dan tinggi), atau berdasarkan unit BKKBN (misalnya sumber daya manusia, keuangan, pemasaran) atau beberapa kombinasi (misalnya *domain server* yang terhubung ke beberapa unit organisasi).
    d. Pemisahan dapat dilakukan dengan menggunakan jaringan yang berbeda secara fisik atau dengan menggunakan jaringan logis.

e. Perimeter setiap domain harus didefinisikan dengan baik. Jika akses antar *domain* jaringan diperbolehkan, itu harus dikendali di Perimeter menggunakan *gateway* (misalnya *firewall, router* penyaringan).

23. Pemfilteran Web
    a. Akses ke situs web eksternal dikelola untuk mengurangi paparan konten berbahaya sehingga bisa melindungi sistem agar tidak disusupi oleh *malware* dan untuk mencegah akses ke sumber daya web yang tidak sah.
    b. BKKBN harus mengurangi Risiko personilnya mengakses situs web yang berisi Informasi ilegal atau diketahui mengandung *virus* atau materi *phishing*, salah satunya dengan memblokir alamat IP atau domain dari situs web yang bersangkutan. atau dapat dikonfigurasi untuk melakukannya.
    c. BKKBN membatasi akses terhadap situs web dan aplikasi berbasis web yang tidak diinginkan atau tidak pantas. Aturan selalu diperbarui.
    d. *Awareness* diberikan kepada personil tentang penggunaan sumber daya *online* yang aman termasuk akses ke web.
24. Penggunaan Kriptografi
    a. Aturan untuk penggunaan kriptografi diterapkan untuk memastikan penggunaan kriptografi yang tepat dan efektif dalam melindungi kerahasiaan, keaslian, atau integrasi Informasi sesuai dengan persyaratan bisnis, hukum, undang-undang, peraturan, dan kontrak yang terkait dengan kriptografi.
    b. Saat menggunakan kriptografi, hal-hal berikut harus dipertimbangkan:
        1) Mengidentifikasi tingkat perlindungan yang diperlukan sesuai klasifikasi Informasi termasuk menetapkan jenis, kekuatan dan kualitas algoritma kriptografi yang diperlukan;
        2) Penggunaan kriptografi untuk perlindungan Informasi yang disimpan pada perangkat Pengguna atau media penyimpanan dan perangkat yang dikirimkan melalui jaringan; dan
        3) Standar kriptografi seperti algoritma kriptografi, kekuatan sandi, solusi kriptografi.
    c. Isi perjanjian atau kontrak dengan Mitra Kerja eksternal layanan kriptografi (misalnya dengan otoritas sertifikasi) mencakup keandalan layanan, dan waktu respons penyediaan layanan.
    d. Manajemen kunci
        1) Manajemen kunci yang tepat meliputi pembuatan, penyimpanan, pengarsipan, distribusik, penghentian dan penghancuran kunci kriptografi; dan
        2) Semua kunci kriptografi harus dilindungi dari modifikasi dan kehilangan. Selain itu, kunci rahasia dan pribadi memerlukan perlindungan terhadap penggunaan yang tidak sah serta pengungkapan. Peralatan yang digunakan untuk menghasilkan, menyimpan, dan mengarsipkan kunci harus dilindungi secara fisik.
25. Siklus Hidup Pengembangan yang Aman
    a. Aturan pengembangan perangkat lunak dan sistem yang aman diterapkan untuk memastikan Keamanan Informasi dirancang

dan diimplementasikan dalam siklus hidup pengembangan tersebut.

b. Pengembangan yang aman adalah persyaratan untuk membangun layanan, arsitektur, perangkat lunak, dan sistem.

c. Untuk mencapai ini, aspek-aspek berikut harus dipertimbangkan:
   1) Pemisahan lingkungan pengembangan, pengujian dan produksi; dan
   2) Panduan tentang keamanan dalam siklus hidup pengembangan perangkat lunak:
      a) Keamanan dalam metodologi pengembangan perangkat lunak;
      b) Pedoman pengkodean yang aman untuk setiap bahasa pemrograman yang digunakan;
      c) Persyaratan keamanan dalam fase spesifikasi dan desain;
      d) Pemeriksaan keamanan dalam proyek;
      e) Pengujian sistem dan keamanan, seperti pengujian regresi, pemindaian kode, dan pengujian penetrasi;
      f) Repositori yang aman untuk kode sumber dan konfigurasi;
      g) Keamanan dalam Kendali versi;
      h) Pengetahuan dan pelatihan keamanan aplikasi yang diperlukan; dan
      i) Kemampuan pengembang untuk mencegah, menemukan dan memperbaiki Kerentanan.

d. Jika pengembangan dialihdayakan, BKKBN harus memperoleh jaminan bahwa Mitra Kerja mematuhi aturan BKKBN dalam pengembangan yang aman.

26. Persyaratan Keamanan Aplikasi
   a. Persyaratan Keamanan Informasi diidentifikasi, ditentukan, dan disetujui saat pengembangan atau akuisisi aplikasi untuk memastikan semua persyaratan Keamanan Informasi diidentifikasi dan ditindaklanjuti.
   b. Persyaratan keamanan aplikasi bisa ditentukan melalui penilaian Risiko.
   c. Persyaratan keamanan aplikasi dapat mencakup berbagai topik, tergantung pada tujuan aplikasi.
   d. Persyaratan keamanan aplikasi, antara lain meliputi:
      1) Tingkat kepercayaan Entitas melalui otentikasi;
      2) Tipe klasifikasi Informasi yang diproses aplikasi;
      3) Kebutuhan pembagian akses aplikasi;
      4) Ketahanan terhadap Serangan siber;
      5) Kebutuhan privasi pihak terkait; dan
      6) Kendali input, proses, dan *output*.

27. Prinsip-prinsip Arsitektur dan Rekayasa Sistem yang Aman
   a. Prinsip-prinsip rekayasa sistem yang aman ditetapkan, didokumentasikan, dipelihara dan diterapkan pada setiap kegiatan pengembangan Sistem Informasi untuk memastikan Sistem Informasi dirancang, diimplementasikan, dan dioperasikan dengan aman dalam siklus hidup pengembangan.
   b. Keamanan dirancang ke dalam semua lapisan arsitektur (bisnis, data, aplikasi, dan teknologi).

c. Prinsip-prinsip rekayasa sistem yang aman diterapkan untuk alih daya pengembangan Sistem Informasi melalui kontrak dengan Mitra Kerja.

28. Pengkodean yang Aman
    a. Prinsip pengkodean yang aman diterapkan pada pengembangan perangkat lunak untuk memastikan perangkat lunak ditulis dengan aman sehingga mengurangi jumlah potensi Kerentanan Keamanan Informasi dalam perangkat lunak.
    b. BKKBN memantau Ancaman terkini tentang Kerentanan perangkat lunak untuk masukan prinsip-prinsip pengkodean aman BKKBN.
    c. Prinsip pengkodean yang aman digunakan untuk pengembangan baru maupun dalam skenario penggunaan kembali.
    d. Pertimbangan selama pengkodean mencakup:
        1) Praktik pengkodean yang aman khusus untuk bahasa dan teknik pemrograman yang digunakan;
        2) Menggunakan teknik pemrograman yang aman, seperti pemrograman berpasangan, pemfaktoran ulang, tinjauan sejawat, iterasi keamanan, dan pengembangan berbasis pengujian;
        3) Menggunakan teknik pemrograman terstruktur;
        4) Mendokumentasikan kode dan menghapus cacat pemrograman, yang memungkinkan Kerentanan Keamanan Informasi dieksploitasi; dan
        5) Melarang penggunaan teknik desain yang tidak aman (misalnya penggunaan *hard-coded password*, contoh kode yang tidak disetujui dan layanan web yang tidak diautentikasi);
    e. Pengujian harus dilakukan selama dan setelah pengembangan. Pengujian keamanan aplikasi statis Proses dapat mengidentifikasi Kerentanan keamanan dalam perangkat lunak.
    f. Sebelum perangkat lunak dibuat operasional, beberapa hal berikut ini dievaluasi:
        1) *Attack surface* dan prinsip hak istimewa minimum; dan
        2) Melakukan analisis kesalahan pemrograman yang paling umum dan mendokumentasikan bahwa ini telah dikurangi.
    g. Setelah kode dibuat operasional:
        1) Pembaruan dilakukan dengan aman;
        2) Kerentanan Keamanan Informasi ditangani dengan baik; dan
        3) Kesalahan maupun Serangan dicatat dan dicatat secara teratur untuk membuat penyesuaian pada kode yang diperlukan.

29. Pengujian Keamanan dalam Pengembangan dan Penerimaan
    a. Proses pengujian keamanan diimplementasikan dalam siklus hidup pengembangan untuk memvalidasi apakah persyaratan Keamanan Informasi terpenuhi saat aplikasi atau kode diimplementasikan ke dalam lingkungan produksi.
    b. Sistem Informasi baru, maupun perubahan harus diuji dan diverifikasi secara menyeluruh selama Proses pengembangan.

Pengujian keamanan menjadi bagian integral dari pengujian sistem atau komponen.

c. Pengujian keamanan dilakukan terhadap serangkaian persyaratan, yang dapat dinyatakan sebagai fungsional atau non-fungsional.
d. Rencana pengujian ditentukan dengan menggunakan seperangkat kriteria. Tingkat pengujian harus sebanding dengan kepentingan, sifat sistem dan dampak potensial atas perubahan.
e. BKKBN dapat memanfaatkan *tools* otomatis, seperti *tools* analisis kode atau pemindai Kerentanan, dan harus memverifikasi perbaikan keamanan.
f. Untuk pengembangan *in-house*, pengujian penerimaan independen dilakukan untuk memastikan bahwa sistem bekerja seperti yang diharapkan.
g. Untuk pengembangan yang dialihdayakan, Proses akuisisi harus diikuti. Kontrak dengan Mitra Kerja membahas persyaratan keamanan.
h. Pengujian dilakukan dalam lingkungan pengujian yang sesuai dengan lingkungan produksi untuk memastikan bahwa sistem tidak menimbulkan Kerentanan terhadap lingkungan BKKBN dan pengujian tersebut dapat diandalkan.

30. Pengembangan yang Dialihdayakan
    a. BKKBN mengarahkan, memantau, dan meninjau aktivitas terkait dengan pengembangan sistem yang dialihdayakan untuk memastikan Keamanan Informasi telah diimplementasikan dalam pengembangan sistem;
    b. Jika pengembangan sistem dialihdayakan, poin-poin berikut dipertimbangkan di seluruh rantai pasokan eksternal BKKBN:
        1) Perjanjian lisensi, kepemilikan kode dan hak kekayaan intelektual terkait dengan konten yang dialihdayakan;
        2) Persyaratan kontrak desain, pengkodean dan pengujian yang aman;
        3) Penyediaan model Ancaman untuk dipertimbangkan oleh pengembang eksternal;
        4) Pengujian penerimaan untuk kualitas dan akurasi kiriman;
        5) Penyediaan bukti bahwa tingkat keamanan dan kemampuan privasi yang dapat diterima;
        6) Penyediaan bukti bahwa pengujian yang memadai telah diterapkan untuk mencegah adanya konten jahat dan Kerentanan;
        7) Perjanjian *escrow* untuk kode sumber perangkat lunak;
        8) Hak kontraktual untuk mengaudit Proses dan pengendalian pengembangan;
        9) Persyaratan keamanan untuk lingkungan pengembangan; dan
        10) Dengan mempertimbangkan undang-undang yang berlaku (misalnya tentang Pelindungan Data Pribadi).
31. Pemisahan Lingkungan Pengembangan, Uji, dan Produksi
    a. Lingkungan pengembangan, pengujian dan produksi dipisahkan dan diamankan untuk melindungi lingkungan produksi dari kompromi data dengan aktivitas pengembangan dan pengujian.

b. Tingkat pemisahan antara lingkungan produksi, pengujian dan pengembangan diidentifikasi dan diimplementasikan.
c. Seseorang tidak boleh melakukan perubahan pada pengembangan dan produksi tanpa persetujuan sebelumnya. Hal ini dapat dicapai misalnya melalui pemisahan hak akses atau melalui aturan yang dipantau.

32. Manajemen Perubahan
    a. Perubahan Fasilitas Pemrosesan Informasi dan Sistem Informasi harus tunduk pada prosedur manajemen perubahan untuk menjaga Keamanan Informasi saat menjalankan perubahan.
    b. Pengenalan sistem baru dan perubahan sistem mengikuti aturan yang disepakati dan Proses formal dalam dokumentasi, spesifikasi, pengujian, Kendali kualitas, dan implementasi.
    c. Prosedur pengendalian perubahan diimplementasikan untuk memastikan kerahasiaan, keutuhan, dan ketersediaan Informasi dalam Fasilitas Pemrosesan Informasi dan Sistem Informasi dalam seluruh siklus hidup pengembangan sistem dari tahap desain awal hingga pemeliharaan.
33. Informasi Uji
    a. Informasi pengujian dilindungi dan dikelola dengan tepat untuk memastikan relevansi pengujian dan perlindungan Informasi operasional yang digunakan dalam pengujian.
    b. Informasi Sensitif (termasuk Informasi pengenal pribadi) tidak boleh disalin ke dalam lingkungan pengembangan dan pengujian.
    c. Untuk melindungi salinan Informasi operasional, saat digunakan untuk tujuan pengujian, beberapa hal berikut dilakukan:
        1) Menerapkan prosedur Kendali akses yang sama antara lingkungan pengujian dengan lingkungan operasional;
        2) Memiliki otorisasi terpisah setiap kali Informasi operasional disalin ke lingkungan pengujian;
        3) Mencatat penyalinan dan penggunaan Informasi operasional dengan menyediakan jejak audit;
        4) Melindungi Informasi Sensitif dengan penghapusan atau masking jika digunakan untuk pengujian; dan
        5) Menghapus Informasi operasional dengan benar dari lingkungan pengujian segera setelah pengujian selesai untuk mencegah penggunaan Informasi pengujian yang tidak sah.
    d. Informasi pengujian harus disimpan dengan aman dan hanya digunakan untuk tujuan pengujian.
34. Proteksi Sistem Informasi selama Pengujian Audit
    a. Pengujian audit dan kegiatan audit lainnya yang melibatkan penilaian sistem operasional disepakati antara penguji dan pimpinan dalam rangka meminimalkan dampak audit dan kegiatan jaminan lainnya pada sistem operasional dan Proses bisnis.
    b. Menyetujui permintaan audit untuk akses ke sistem dan data dengan pimpinan yang relevan.
    c. Menyetujui dan mengendalikan ruang lingkup pengujian audit teknis.
    d. Membatasi pengujian audit hanya dengan akses baca saja ke perangkat lunak maupun data.

e. Jika akses diberikan, dilakukan verifikasi persyaratan keamanan (misalnya *antivirus* dan *patching*) atas perangkat yang digunakan.
f. Hanya mengizinkan akses selain hanya baca untuk salinan *file system* yang terisolasi, menghapusnya saat audit selesai, atau memberi mereka perlindungan yang sesuai jika ada kewajiban untuk menyimpan *file* tersebut di bawah persyaratan dokumentasi audit.
g. Mengidentifikasi dan menyetujui permintaan untuk pemrosesan khusus seperti menjalankan *tools* audit.
h. Menjalankan tes audit di luar jam kerja, apabila dapat mempengaruhi Ketersediaan sistem.
i. Memantau dan mencatat semua akses untuk tujuan audit dan pengujian.

KEPALA BADAN KEPENDUDUKAN
DAN KELUARGA BERENCANA NASIONAL
REPUBLIK INDONESIA,

ttd

HASTO WARDOYO

Salinan sesuai dengan aslinya
Badan Kependudukan dan Keluarga Berencana Nasional
Kepala Biro Hukum, Organisasi, dan Tata Laksana

Puji Pratiningsih