PEDOMAN
NOMOR 2 TAHUN 2024
TENTANG
KEBIJAKAN PENGAMANAN INFORMASI
KEMENTERIAN PERENCANAAN PEMBANGUNAN NASIONAL/
BADAN PERENCANAAN PEMBANGUNAN NASIONAL

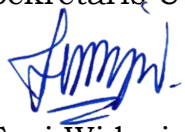
KATA PENGANTAR

Puji syukur kami panjatkan kepada Allah SWT, Tuhan Yang Maha Kuasa, karena atas berkat dan rahmat Nya, sehingga Dokumen Kebijakan Pengamanan Informasi di Kementerian Perencanaan Pembangunan Nasional/Badan Perencanaan Pembangunan Nasional (Kementerian PPN/Bappenas) telah selesai disusun. Tujuan dari disusunnya dokumen Kebijakan ini adalah sebagai panduan dalam melaksanakan Pengamanan Informasi di Kementerian PPN/Bappenas. Sebagaimana diketahui bahwa keamanan informasi merupakan salah satu aspek penting dalam mendukung pelaksanaan System Pemerintahan Berbasis Elektronik (SPBE).

Terima kasih kami ucapkan kepada semua pihak yang terlibat dalam penyusunan Dokumen Kebijakan Pengamanan Informasi di Kementerian PPN/Bappenas ini. Diharapkan kebijakan ini dapat diterapkan sehingga data dan informasi dapat terjaga kerahasiaan, keutuhan dan ketersediannya. Kami terbuka untuk mendapatkan kritik dan saran yang membangun dari semua pihak, demi perbaikan ke arah yang lebih baik.

Akhir kata, semoga Dokumen Kebijakan Pengamanan Informasi ini dapat bermanfaat untuk meningkatkan keamanan informasi di lingkungan Kementerian PPN/Bappenas.

Jakarta, 1 Maret 2024
Sekretaris Kementerian PPN/
Sekretaris Utama Bappenas



Teni Widuriyanti

DAFTAR ISI

BAB I
PENDAHULUAN

A. Latar Belakang

Informasi merupakan elemen yang sangat penting dalam rangka kegiatan operasional di Kementerian PPN/Bappenas. Untuk menjamin kesesuaian dan kebenaran informasi, terdapat tiga aspek yang harus dijaga yaitu:

1. Kerahasiaan (*confidentiality*), informasi tidak bocor atau diketahui oleh pihak yang tidak berwenang.
2. Integritas (*integrity*), akurasi, kebenaran, dan kelengkapan dari informasi tetap terjaga.
3. Ketersediaan (*availability*), informasi tersedia untuk diakses oleh pihak yang berwenang pada saat informasi tersebut dibutuhkan.

Kebijakan Pengamanan Informasi ini dapat memberikan panduan dalam membangun, mengimplementasikan, mengoperasikan, memonitor, memelihara, dan meningkatkan Sistem Manajemen Keamanan Informasi (SMKI) di lingkungan Kementerian PPN/Bappenas. Kebijakan Pengamanan Informasi ini juga ditujukan untuk meningkatkan pemahaman umum mengenai penerapan SMKI yang disesuaikan dengan standar ISO/IEC 27001:2022.

B. Tujuan

Sejalan dengan pentingnya informasi di Kementerian PPN/Bappenas, maka maksud utama dari pembuatan Kebijakan Pengamanan Informasi ini adalah memberikan arahan mengenai proses-proses pengamanan informasi terkait dengan perlindungan terhadap aset teknologi informasi yang digunakan. Keamanan informasi dapat dicapai dengan penerapan secara menyeluruh dan konsisten terhadap kontrol keamanan informasi yang tertuang dalam Kebijakan Pengamanan Informasi ini. Penggunaan dan pengelolaan informasi melatarbelakangi disusunnya Kebijakan Pengamanan Informasi yang mengacu pada standar internasional ISO/IEC 27001:2022 sebagai panduan dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI) di lingkungan Kementerian PPN/Bappenas.

Kebijakan Pengamanan Informasi ini akan memberikan panduan dalam membangun, mengimplementasikan, mengoperasikan, memonitor, memelihara dan meningkatkan SMKI di lingkungan Kementerian PPN/Bappenas dalam Kebijakan Pengamanan Informasi ini dibuat dengan mengacu kepada kontrol-kontrol yang ada pada *Annex A* ISO/IEC 27001:2022. SMKI yang diterapkan di Kementerian PPN/Bappenas secara spesifik bertujuan untuk:

1. Mengembangkan, mengimplementasikan, memonitor dan memperbaiki secara terus menerus Sistem Manajemen Keamanan Informasi dengan memastikan tersedianya kebijakan dan proses yang dibutuhkan untuk menjamin terjaganya keamanan informasi;
2. Menjaga aspek kerahasiaan, integritas dan ketersediaan seluruh aset informasi yang dikelola Kementerian PPN/Bappenas terhadap risiko kegagalan proses, penyalahgunaan, dan berbagai jenis kerusakan lainnya yang dapat menimbulkan kerugian bagi Kementerian PPN/Bappenas;
3. Pengelolaan secara terpadu dari proses penyediaan dan peningkatan sumber daya yang dibutuhkan bagi pelaksanaan proses keamanan informasi di Kementerian PPN/Bappenas; dan
4. Pengelolaan secara terpadu dalam pengembangan dan implementasi proses manajemen risiko dan pelaksanaan kontrol risiko terkait dengan keamanan informasi di Kementerian PPN/Bappenas.

C. Ruang Lingkup

Kebijakan ini berlaku di lingkungan Unit Kerja yang termasuk dalam proses implementasi SMKI di Kementerian PPN/Bappenas. Ruang lingkup Kebijakan Sistem Manajemen Keamanan Informasi (SMKI) ini adalah mencakup semua proses yang termasuk dalam proses implementasi SMKI yang dijalankan.

D. Definisi

1. Aplikasi adalah sistem dan prosedur yang telah di otomasikan untuk memproses data menjadi informasi yang dibuat dan disesuaikan terhadap kebutuhan Kementerian PPN/Bappenas sehingga dapat membantu proses bisnis yang dijalankan;
2. Aset adalah segala sesuatu yang mempunyai nilai di Kementerian PPN/Bappenas;
3. Pimpinan adalah suatu peran dalam manajemen keamanan informasi di Kementerian PPN/Bappenas yang bertanggung jawab terhadap pelaksanaan koordinasi perumusan petunjuk pelaksanaan keamanan informasi Kementerian PPN/Bappenas; mengusulkan rencana kerja dan target keamanan informasi, memastikan efektivitas dan konsistensi penerapan petunjuk pelaksanaan keamanan informasi Kementerian PPN/Bappenas; mengkoordinasikan pemberian akses data kepada pihak eksternal sesuai permintaan atau izin dari Data Owner; mengawasi dan mengevaluasi penerapan petunjuk pelaksanaan

keamanan informasi Kementerian PPN/Bappenas; dan melaporkan kinerja pelaksanaan petunjuk pelaksanaan keamanan informasi Kementerian PPN/Bappenas serta pencapaian target keamanan informasi;

4. Data adalah sekumpulan teks, angka, dan simbol yang bersumber dari fakta namun belum mempunyai makna/arti, yang diperoleh berdasarkan fakta-fakta, baik secara pengukuran maupun pernyataan yang tidak dapat diukur (laten).
5. *Denial of Service* adalah suatu kondisi dimana sistem tidak dapat memberikan layanan secara normal, yang disebabkan oleh suatu proses yang diluar kendali baik dari dalam maupun dari luar sistem.
6. Informasi adalah data dalam berbagai bentuk (input, output, dan data terproses) yang digunakan dalam aktivitas di Kementerian PPN/Bappenas;
7. Insiden yang termasuk didalamnya insiden siber adalah suatu kejadian operasi penggunaan data/informasi yang bisa mengakibatkan penurunan keutuhan/ integritas sistem, gangguan ketersediaan, dan pengungkapan kerahasiaan data/informasi, meliputi antara lain: probing, phishing, browsing dan akses secara tak berwenang, denial of service, pengubahan atau penghancuran input, proses, storage, atau output informasi, termasuk perubahan karakteristik sistem atau software secara tak berwenang;
8. Infrastruktur adalah teknologi dan fasilitas (hardware, sistem operasi, database management system, networking, multimedia, beserta lingkungan yang memfasilitasi dan mendukungnya) yang memungkinkan pemrosesan aplikasi-aplikasi teknologi informasi Kementerian PPN/Bappenas;
9. Pegawai adalah orang yang bekerja di Kementerian PPN/Bappenas, yang berstatus sebagai pegawai tetap dan tidak tetap dan menerima gaji berdasarkan hubungan kerja;
10. Kerahasiaan (*confidentiality*) adalah karakteristik data/informasi yang hanya dapat diketahui oleh mereka yang berwenang melalui cara yang diotorisasikan;
11. Ketersediaan (*availability*) adalah karakteristik data/informasi yang menjamin bahwa pengguna yang berwenang dapat mengakses informasi pada saat diperlukan.
12. Keutuhan (*integrity*) adalah karakteristik data/informasi yang menjamin informasi akurat, lengkap, tidak berubah selama pengiriman dan pemrosesannya;

13. 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.
14. Pengguna adalah individu atau kelompok yang memanfaatkan Layanan Teknologi Informasi, dari internal maupun eksternal Kementerian PPN/Bappenas;
15. Pengguna internal adalah pegawai tetap dan pegawai tidak tetap yang diikat oleh perjanjian kerja langsung dengan Kementerian PPN/Bappenas dengan pemberian hak akses user dibatasi sesuai masa kontrak (sementara);
16. Pengguna eksternal adalah pihak instansi lain (Kementerian/ Lembaga/ Daerah) sebagai Wali Data dan pihak ketiga berdasarkan perjanjian/ kontrak pengadaan barang/ jasa atau perjanjian/ kontrak/ surat tugas untuk melakukan pemeriksaan/ asesmen/ audit (pajak/ keuangan/ lainnya);
17. Penghapusan/ pemusnahan/ disposal/ *retirement* aset adalah penarikan aktiva tetap dan/atau penghentian aset tetap dalam pengakuan secara finansial maupun fisik;
18. *Platform-as-a-Service* (PaaS) adalah lingkungan pengembangan dan penyebaran yang lengkap di cloud, layanan cloud yang disediakan dalam bentuk platform dan dapat dimanfaatkan pengguna untuk membuat aplikasi di atasnya. PaaS memberikan framework bagi developer yang dapat bangun dan gunakan untuk membuat aplikasi yang telah disesuaikan.
19. Pihak Ketiga adalah semua unsur di luar pengguna unit TI Kementerian PPN/Bappenas yang bukan bagian dari Kementerian PPN/Bappenas, misal mitra kerja Kementerian PPN/Bappenas (seperti: konsultan, penyedia jasa komunikasi, pemasok dan pemelihara perangkat pengolah informasi), dan institusi lain;
20. *Plan-Do-Check-Act* (PDCA) adalah pendekatan tahapan berkelanjutan untuk meningkatkan proses implementasi SMKI di Kementerian PPN/Bappenas;
21. Proses organisasi adalah sekumpulan aktivitas lintas fungsi unit kerja yang saling terkait untuk menghasilkan produk atau layanan bagi pengguna/ pengguna;
22. Pseudonimisasi adalah pemrosesan data pribadi dengan cara yang membuat data pribadi tersebut tidak dapat dikaitkan lagi ke subjek data pribadi;

23. Risiko adalah segala kejadian dalam setiap aktivitas yang mungkin timbul karena faktor ketidakpastian, yang mengandung potensi untuk menghambat pencapaian tujuan Kementerian PPN/Bappenas;
24. *Service Level Agreement* (SLA) adalah perjanjian dari penyedia layanan dengan pengguna yang memberikan jaminan tingkat pelayanan yang dapat diharapkan;
25. Sistem Informasi adalah suatu sistem terpadu yang terdiri dari Aplikasi/ perangkat lunak/ *software*, infrastruktur/ perangkat keras/*hardware*, sumber Data dan sumber daya manusia/ *brainware*, serta prosedur untuk mengumpulkan, mentransformasikan, dan menyebarkan informasi dalam suatu organisasi;
26. SMKI (Sistem Manajemen Keamanan Informasi) adalah suatu sistem manajemen yang meliputi petunjuk pelaksanaan, organisasi, perencanaan, penanggung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko organisasi untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan keamanan informasi Kementerian PPN/Bappenas;
27. *Threat intelligence* merupakan bagian dari strategi sistem keamanan yang melindungi suatu organisasi dari ancaman eksternal maupun internal. Solusi ini memungkinkan perusahaan menjadi lebih proaktif dalam mengatur kontrol keamanan untuk mendeteksi dan mencegah serangan lebih lanjut. Proses tersebut dilakukan menggunakan pendekatan otomatisasi sehingga keamanan tetap selaras dengan kondisi sistem secara real-time.
28. Teknologi Informasi (TI) suatu teknologi yang mencakup perangkat keras (hardware), perangkat lunak (software), network komunikasi, serta teknik manajemen sumber data yang membantu mengumpulkan dan mentransformasikan sumber data menjadi produk informasi serta menyebarkan informasi tersebut kepada Pengguna;
29. Unit Kerja adalah direktorat atau unit kerja yang bertanggung jawab terhadap terlaksananya suatu kegiatan atau aktivitas tertentu di Kementerian PPN/Bappenas; dan
30. *Vulnerability Assessment* yang termasuk didalamnya *Penetration Test* adalah kegiatan untuk mendapatkan informasi mengenai kelemahan/kerentanan keamanan pada lingkungan/sistem TI Kementerian PPN/Bappenas. Penilaian kerentanan juga dapat memberikan arahan mengenai cara-cara untuk memulihkan atau

mengurangi kerentanan tersebut sebelum dapat dieksploitasi. VA ini juga termasuk kegiatan yang dirancang untuk mencapai tujuan tertentu melalui simulasi eksploitasi sistem TI berdasarkan permintaan dari pengguna/ pemohon.

BAB 2
KETENTUAN UMUM

A. Area & Domain Penerapan SMKI

Kementerian PPN/Bappenas menetapkan, menerapkan, memelihara dan melaksanakan perbaikan berkesinambungan terhadap Keamanan Informasi sesuai persyaratan ISO/IEC 27001.

Area dan domain penerapan SMKI Kementerian PPN/Bappenas adalah sebagai berikut:

1. Kebijakan Keamanan Informasi
   Arahan manajemen dan dukungan untuk Keamanan Informasi sesuai dengan persyaratan di Kementerian PPN/Bappenas dan peraturan yang relevan.
2. Organisasi Keamanan Informasi
   Menjaga keamanan informasi di Kementerian PPN/Bappenas dan fasilitas pemrosesannya yang diakses, diproses, dikomunikasikan kepada, atau dikelola oleh pihak eksternal.
3. Keamanan Sumber Daya Manusia
   Peran dan tanggung jawab yang jelas, kesadaran dan pelatihan Keamanan Informasi, keluar dari Kementerian PPN/Bappenas secara tertib.
4. Pengelolaan Aset
   Untuk mengklasifikasikan dan melindungi aset di Kementerian PPN/Bappenas dengan tepat.
5. Kontrol Akses
   Mencegah akses tidak sah ke sistem informasi, layanan jaringan, sistem operasi, sistem aplikasi, dan memastikan Keamanan Informasi saat menggunakan komputasi seluler dan fasilitas *teleworking*.
6. Cryptography
   Berhubungan dengan kontrol kriptografi.
7. Keamanan Fisik dan Lingkungan
   Mencegah akses fisik yang tidak sah di lokasi dan kehilangan/ kerusakan/ pencurian peralatan.
8. Keamanan Operasional
   Memastikan jaringan yang aman, memelihara perjanjian pengiriman layanan pihak ketiga yang sesuai, meminimalkan risiko kegagalan sistem, dan melindungi integritas perangkat lunak dan informasi.
9. Keamanan Komunikasi
   Berhubungan dengan komunikasi Jaringan, transfer informasi dan komunikasi dengan pemasok.

10. Akuisisi, Pengembangan, dan Pemeliharaan Sistem
    Mencegah kesalahan, kehilangan, modifikasi yang tidak sah atau penyalahgunaan informasi dalam aplikasi, memastikan keamanan file sistem dan perangkat lunak, dan mengurangi risiko akibat eksploitasi kerentanan teknis yang dipublikasikan.
11. Hubungan Pemasok
    Keamanan informasi dalam hubungan pemasok dan perjanjian pemasok.
12. Manajemen Insiden Keamanan Informasi
    Komunikasi tepat waktu tentang kejadian dan kelemahan serta mengambil tindakan korektif.
13. Aspek Keamanan Informasi dalam *Business Continuity Management*
    Menangkal gangguan terhadap aset Kementerian PPN/Bappenas dan melindungi proses bisnis penting dari efek kegagalan besar atau bencana, dan untuk memastikan dimulainya kembali secara tepat waktu.
14. Kepatuhan
    Mematuhi persyaratan yang berlaku di Kementerian PPN/Bappenas, petunjuk pelaksanaan dan standar keamanan.

B. Kebijakan Keamanan Informasi
1. Kebijakan keamanan informasi bertujuan untuk melindungi aset Kementerian PPN/Bappenas yang dikelola dan digunakan agar terhindar dari berbagai ancaman internal maupun eksternal yang meliputi keamanan data, perangkat teknologi, infrastruktur dan sistem, seluruh aktivitas serta proses yang terkait dengan penyediaan informasi.
2. Pimpinan menetapkan Kebijakan Keamanan Informasi sebagai acuan dalam implementasi sistem manajemen keamanan informasi pada layanan Kementerian PPN/Bappenas.
3. Petunjuk pelaksanaan Keamanan Informasi dilakukan reviu secara berkala, 1 (satu) kali dalam setahun untuk memastikan peningkatan implementasi sistem manajemen keamanan informasi.

C. Organisasi Keamanan Informasi
1. Internal Organisasi
    a. Pimpinan menetapkan tim pelaksana implementasi sistem manajemen keamanan informasi.

b. Memastikan pemisahan peran dan tanggung jawab untuk setiap pegawai yang termasuk dalam tim pelaksana sistem manajemen keamanan informasi.
c. Kementerian PPN/Bappenas dapat menjalin hubungan komunikasi dengan kelompok/komunitas yang memiliki pengetahuan/keahlian khusus dalam bidang keamanan informasi atau yang relevan dengan keamanan informasi, seperti namun tidak terbatas pada: *Indonesia Security Incident Response Team on Internet and Infrastructure* (ID-SIRTII), *Unit cybercrime* POLRI, BSSN, dan ISACA.
d. Menerapkan sistem manajemen keamanan informasi dalam proses pengelolaan proyek yang dilaksanakan di lingkungan Kementerian PPN/Bappenas.

2. *Mobile Device* and *Teleworking*
a. Proses ini bertujuan untuk memastikan keamanan informasi saat bekerja menggunakan perangkat *mobile computing* dan *teleworking*.
b. Pengguna fasilitas notebook dan *smartphone/tablet* harus menjaga keamanan dari perangkat dan informasi yang disimpan pada perangkat pada saat digunakan di luar area Kementerian PPN/Bappenas.
c. Penggunaan fasilitas notebook dan *smartphone/tablet* di luar area Kementerian PPN/Bappenas harus dilengkapi dengan kontrol keamanan fisik untuk mencegah terjadinya pencurian/kehilangan perangkat.
d. Fasilitas notebook dan *smartphone/tablet* milik Kementerian PPN/Bappenas tidak boleh ditinggalkan tanpa pengawasan atau tanpa pengamanan pada saat digunakan di luar area Kementerian PPN/Bappenas.
e. Penggunaan fasilitas notebook dan *smartphone/tablet* milik Kementerian PPN/Bappenas yang menyimpan informasi sensitif pada area publik, seperti restoran, stasiun, atau bandara harus sangat dibatasi.
f. Penggunaan fasilitas wifi publik untuk mengirim informasi sensitif milik Kementerian PPN/Bappenas harus sangat dibatasi.
g. Aktivitas *teleworking* didefinisikan sebagai aktivitas yang memungkinkan pegawai Kementerian PPN/Bappenas untuk bekerja secara remote dari sebuah lokasi tetap yang telah ditentukan, seperti rumah atau area kerja lain, di luar jaringan komunikasi Kementerian PPN/Bappenas.

h. Kegiatan *teleworking* hanya dilaksanakan untuk keperluan kedinasan.
i. Pegawai yang akan melaksanakan kegiatan *teleworking* perlu memperhatikan lokasi tempat bekerja, antara lain sebagai berikut:
j. Menghindari bekerja di tempat umum yang terbuka.
k. Memperhatikan keamanan fisik sekitar lokasi tempat *teleworking* dilakukan.
l. Setiap jaringan lokal *teleworking* yang dipersiapkan harus memperhatikan faktor keamanan jaringan.

3. Threat Intelligence

a. Informasi tentang ancaman yang ada atau muncul dikumpulkan dan dianalisis untuk:
   1) Memfasilitasi tindakan yang diinformasikan untuk mencegah ancaman yang menyebabkan kerugian bagi Kementerian PPN/Bappenas;
   2) Mengurangi dampak dari ancaman tersebut.
   3) *Threat Intelligence* dapat dibagi menjadi tiga lapisan, yang semuanya harus dipertimbangkan:
   4) *Threat Intelligence* strategis: pertukaran informasi tingkat tinggi tentang perubahan ancaman lanskap (misalnya jenis penyerang atau jenis serangan);
   5) *Threat Intelligence* taktis: informasi tentang metodologi, alat, dan teknologi penyerang terlibat;
   6) *Threat Intelligence* operasional: perincian tentang serangan spesifik, termasuk indikator teknis.
b. *Threat Intelligence* harus:
   1) Relevan (yaitu terkait dengan perlindungan di Kementerian PPN/Bappenas);
   2) Wawasan (yaitu menyediakan pemahaman yang akurat dan rinci tentang lanskap ancaman di Kementerian PPN/Bappenas);
   3) Kontekstual, untuk memberikan kesadaran situasional (yaitu menambahkan konteks pada informasi berdasarkan waktu kejadian, tempat terjadinya, pengalaman sebelumnya dan prevalensi di instansi serupa);
   4) Dapat ditindaklanjuti (yaitu Kementerian PPN/Bappenas dapat bertindak berdasarkan informasi dengan cepat dan efektif).
c. Kegiatan*Threat Intelligence* harus mencakup:

1) Menetapkan tujuan kegiatan intelijen ancaman;
2) Mengidentifikasi, memeriksa dan memilih sumber informasi internal dan eksternal yang diperlukan dan tepat untuk memberikan informasi yang diperlukan untuk kegiatan intelijen ancaman;
3) Mengumpulkan informasi dari sumber-sumber terpilih, yang dapat bersifat internal dan eksternal;
4) Memproses informasi yang dikumpulkan untuk mempersiapkannya untuk analisis (misalnya dengan menerjemahkan, memformat, atau informasi yang menguatkan);
5) Menganalisis informasi untuk memahami bagaimana informasi tersebut berkaitan dan bermakna bagi Kementerian PPN/Bappenas;
6) Mengomunikasikan dan membagikannya kepada individu yang relevan dalam format yang dapat dipahami.

d. Kegiatan Threat Intelligence harus dianalisis dan kemudian digunakan:
1) Dengan menerapkan proses untuk menyertakan informasi yang dikumpulkan dari sumber intelijen ancaman ke dalam proses manajemen risiko keamanan informasi di Kementerian PPN/Bappenas;
2) Sebagai input tambahan untuk kontrol preventif dan detektif teknis seperti firewall, deteksi intrusi sistem, atau solusi anti malware;
3) Sebagai masukan untuk proses dan teknik pengujian keamanan informasi.

e. Kementerian PPN/Bappenas dapat berbagi informasi terkait kegiatan Threat Intelligence dengan instansi lain secara saling menguntungkan untuk meningkatkan intelijen ancaman secara keseluruhan.

4. Keamanan Informasi untuk Penggunaan Layanan *Cloud*
a. Kementerian PPN/Bappenas harus menetapkan dan mengomunikasikan kebijakan khusus tentang penggunaan layanan *cloud* kepada semua pihak terkait yang berkepentingan.
b. Kementerian PPN/Bappenas harus mendefinisikan dan mengomunikasikan cara untuk mengelola risiko keamanan informasi terkait dengan penggunaan layanan *cloud*. Ini bisa menjadi perpanjangan atau bagian dari pendekatan yang

ada untuk bagaimana mengelola layanan yang diberikan oleh pihak eksternal.

c. Organisasi harus menetapkan dan mengkomunikasikan kebijakan yang spesifik mengenai penggunaan layanan cloud kepada semua pihak terkait yang berkepentingan. Kementerian PPN/Bappenas perlu mendefinisikan dan mengomunikasikan cara mengelola risiko keamanan informasi yang terkait dengan penggunaan layanan cloud. Hal ini dapat menjadi pengembangan atau bagian dari pendekatan yang ada bagaimana mengelola layanan yang diberikan oleh pihak eksternal terkait layanan cloud.

d. Dalam penggunaan layanan *cloud,* Kementerian PPN/Bappenas harus mendefinisikan:
   1) Semua persyaratan keamanan informasi yang relevan terkait dengan penggunaan layanan *cloud*;
   2) Kriteria pemilihan layanan *cloud* dan ruang lingkup penggunaan layanan *cloud*;
   3) Peran dan tanggung jawab terkait penggunaan dan pengelolaan layanan *cloud*;
   4) Kontrol keamanan informasi mana yang dikelola oleh penyedia layanan *cloud* dan yang mana dikelola oleh organisasi sebagai pengguna layanan *cloud*;
   5) Cara mendapatkan dan memanfaatkan kemampuan keamanan informasi yang disediakan oleh penyedia layanan *cloud*;
   6) Cara mendapatkan jaminan atas kontrol keamanan informasi yang diterapkan oleh penyedia layanan *cloud*;
   7) Bagaimana mengelola kontrol, antarmuka, dan perubahan layanan ketika menggunakan banyak layanan *cloud*, khususnya dari berbagai penyedia layanan *cloud*;
   8) Prosedur penanganan insiden keamanan informasi yang terjadi sehubungan dengan penggunaan layanan *cloud*;
   9) Menetapkan pendekatan untuk memantau, meninjau, dan mengevaluasi penggunaan layanan cloud yang sedang digunakan untuk mengelola risiko keamanan informasi dari penggunaan layanan cloud tersebut;
   10) Terdapat mekanisme dalam mengubah atau menghentikan penggunaan layanan cloud, termasuk strategi jika ingin berhenti menggunakan layanan cloud.

e. Perjanjian layanan *cloud* seringkali berupa *subscription/generic* dari layanan sehingga tidak terbuka untuk membahas dalam bentuk perjanjian. Untuk semua layanan *cloud*, Kementerian PPN/Bappenas harus meninjau perjanjian layanan *cloud* dengan penyedia layanan cloud. Sebuah awan perjanjian layanan harus membahas kerahasiaan, integritas, ketersediaan dan penanganan informasi persyaratan organisasi, dengan tujuan tingkat layanan cloud dan layanan cloud yang sesuai tujuan kualitatif. Kementerian PPN/Bappenas juga harus melakukan penilaian risiko yang relevan untuk mengidentifikasi risiko yang terkait dengan penggunaan layanan cloud. Risiko residual apa pun yang terkait dengan penggunaan cloud layanan harus secara jelas diidentifikasi dan diterima oleh manajemen organisasi yang sesuai.

f. Perjanjian antara penyedia layanan cloud dan Kementerian PPN/Bappenas, harus mencakup ketentuan berikut dalam upaya perlindungan data dan ketersediaan layanan:
   1) Memberikan solusi berdasarkan standar yang berlaku untuk arsitektur dan infrastruktur;
   2) Mengelola kontrol akses layanan *cloud* untuk memenuhi persyaratan;
   3) Menerapkan solusi pemantauan dan perlindungan malware;
   4) Memproses dan menyimpan informasi sensitif milik Kementerian PPN/Bappenas di lokasi yang disetujui (mis. negara atau wilayah tertentu) atau di dalam atau tunduk pada yurisdiksi tertentu;
   5) Memberikan dukungan khusus jika terjadi insiden keamanan informasi di layanan *cloud*;
   6) Memastikan bahwa persyaratan keamanan informasi di Kementerian PPN/Bappenas terpenuhi jika layanan cloud disubkontrakkan ke pihak lain (atau melarang layanan cloud disubkontrakkan);
   7) Mendukung Kementerian PPN/Bappenas dalam mengumpulkan bukti digital, dengan mempertimbangkan undang-undang dan peraturan untuk bukti digital di berbagai yurisdiksi;
   8) Memberikan dukungan yang tepat dan ketersediaan layanan untuk kerangka waktu yang tepat ketika

Kementerian PPN/Bappenas ingin keluar dari layanan *cloud*;

9) Menyediakan cadangan data dan informasi konfigurasi yang diperlukan serta mengelola cadangan dengan aman sebagaimana berlaku, berdasarkan kemampuan penyedia layanan *cloud* yang digunakan oleh Kementerian PPN/Bappenas, bertindak sebagai pengguna layanan *cloud*;

10) Menyediakan dan mengembalikan informasi seperti file konfigurasi, kode sumber dan data yang dimiliki oleh Kementerian PPN/Bappenas, saat diminta selama penyediaan layanan atau pada penghentian layanan.

g. Kementerian PPN/Bappenas, yang bertindak sebagai pengguna layanan *cloud*, harus mempertimbangkan apakah dalam perjanjian tersebut mewajibkan penyedia layanan *cloud* untuk memberikan pemberitahuan terlebih dahulu ke Kementerian PPN/Bappenas jika terjadi perubahan yang dilakukan pada layanan, seperti:

1) Perubahan infrastruktur teknis (misalnya relokasi, konfigurasi ulang, atau perubahan perangkat keras atau perangkat lunak) yang mempengaruhi atau mengubah layanan *cloud*;

2) Memproses atau menyimpan informasi pada lokasi geografis atau yurisdiksi hukum yang berbeda;

3) Penggunaan penyedia layanan *cloud* sejenis atau subkontraktor lainnya (termasuk mengubah atau menggunakan pihak lain).

h. Unit kerja pada Kementerian PPN/Bappenas yang menggunakan layanan *cloud* harus menjaga kontak dengan penyedia layanan *cloud*-nya. Hal ini agar dapat memudahkan dalam bertukar informasi ataupun terkait isu keamanan terkait penggunaan layanan cloud. Termasuk bagaimana dalam perjanjian dengan layanan cloud dapat mencantumkan secara jelas bagaimana mekanisme untuk memantau karakteristik layanan ataupun tingkat layanan yang diperjanjikan serta apabila ada ketidaksesuaian dengan layanan.

D. Keamanan Sumber Daya Manusia (SDM)

1. Biro SDM dan Pimpinan harus memastikan pengelolaan keamanan SDM pada saat sebelum bekerja, selama bekerja dan pada saat pindah/ berhenti bekerja.

2. Biro SDM harus melaksanakan proses penyaringan (*screening*) secara proporsional dengan memperhitungkan latar belakang dan pengetahuan keamanan informasi seluruh calon pegawai dan/atau pihak ketiga.
3. Dalam proses penyaringan, Biro SDM harus melakukan pengecekan latar belakang melalui:
   a. Dokumen Daftar Riwayat Hidup (Curriculum Vitae/CV) yang dilampirkan.
   b. Pencarian profil dan perilaku calon pegawai/pihak ketiga melalui media sosial dan referensi pihak lain.
   c. Dokumen Surat Keterangan Catatan Kepolisian (SKCK) yang dilampirkan (jika ada).
4. Pihak ketiga harus menyetujui dan menandatangani ketentuan NDA yang berisikan tanggung jawab terkait keamanan informasi.
5. Biro SDM dan Pimpinan bertanggung jawab untuk memberikan pemahaman keamanan informasi yang cukup untuk menjalankan prosedur keamanan informasi dalam pekerjaannya dan mengeliminasi risiko terjadinya human error.
6. Pegawai Kementerian PPN/Bappenas dan pihak ketiga harus mendapatkan pembekalan pemahaman keamanan informasi (*Security Awareness*) dan sosialisasi Kebijakan Keamanan Informasi dan SOP terkait SMKI secara berkala (1 tahun sekali) yang diprogramkan oleh Tim SMKI untuk hal-hal yang terkait dengan pekerjaannya.
7. Pegawai Kementerian PPN/Bappenas dan pihak ketiga sebelum menjalankan tugas/pekerjaannya harus mendapatkan dan memahami:
   a. Uraian tugas (*job description*) pegawai;
   b. Prosedur penggunaan aset TI;
   c. *Non-Disclosure Agreement* (NDA); dan
   d. Dokumen kontrak kerjasama.
8. Pemberian akses informasi berklasifikasi Rahasia Tercatat, Rahasia Terbatas, dan Rahasia kepada pegawai tetap, pegawai kontrak, pegawai magang, maupun pihak ketiga harus mendapatkan persetujuan dari Pimpinan.
9. Pimpinan harus menjamin pegawai di unit kerjanya mematuhi seluruh ketentuan keamanan informasi dan melakukan pengawasan terhadap pelaksanaannya.
10. Pegawai dan pihak ketiga yang telah habis masa kerja/kontraknya harus melaporkan dan mengembalikan seluruh aset TI serta hak akses terhadap aset TI dan aset lain

yang dipergunakan selama bekerja di Kementerian PPN/Bappenas.

11. Hak akses yang diberikan kepada pegawai, pekerja kontrak, dan pihak ketiga terhadap informasi dan fasilitas pengolahan informasi harus ditinjau kembali, termasuk kemungkinan pencabutan atau perubahan hak akses pada saat terjadi penggantian penugasan yang dapat diakibatkan oleh pemberhentian, promosi, demosi, mutasi, atau cuti jangka panjang, dan dikendalikan oleh pimpinan unit kerja masing-masing.
12. Pusdatinrenbang memiliki hak untuk mencabut sementara atau permanen hak akses pegawai yang sedang menjalani pemeriksaan terkait masalah fraud atau masalah hukum dari pihak berwenang.

E. Pengelolaan Aset

1. Ketentuan Pengelolaan Aset
   a. Pengelolaan aset mencakup:
      1) Informasi (*softcopy* dan *hardcopy*), termasuk namun tak terbatas pada: data pegawai, IT Blueprint/IT Master Plan, hasil kajian risiko (*Risk Register*), laporan audit, laporan *vulnerability assessment*, dokumen tender dan kontrak, kebijakan, pedoman, dan prosedur, topologi jaringan, materi training, dan bukti implementasi kebijakan, pedoman, dan prosedur.
      2) Perangkat Lunak (*Software*) termasuk namun tidak terbatas pada: aplikasi utama dan aplikasi pendukung yang ada di Kementerian PPN/Bappenas.
      3) Perangkat keras (*Hardware*) dan Perangkat Jaringan termasuk namun tidak terbatas pada: Server, PC/Desktop & Laptop, perangkat jaringan, *removable media* (hard disk, tape, USB), dan perangkat lainnya yang digunakan dalam penyelenggaraan layanan sistem elektronik.
      4) Perangkat Pendukung termasuk namun tidak terbatas pada: Ruang Server/Pusat Pengelolaan Teknologi Informasi, Ruang NOC, UPS, Genset, A/C, CCTV, alat pemadam kebakaran (Fire Suppression, APAR, FM200), penangkal petir, Access Door.
   b. Format informasi yang tercakup dalam pedoman ini meliputi:

1) Format Cetakan/Kertas (*Hardcopy*), yaitu informasi dalam bentuk dokumen tercetak/kertas;
2) Format File Elektronik (*Softcopy*), yaitu informasi yang disimpan dalam berbagai media elektronik seperti Hardisk Internal, Hardisk Eksternal, Flashdisk, CD, tape atau media simpan elektronik lainnya.

c. Klasifikasi aset informasi
1) Klasifikasi aset informasi di Kementerian PPN/Bappenas didefinisikan berdasarkan tingkat kerahasiaan (*Confidentiality*).
2) Kementerian PPN/Bappenas dapat menetapkan klasifikasi informasi sesuai dengan kebutuhan di Kementerian PPN/Bappenas.

2. Inventarisasi dan Pengalihan Aset
a. Seluruh aset yang terkait dengan informasi, fasilitas pengolahan/ pemroses informasi, dan sarana pendukungnya, yang dipergunakan dalam proses penyelenggaraan layanan di Kementerian PPN/Bappenas, harus diidentifikasi dan diinventarisasi.
b. Tim Manajemen Aset dan Risiko bertanggung jawab untuk mengidentifikasi, menginventarisasi, serta mengkoordinasikan dan memantau penggunaan, perubahan, pemusnahan, penghapusan, dan pembaharuan/pengkinian aset terkait informasi dan sistem informasi Kementerian PPN/Bappenas.
c. Hasil identifikasi dan inventarisasi aset harus didokumentasikan, dipelihara, dan diperiksa secara berkala kesesuaiannya, minimal 1 (satu) kali setiap 6 (enam) bulan.
d. Aset yang harus diidentifikasi dan diinventarisasi di Kementerian PPN/Bappenas meliputi kategori sebagai berikut:
1) Aset Perangkat Keras, meliputi: komputer/PC, Notebook, Server, Printer, Scanner, peralatan telekomunikasi, *removable media* (External Hard Disk, USB, dll).
2) Aset Perangkat Lunak, meliputi: sistem informasi dan aplikasi.
3) Aset Informasi, meliputi: kebijakan dan prosedur, dokumentasi proses Kementerian PPN/Bappenas, database system, data pengguna, data pihak ketiga, dan lain-lain.
4) Aset Sumber Daya Manusia/Pegawai.

5) Aset sarana dan fasilitas pendukung, meliputi: ruang kerja, jaringan komunikasi, listrik, UPS, genset, Precision Air Conditioner (AC).
6) Aset tak berwujud (intangible asset), meliputi: reputasi Kementerian PPN/Bappenas.

e. Identifikasi dan inventarisasi aset setidaknya mencakup informasi keterangan sebagai berikut:
1) Identitas perangkat, misalnya ID aset, nama perangkat, alamat jaringan (static IP address).
2) Jenis aset.
3) Spesifikasi aset.
4) Identitas pembuat/merek aset, pemilik aset, dan pengguna aset.
5) Status aset (aktif, dalam perbaikan, rusak, dalam penyimpanan).
6) Lokasi bagian yang menggunakan/menyimpan aset.
7) Lokasi penyimpanan aset.
8) Siklus aset, misalnya: tanggal pengadaan, tanggal instalasi, tanggal operasional.
9) Penilaian klasifikasi aset berdasarkan aspek kerahasiaan, integritas, dan ketersediaan.

f. Klasifikasi terhadap aset ditentukan berdasarkan kritikalitas aset berdasarkan aspek kerahasiaan, integritas dan ketersediaan dari aset.

g. Kepemilikan aset di lingkup Kementerian PPN/Bappenas dikategorikan menjadi 3 (tiga) kelompok kepemilikan sebagai berikut:
1) Aset Barang Milik Kementerian PPN/Bappenas. Dalam hal ini merupakan aset milik Kementerian PPN/Bappenas dengan sumber dana pembelian dari anggaran belanja Kementerian PPN/Bappenas. Aset Kementerian PPN/Bappenas diberikan identifikasi label aset dengan format sesuai ketentuan pengelolaan aset Kementerian PPN/Bappenas.
2) Aset milik pribadi pegawai Kementerian PPN/Bappenas. Dalam hal ini merupakan aset milik pribadi dari pegawai Kementerian PPN/Bappenas. Aset pribadi yang akan digunakan untuk keperluan pekerjaan dan operasional Kementerian PPN/Bappenas, diberikan label aset dengan ketentuan format serupa dengan ketentuan label aset.

3) Aset milik pihak ketiga yang ditempatkan di dan/atau digunakan oleh dan untuk keperluan proses Kementerian PPN/Bappenas. Aset milik pihak ketiga yang akan digunakan untuk keperluan pekerjaan dan operasional Kementerian PPN/Bappenas, jika belum terdapat label aset dari pemilik aset, maka akan diberikan label aset dengan ketentuan format serupa dengan ketentuan label aset Non Kementerian PPN/Bappenas.

h. Setiap perpindahan atau pengalihan aset, harus didokumentasikan secara formal menggunakan formulir Serah Terima Aset. hal ini diantaranya:
   1) Penyerahan aset dari proses pengadaan kepada Tim Manajemen Aset dan Risiko;
   2) Penyerahan atau pengalokasian aset dari Tim Manajemen Aset dan Risiko kepada pengguna aset;
   3) Pengembalian aset dari pengguna aset kepada Tim Manajemen Aset dan Risiko; dan
   4) Penyerahan aset dari Kementerian PPN/Bappenas kepada pihak ketiga atau sebaliknya, misalnya untuk proses perbaikan aset.

i. Pengguna aset bertanggung jawab untuk:
   1) memastikan bahwa aset yang menjadi tanggung jawabnya telah teridentifikasi dan terinventarisasi;
   2) memastikan bahwa setiap aset telah diklasifikasikan dan dilindungi secara memadai;
   3) mendefinisikan dan meninjau pengendalian akses ke aset tersebut; dan
   4) memastikan penanganan yang baik untuk aset.

j. Penempatan aset Kementerian PPN/Bappenas di lokasi pihak ketiga atau sebaliknya, harus disertai dengan surat perjanjian yang mengatur hak dan kewajiban masing-masing pihak terkait penyimpanan, pengelolaan, dan pengamanan aset serta pernyataan menjaga kerahasiaan.

3. Penggunaan Aset yang Diperbolehkan
   a. Aset Milik Kementerian PPN/Bappenas
      1) Kementerian PPN/Bappenas menyediakan aset perangkat pengolah/pemroses informasi bagi para pegawainya dengan penggunaannya hanya diperbolehkan untuk keperluan pekerjaan dan operasional Kementerian PPN/Bappenas.

2) Pengguna aset dilarang untuk melakukan perubahan terhadap perangkat keras ataupun perangkat lunak (*software*) tanpa persetujuan dari pimpinan Kementerian PPN/Bappenas.
3) Pengguna aset bertanggung jawab atas pengamanan dan perlindungan terhadap aset baik dari sisi fisik ataupun kendali akses logikal.
4) Setiap proses instalasi perangkat lunak (*software*) pada PC dan/atau Notebook harus mengikuti ketentuan pengelolaan perangkat lunak.
5) Pegawai dan pengguna pihak eksternal yang menggunakan atau memiliki akses ke aset Kementerian PPN/Bappenas harus mengetahui persyaratan keamanan informasi dari aset yang terkait dengan informasi, serta fasilitas dan sumber daya pemrosesan informasi.
6) Pegawai dan pengguna pihak eksternal harus bertanggung jawab atas penggunaan sumber daya pemrosesan informasi apapun dan untuk penggunaan semacam itu yang dilakukan di bawah tanggung jawabnya.

b. Aset Pribadi
1) Penggunaan aset pribadi untuk keperluan pekerjaan dan operasional Kementerian PPN/Bappenas, mengikuti ketentuan yang telah ditetapkan terkait penggunaan aset pribadi.
2) Aset pribadi yang akan digunakan untuk keperluan pekerjaan dan operasional Kementerian PPN/Bappenas harus:
    a) Memperoleh persetujuan dari atasan pegawai yang bersangkutan;
    b) dilaporkan kepada Tim Manajemen Aset dan Risiko untuk dicatat dalam Asset Register (aset Non Kementerian PPN/Bappenas);
    c) mengikuti seluruh ketentuan standar keamanan informasi yang berlaku di Kementerian PPN/Bappenas.
3) Pengamanan dan perlindungan serta segala risiko dan biaya yang ditimbulkan terkait penggunaan aset pribadi menjadi tanggung jawab dari pemilik aset pribadi tersebut.

4) Aset atau perangkat milik pribadi dapat digunakan di lingkungan Kementerian PPN/Bappenas tanpa harus terikat dengan aturan ketentuan standar keamanan informasi di Kementerian PPN/Bappenas selama perangkat tersebut:
   a) Tidak digunakan untuk keperluan pekerjaan dan operasional Kementerian PPN/Bappenas;
   b) Tidak menggunakan fasilitas dan/atau mengakses jaringan internet/intranet Kementerian PPN/Bappenas;
   c) Tidak mengakses dan/atau menyimpan informasi sensitif (rahasia dan/atau internal) milik Kementerian PPN/Bappenas;
   d) Tidak menggunakan akses USB, External Storage (*removable media*); dan penggunaannya tidak mengganggu kelancaran kegiatan proses pekerjaan dan operasional di Kementerian PPN/Bappenas.
5) Tim Manajemen Aset dan Risiko bertanggung jawab untuk memantau penggunaan aset pribadi dan kesesuaiannya dengan ketentuan standar keamanan informasi yang berlaku di Kementerian PPN/Bappenas.

c. Aset Milik Pihak Ketiga
1) Aset milik pihak ketiga yang digunakan untuk kebutuhan pekerjaan dan operasional Kementerian PPN/Bappenas harus disertai dengan perjanjian/kesepakatan formal mengenai penggunaan, pengelolaan, dan pemeliharaan aset serta hak dan kewajiban dari masing-masing pihak.
2) Perjanjian tersebut harus memuat persyaratan bahwa penggunaan aset milik pihak ketiga juga harus mengikuti seluruh ketentuan terkait aset yang tercantum pada kebijakan dan prosedur Kementerian PPN/Bappenas yang berlaku.
3) Dokumentasi terkait pengelolaan aset milik pihak ketiga harus dipelihara dan ditinjau secara berkala.

4. Pengembalian dan Penggunaan Kembali Aset
a. Seluruh aset milik Kementerian PPN/Bappenas harus dikembalikan apabila pegawai pengguna aset yang bersangkutan:
1) Tidak lagi memiliki hubungan kepegawaian (berhenti) dari Kementerian PPN/Bappenas;

2) Mendapatkan penugasan lain (mutasi/promosi) diluar Kementerian PPN/Bappenas; dan
3) Akan mengajukan cuti atau ijin dengan jangka waktu lebih dari 1 (satu) bulan.

b. Untuk setiap aset yang dikembalikan, harus diperhatikan mengenai hal-hal sebagai berikut:
1) Proses serah terima aset harus terdokumentasi secara formal.
2) Informasi yang terdapat pada aset harus diamankan dengan cara:
a) Melakukan backup informasi;
b) Menyimpan data backup ke hardisk eksternal; dan kemudian
c) Menghapus informasi dari aset secara aman (antara lain dengan Secure Format atau instalasi ulang sistem operasi secara menyeluruh).

c. Tim Manajemen Aset dan Risiko bertanggung jawab untuk memastikan bahwa seluruh proses tersebut telah dilaksanakan secara memadai.

d. Pengelolaan dan penyimpanan aset yang telah dikembalikan namun belum dialokasikan kembali kepada pegawai pengguna lainnya menjadi tanggung jawab Tim Manajemen Aset dan Risiko.

e. Untuk setiap aset yang akan dialokasikan kembali kepada pegawai pengguna lainnya, harus diperhatikan hal-hal sebagai berikut:
1) Memastikan bahwa aset tersebut tidak memuat informasi yang sensitif yang bukan menjadi hak dari pegawai pengguna lainnya tersebut.
2) Proses serah terima aset harus terdokumentasi secara formal.

f. Tim Manajemen Aset dan Risiko bertanggung jawab untuk melakukan pengkinian status informasi pengguna aset pada dokumentasi identifikasi dan inventarisasi aset ketika terdapat proses pengembalian dan/atau penggunaan kembali aset untuk pegawai pengguna lainnya.

g. Semua peralatan yang mengandung media penyimpanan harus diverifikasi untuk menjamin bahwa data rahasia dan perangkat lunak berlisensi apapun sudah dihapus atau ditimpa secara aman sebelumnya untuk dibuang/disposal atau dipergunakan kembali.

h. Semua pegawai dan pengguna pihak eksternal harus mengembalikan semua aset Kementerian PPN/Bappenas yang dikuasainya ketika terjadi penghentian kerja, kontrak atau perjanjian mereka.

5. Pemeliharaan Aset
   a. Pemeliharaan preventif dan korektif (pemeliharaan rutin) harus dilakukan secara berkala sesuai dengan prasyarat dari produsen aset untuk menjamin daya tahan penggunaan dari perangkat. Hal ini juga mencakup mengenai kepastian dalam layanan purna jual dan suku cadang.
   b. Jika proses pemeliharaan rutin/preventif diserahkan kepada pihak ketiga, maka harus dipilih penyedia jasa yang kompeten dan relevan, dengan pengelolaan hubungan kerja mengikuti ketentuan pada bagian hubungan pemasok.
   c. Setiap aset yang mengalami gangguan dan/atau kerusakan harus segera dilaporkan kepada Tim Manajemen Aset dan Risiko untuk dilakukan pemeriksaan dan tindak lanjut penanganan.
   d. Apabila terdapat aset/ perangkat yang akan dibawa keluar area Kementerian PPN/Bappenas dan/ atau diserahkan kepada Pihak Ketiga untuk pemeliharaan atau perbaikan, maka harus dipastikan bahwa telah dilakukan pengamanan yang memadai terhadap informasi yang tersimpan di media penyimpan informasi pada aset/ perangkat.
   e. Pelaksanaan proses terkait pemeliharaan aset harus didokumentasikan.
   f. Tim Manajemen Aset dan Risiko bertanggung jawab untuk koordinasi pelaksanaan dan pemantauan proses pemeliharaan aset.
6. Perlindungan dan Pengamanan Aset
   a. Pengguna aset bertanggung jawab atas perlindungan dan pengamanan selama aset tersebut berada dibawah pengawasan dan digunakan oleh pengguna aset tersebut.
   b. Setiap kejadian insiden terkait aset harus segera dilaporkan kepada operator helpdesk dan Koordinator Tim Manajemen TIK.
   c. Perangkat dan aset pengolah/pemroses informasi harus diletakkan sedemikian rupa secara aman untuk mengurangi risiko dari ancaman lingkungan atau akses yang tidak terotorisasi.
   d. Perangkat dan aset pengolah/pemroses informasi harus diberikan perlindungan yang memadai dari gangguan

sumber daya dan/atau gangguan yang disebabkan oleh kerusakan pada fasilitas pendukung.

e. Peralatan, informasi atau perangkat lunak tidak boleh dibawa keluar lokasi tanpa izin yang berwenang.

f. Jalur kabel daya dan kabel data/komunikasi harus ditata dan diberikan perlindungan yang memadai agar terlindungi dari risiko kerusakan fisik serta gangguan interferensi dan intersepsi. Jika dimungkinkan, harus dibuat jalur yang terpisah antara kabel daya dan kabel data/komunikasi.

g. Aset perangkat komputer (PC) dan Notebook yang akan ditinggalkan penggunanya, harus diberikan perlindungan dan pengamanan yang memadai untuk menghindari risiko akses yang tidak terotorisasi dengan cara sebagai berikut:
   1) Memastikan bahwa komputer (PC) dan Notebook telah diberikan pengamanan akses logical dengan kata sandi yang sesuai ketentuan yang berlaku di Kementerian PPN/Bappenas.
   2) Menonaktifkan atau mengunci layar (dengan mengaktifkan Screensaver Lock) komputer dan Notebook jika akan ditinggalkan dalam waktu yang lama.
   3) Menjamin bahwa peralatan yang tidak diawasi memiliki perlindungan yang layak.
   4) Untuk aset perangkat notebook yang akan dibawa keluar area kantor Kementerian PPN/Bappenas, maka harus dilakukan langkah perlindungan dan pengamanan sebagai berikut:
      a) Memastikan bahwa Notebook telah diberikan pengamanan akses logikal dengan kata sandi sesuai dengan ketentuan yang berlaku di Kementerian PPN/Bappenas.
      b) Tidak meninggalkan Notebook di area publik dan/atau di dalam kendaraan dalam keadaan tidak terjaga. Jika diharuskan untuk meninggalkan Notebook, menyimpan Notebook di tempat yang aman seperti *Safe Deposit Box* atau loker yang terkunci atau gunakan alat pengaman fisik seperti *cable lock*.
      c) Jika terdapat aset Kementerian PPN/Bappenas yang ditempatkan di lokasi Pihak Ketiga atau sebaliknya, maka kewajiban pengamanan aset tersebut menjadi tanggung jawab pihak dimana

aset ditempatkan dan diatur dalam surat perjanjian formal.

7. Pemusnahan dan Penghapusan Aset
   a. Aset dapat dimusnahkan apabila aset tersebut:
      1) fungsinya telah digantikan oleh aset/perangkat yang lebih baru; dan
      2) mengalami kerusakan dan tidak memungkinkan untuk dapat diperbaiki dan/atau digunakan kembali.
   b. Pemusnahan aset harus memperoleh persetujuan dari Penanggung Jawab Kementerian PPN/Bappenas.
   c. Sebelum pelaksanaan pemusnahan (disposal) dan/atau penghapusan aset, harus dilakukan pengamanan terhadap informasi yang tersimpan di media penyimpanan pada aset, dengan langkah-langkah sebagai berikut:
      1) Melakukan *backup* terhadap seluruh informasi yang tersimpan pada aset.
      2) Setelah dilakukan *backup*, hapus seluruh informasi secara aman, misalnya dengan *secure format*.
      3) Menghapus dan/atau memindahkan lisensi perangkat lunak dari aset.
   d. Untuk aset dengan media penyimpan informasi yang telah mengalami kerusakan permanen dan/atau tidak lagi dapat diakses secara logikal, maka harus dilakukan pemusnahan fisik secara aman untuk memastikan bahwa informasi didalamnya tidak lagi dapat diakses oleh pihak yang tidak berwenang. Contoh: Hardisk yang rusak dimusnahkan dengan cara melubangi piringan penyimpan data dengan menggunakan bor listrik.
   e. Untuk proses penghapusan aset mengikuti ketentuan peraturan pemerintah mengenai pengelolaan aset barang milik negara.
   f. Proses pemusnahan dan penghapusan aset harus didokumentasikan.

F. Kontrol Akses
   1. Hak Akses Pengguna
      a. Seluruh proses pemberian atau perubahan hak akses harus berdasarkan permintaan dari Pengguna atau unit kerja terkait.
      b. Seluruh proses pemberian atau perubahan hak akses harus terdokumentasi dengan baik.
      c. Kriteria Akses Pengguna pada Aplikasi/*Software*

1) Pengguna dapat berasal dari internal Kementerian PPN/Bappenas atau eksternal (Pihak Ketiga).
2) Aplikasi/*Software* yang akan diatur hak akses User-nya adalah aplikasi yang sudah divalidasi sesuai ketentuan.
3) Pemberian hak Akses User (baru/ hapus/ ubah role/ reset kata sandi) pada Aplikasi berpedoman pada Aplikasi/ *Software* yang terdaftar di masing-masing Unit Kerja dan *User Access Matrix* (UAM) yang sudah diterima dari Unit Kerja.
4) *User Access Matrix* (UAM) dibuat oleh Pengguna dengan ketentuan:
    a) Pengguna yang ditunjuk adalah pegawai yang memiliki *job description*, kualifikasi dan pelatihan penggunaan Software/Aplikasi yang akan dioperasikannya;
    b) *Role User* yang diberikan merujuk kepada User Manual Aplikasi, mempertimbangan prinsip-prinsip *Segregation of Duties* (SoD), *job description* Pengguna serta kompetensi Pengguna yang ditunjuk.
5) Secara umum *Role User* pada Aplikasi adalah:
    a) Administrator ditunjuk oleh koordinator tim terkait berwenang penuh dalam pelaksanaan setting hak Akses User (baru, hapus, perubahan Role, hak akses sementara, reset Kata Sandi);
    b) Admin User (khusus untuk Software terkait peralatan) yang ditunjuk oleh Koordinator Tim terkait, berwenang penuh untuk konfigurasi *software*, misalnya setting metode dan parameter uji;
    c) Operator yang ditunjuk oleh koordinator tim terkait atau surat tugas dari pimpinan, berwenang penuh untuk entri/input data; dan
    d) Reviewer/Validator/Conform/Approver ditunjuk dengan surat tugas dari Pimpinan yang berwenang penuh untuk mereview atau menyetujui data yang telah diinput oleh operator.
6) Setiap perubahan posisi jabatan pegawai harus diinformasikan oleh Biro SDM dan pimpinan unit kerja pegawai/pengguna ke Pusdatinrenbang untuk dapat dilakukan penyesuaian hak akses pada aplikasi terkait.

d. Pembaharuan, Penghapusan, Perubahan Role, Hak Akses Sementara
   1) Penambahan pengguna baru diberikan kepada pegawai baru sesuai kriteria yang ditentukan pada ketentuan *User Access Matrix*.
   2) Penghapusan hak Akses User secara permanen:
      a) Pengguna berhenti dari Kementerian PPN/Bappenas atau meninggal;
      b) Pengguna yang sudah tidak diberi kewenangan untuk akses ke Aplikasi karena sudah berubah *job description*-nya atau dicabut; dan
      c) Pengguna yang sudah berakhir hak akses sementaranya.
   3) Perubahan *Role User* berlaku untuk Pengguna dengan posisi jabatan yang sama dan unit kerja yang sama. Jika perubahan Role tersebut berbeda dengan User Manual atau berisiko melanggar *Segregation of Duties* (SoD) maka perlu dibuat kajian untuk memastikan bahwa risiko dapat dimitigasi.
   4) Pemberian hak Akses User sementara:
      a) Adanya pegawai kontrak yang dikontrak langsung oleh Kementerian PPN/Bappenas dan diusulkan menjadi Pengguna.
      b) Terjadi pendelegasian wewenang kepada pegawai lain sehubungan Pengguna untuk sementara tidak dapat menggunakan hak aksesnya pada *Software*/Aplikasi karena sakit, cuti, dinas, sibuk sementara proses Kementerian PPN/Bappenas harus berjalan, berdasarkan permintaan atasan Pengguna atau surat pendelegasian wewenang.
      c) Pihak Ketiga yang dalam lingkup pekerjaannya membutuhkan akses ke Aplikasi/*Software*.
      d) Jangka waktu dibatasi sesuai dengan masa perjanjian/ kontrak/ surat tugas/ surat pendelegasian wewenang atau keperluan Pengguna.
      e) Jika pemberian hak Akses User sementara tersebut berbeda dengan Role dalam user manual atau berisiko melanggar *Segregation of Duties* (SoD), maka perlu dibuat kajian untuk memastikan bahwa risiko dapat dimitigasi.

2. Hak Akses Intranet, Internet dan VPN
   a. Hak akses Internet ada 2 (dua), internal (intranet) dan eksternal.
   b. Hak akses Intranet diberikan kepada pimpinan, pegawai tetap dan tidak tetap yang dikontrak langsung oleh Kementerian PPN/Bappenas.
   c. Hak akses Internet diberikan kepada:
      1) Menteri PPN/Kepala Bappenas, Sekretaris Kementerian PPN/Sekretaris Utama Bappenas;
      2) Deputi bidang terkait;
      3) Direktur bidang terkait;
      4) Kepala Biro bidang terkait;
      5) Kepala Pusat bidang terkait;
      6) Pegawai setingkat Koordinator dan Wakil Koordinator;
      7) Pegawai setingkat Kepala Seksi, Staf, dan Non Staf dengan alasan khusus; dan
      8) Pihak Ketiga dengan pembatasan, terkait dengan pelaksanaan pekerjaan.
   d. Akses informasi ke internet yang tidak berhubungan dengan pekerjaan dibatasi dengan menetapkan beberapa situs Internet yang secara default tidak dapat diakses oleh Pengguna, misalnya situs multimedia, atau situs sosial media, dan situs lain yang sejenis. Jika situs-situs tersebut diperlukan untuk memperlancar pekerjaan, dapat diajukan secara tertulis ke Pusat Data dan Informasi Perencanaan Pembangunan.
   e. Untuk keperluan khusus, seperti giat khusus/*event*, *online meeting*/*collaboration* atau yang lain yang sejenis, dimana memerlukan bandwidth internet yang lebih besar maka dimungkinkan penambahan bandwidth internet dan bersifat sementara, dengan mengajukan permintaan secara tertulis ke Pusat Data dan Informasi Perencanaan Pembangunan.
   f. Fasilitas VPN diberikan kepada Pengguna internal di Kementerian PPN/Bappenas atau Pihak Ketiga dengan ketentuan:
      1) Akses VPN internal diberikan kepada Pengguna tertentu sesuai *job description* yang dalam pekerjaannya membutuhkan koneksi dengan jaringan komputer saat berada di luar koneksi jaringan komputer Kementerian PPN/Bappenas dengan permintaan secara tertulis ke Pusat Data dan Informasi Perencanaan Pembangunan.

2) Akses VPN Pihak Ketiga diberikan kepada pihak di luar Kementerian PPN/Bappenas yang dalam lingkup pekerjaannya membutuhkan akses VPN ke aset TI dengan jangka waktu dibatasi sesuai dengan masa perjanjian/kontrak / surat tugas.

g. Pengguna yang diberi hak akses Intranet dan/ atau Internet dan VPN hanya digunakan untuk kepentingan Kementerian PPN/Bappenas.

h. Setiap Pengguna tidak diperkenankan mengakses, mengunggah, mengunduh, mendistribusikan materi dari internet sebagai berikut:
   1) Politik, ilegal, kriminal, materi yang mengandung pemahaman seksual, pesan/lampiran ilegal, hal tidak senonoh, memfitnah / menghina, diskriminasi (usia, ras, gender, orientasi seksual, agama, politik), ujaran kebencian, dan materi yang melanggar hak cipta/kekayaan intelektual.
   2) Melakukan vandalisme atau perusakan properti individu atau organisasi lain.
   3) Menyerang atau penyalahgunaan privasi orang lain.
   4) Melanggar hak cipta atau penggunaan materi tanpa izin intelektual.
   5) Mengganggu performa jaringan.
   6) Menyebarkan virus, worm, trojan atau sejenisnya yang dapat merusak komputer lain.
   7) Mengakses *game online*.

i. Pegawai yang sudah pensiun atau tidak bekerja lagi maka hak akses intranet/internet langsung dinonaktifkan.

j. File hasil *download* dari situs yang berkaitan dengan pekerjaan menjadi milik Kementerian PPN/Bappenas, sedangkan untuk yang pribadi menjadi tanggung jawab dari pegawai yang bersangkutan.

k. Pusat Data dan Informasi Perencanaan Pembangunan bertanggung jawab untuk melakukan pengawasan terhadap aktivitas situs internet yang diakses.

l. Pusat Data dan Informasi Perencanaan Pembangunan bertanggung jawab untuk menyediakan layanan Internet, Intranet, dan VPN untuk mendukung Kementerian PPN/Bappenas termasuk di dalamnya adalah untuk meningkatkan produktivitas kerja Kementerian PPN/Bappenas.

m. Jika dalam penggunaan Internet dan VPN ditemukan adanya kejanggalan yang dapat menyebabkan kerugian bagi Kementerian PPN/Bappenas maka:
   1) Pusat Data dan Informasi Perencanaan Pembangunan harus mengklarifikasi kepada Pengguna yang bersangkutan;
   2) Jika hasil klarifikasi tidak dapat diterima, Pusat Data dan Informasi Perencanaan Pembangunan akan menginformasikan secara tertulis kepada pimpinan dari Pengguna tersebut untuk diberikan pembinaan; dan
   3) Jika Pengguna tidak dapat dibina, pimpinan dari Pengguna melaporkan secara tertulis ke Biro SDM untuk diberikan sanksi sesuai aturan Kementerian PPN/Bappenas.

3. Kata Sandi
   a. Kata sandi harus mengikuti aturan penggunaan kata sandi yaitu:
      1) Jumlah karakter kata sandi minimal berjumlah 8 (delapan) karakter.
      2) Tidak berasal dari karakter yang mudah ditebak seperti nama diri atau keluarga, tanggal lahir, alamat rumah, lokasi kerja, dan hal lain yang berhubungan dengan pribadi pemilik kata sandi.
      3) Menggunakan kombinasi huruf besar, huruf kecil, angka, dan sedapat mungkin menggunakan tanda baca dan karakter khusus (special character), seperti: !$%#*, kecuali apabila perangkat atau aplikasi tidak memungkinkan.
   b. Administrator harus segera merubah kata sandi Administrator apabila:
      1) Umur kata sandi sudah mendekati 3 (tiga) bulan.
      2) Terjadi penggunaan kata sandi oleh Administrator pengganti dalam keadaan mendesak.
   c. Kata Sandi Administrator dapat diserahkan kepada pegawai pengganti apabila:
      1) Terjadi pergantian pegawai yang ditunjuk sebagai Administrator.
      2) Dalam keadaan mendesak (*urgent*) Administrator berhalangan hadir sehingga tidak dapat membuka akses ke dalam sistem, aplikasi, atau database.

d. Setiap pegawai pengguna dan operator harus mengganti kata sandi paling lama setiap 3 (tiga) bulan sekali.

G. *Cryptography*

1. Teknik kriptografi yang akan digunakan Kementerian PPN/Bappenas harus mendapatkan persetujuan dari Pusdatinrenbang Kementerian PPN/Bappenas.
2. Seluruh kunci kriptografi harus dilindungi dari kerusakan, modifikasi, atau kehilangan dengan cara:
   a. Hanya didistribusikan kepada Pengguna yang dikehendaki;
   b. Mengubah atau mengganti kunci bila diduga telah disalahgunakan;
   c. Membatasi masa berlaku kunci; dan
   d. Disimpan oleh Koordinator Tim Manajemen TIK, Koordinator Tim Keamanan Informasi, Koordinator Tim Aplikasi Pusdatinrenbang.

H. Keamanan Fisik dan Lingkungan

1. Akses Fisik ke Ruang Kerja
   a. Seluruh pegawai dan pihak ketiga yang memasuki ruang kerja Pusdatinrenbang Kementerian PPN/Bappenas harus mengenakan kartu identitas (*ID Card*) yang berlaku.
   b. Ruang kerja Pusdatinrenbang Kementerian PPN/Bappenas harus diberi pengamanan fisik yang memadai, baik dengan sistem akses pintu elektronik untuk melindungi dari akses fisik secara tidak berwenang, petugas keamanan, alarm, alat pemadam kebakaran, dan alat perlindungan lainnya.
   c. Pihak ketiga yang memasuki ruang kerja Pusdatinrenbang Kementerian PPN/Bappenas harus mengisi buku tamu, mencatat waktu masuk dan keluar.
   d. Ruangan yang dapat diakses publik, termasuk area keluar-masuk barang harus dipantau dari penyalahgunaannya sebagai sarana akses ke ruang lain yang sensitif.
2. Keamanan Perangkat
   a. Perangkat komputer, perangkat komunikasi (*network*), facsimile, telepon, mesin fotocopy, dan fasilitas pengolah informasi lainnya harus ditempatkan di lokasi yang jauh dari risiko kebakaran, kebocoran, banjir, pencurian, dan bahaya lingkungan lainnya. Penempatan perangkat sebagaimana disebutkan di atas harus diposisikan sedemikian rupa sehingga terhindar dari akses oleh pihak yang tidak berwenang.

b. Ruangan yang menyimpan perangkat TI yang kritikal harus dilindungi dari kemungkinan gangguan atau ketidakstabilan aliran listrik dengan memasang *Uninterruptible Power Supply* (UPS) yang kapasitasnya memadai. Perangkat UPS harus secara berkala diperiksa dan diuji.

c. Jalur kabel listrik dan kabel telekomunikasi harus diberi perlindungan fisik untuk mencegah kerusakan terjadinya korsleting. Jika dimungkinkan ditempatkan di dalam tanah, di atas langit-langit, di dalam dinding, atau lokasi lain yang tertutup dari penglihatan umum.

d. Perangkat TI dan perangkat pendukungnya harus dirawat oleh pegawai yang kompeten atau oleh vendor terkait. Rekaman tindakan pencegahan dan perbaikan perangkat TI harus dipelihara untuk meningkatkan efektivitas pengelolaan dan perawatan.

e. Perangkat TI dan *software* yang digunakan di luar kantor harus dilindungi secara fisik maupun lojik dari segala risiko yang mengancam keamanan informasi, meliputi:

   1) Perangkat TI dan media penyimpan informasi yang tidak digunakan lagi, akan dilelang, disumbangkan, atau dihancurkan, harus dipastikan tidak menyimpan informasi berklasifikasi Rahasia Tercatat, Rahasia Terbatas, dan Rahasia. Tim Manajemen TIK dan Tim Keamanan Informasi Pusdatinrenbang harus memastikan bahwa informasi yang disimpan dalam perangkat tersebut telah dihapus sehingga tidak dapat diakses Kembali.

   2) Pemindahan perangkat TI, software termasuk media penyimpan informasi keluar lokasi kerja harus mendapat ijin dari Koordinator Manajemen TIK dan Koordinator Keamanan Informasi Pusdatinrenbang Kementerian PPN/Bappenas.

3. Pemantauan Keamanan Fisik

   a. Tempat fisik harus dipantau oleh sistem pengawasan, yang dapat mencakup penjaga, penyusup alarm, sistem pemantauan video seperti televisi sirkuit tertutup dan informasi keamanan fisik perangkat lunak manajemen baik dikelola secara internal atau oleh penyedia layanan pemantauan.

   b. Akses ke bangunan yang menampung sistem kritis harus terus dipantau untuk mendeteksi pihak yang tidak berwenang akses atau perilaku mencurigakan dengan:

1) Memasang sistem pemantauan video seperti televisi sirkuit tertutup untuk melihat dan merekam akses area sensitif di dalam dan di luar lokasi Kementerian PPN/Bappenas;
2) Memasang, sesuai dengan standar relevan yang berlaku, dan secara berkala menguji kontak, suara atau detektor gerakan untuk memicu alarm penyusup seperti:
   i. Memasang detektor kontak yang memicu alarm ketika kontak dibuat atau rusak di sembarang tempat di mana kontak dapat dibuat atau rusak (seperti jendela dan pintu dan benda di bawahnya) untuk digunakan sebagai alarm panik;
   ii. Pendeteksi gerakan berbasis teknologi infra merah yang dapat mendeteksi/memicu alarm ketika ada objek yang melewati area yang ditentukan;
   iii. Memasang sensor yang peka terhadap suara kaca pecah yang dapat digunakan untuk memicu alarm untuk mengingatkan petugas keamanan;
3) Menggunakan alarm tersebut untuk menutup semua pintu luar dan jendela yang dapat diakses. Daerah yang tidak berpenghuni seharusnya khawatir setiap saat; penutup juga harus disediakan untuk area lain (misalnya komputer atau komunikasi kamar).

c. Rancangan sistem pemantauan harus dirahasiakan karena pengungkapan dapat memudahkan pembobolan yang tidak terdeteksi.
d. Sistem pemantauan harus dilindungi dari akses yang tidak sah untuk mencegah pengawasan informasi, seperti umpan video, agar tidak diakses oleh orang atau sistem yang tidak berwenang dinonaktifkan dari jarak jauh.
e. Panel kontrol sistem alarm harus ditempatkan di zona waspada dan, untuk alarm keselamatan, di suatu tempat yang memungkinkan rute keluar yang mudah bagi orang yang menyetel alarm. Panel kontrol dan detektor harus memiliki mekanisme tamperproof. Sistem harus diuji secara teratur untuk memastikannya berfungsi sebagaimana mestinya, terutama jika komponennya bertenaga baterai.
f. Setiap mekanisme pemantauan dan pencatatan harus digunakan dengan mempertimbangkan hukum setempat dan peraturan termasuk perlindungan data dan undang-

undang perlindungan PII, terutama tentang pemantauan pegawai dan periode retensi video yang direkam.

I. Keamanan Operasional

1. Pengendalian dan pemantauan lingkungan operasional
   a. Tanggung jawab penyelenggaraan dan pengelolaan TI didefinisikan dalam struktur organisasi Pusat Data dan Informasi Perencanaan Pengembangan Kementerian PPN/Bappenas dengan mempertimbangkan pemisahan tugas untuk mengurangi risiko kesalahan penggunaan sistem, baik secara sengaja atau tidak.
   b. Perubahan terhadap fasilitas dan sumber daya TI di lingkungan operasional yang dikelola Pusat Data dan Informasi Perencanaan Pengembangan Kementerian PPN/Bappenas seperti: sistem operasi, konfigurasi server, perangkat network, dan aplikasi harus mendapat persetujuan dari Koordinator Manajemen TIK di Pusat Data dan Informasi Perencanaan Pengembangan Kementerian PPN/Bappenas.
   c. Untuk mengurangi risiko terjadinya perubahan yang tidak terkendali terhadap aplikasi, fasilitas TI untuk pengembangan dan pengujian (*testing*) dipisahkan dari fasilitas untuk operasional.
2. *IT Change Management*
   a. Hal yang perlu diperhatikan dalam pelaksanaan *IT Change Management* adalah sebagai berikut:
      1) Parameter *review* untuk persetujuan pengajuan *Change Request* antara lain:
         i. Latar belakang perubahan.
         ii. Tujuan perubahan.
         iii. Dampak dan risiko dari perubahan.
         iv. Keselarasan dengan inisiatif strategis TI.
         v. Ketersediaan budget yang sesuai dengan peruntukannya.
         vi. Ketersediaan sumber daya.
         vii. Berada dalam ruang lingkup atau batasan *Change Request*.
      2) Penilaian analisis prioritas atau kritikalitas *Change Request* dilakukan dengan mempertimbangkan aspek-aspek sebagai berikut:
         i. Infrastruktur atau aplikasi dipergunakan secara *enterprise* atau,

ii. Infrastruktur atau aplikasi dengan kategori *Very Critical* atau,
iii. Infrastruktur atau aplikasi yang mendukung sistem yang melibatkan pihak ketiga atau,
iv. Infrastruktur atau aplikasi yang mendukung sistem karakteristik *face-public* internet atau diakses langsung oleh pengguna atau,
v. Infrastruktur atau aplikasi yang mendukung sistem untuk produk dan aktivitas baru atau,
vi. Terkait dengan *regulatory*.

b. Melakukan penyusunan rencana implementasi perubahan, yaitu proses pemahaman permasalahan dan kebutuhan untuk menentukan solusi yang dapat dikembangkan dan mendeskripsikan fungsional infrastruktur yang akan dikembangkan. Kemudian proses pengumpulan informasi mengenai tujuan pengembangan infrastruktur, hasil yang diinginkan, dan bagaimana infrastruktur akan digunakan.
c. Pengajuan *Change Request* dilakukan dengan mengisi formulir *Change Request* dan melampirkan *Change Management Form.*

3. *IT Configuration Management*
   a. Konfigurasi perangkat TI harus distandarisasi untuk memudahkan pengelolaan dan perawatan sistem terkait.
   b. Pengelolaan konfigurasi perangkat TI harus melindungi perangkat TI dari ancaman eksploitasi teknis terhadap kelemahan yang diakibatkan oleh kesalahan konfigurasi sistem.
   c. Standarisasi konfigurasi perangkat TI oleh Pusdatinrenbang dan pelaksanaannya dilakukan oleh Tim Manajemen TIK.
   d. Backup hasil konfigurasi dilakukan kedalam 1 (satu) server minimal sebulan sekali.
4. *Capacity Management*
   a. Perencanaan Kapasitas
      1) Informasi mengenai performa harus dikumpulkan dan dicatat atau didokumentasikan dalam suatu periode yang telah ditentukan.
      2) Pusat Data dan Informasi Perencanaan Pengembangan harus melakukan perencanaan kebutuhan kapasitas sumber daya TI di masa depan berdasarkan analisis saat ini dan data historis sebelumnya dan menentukan ambang batas dari masing-masing sumber daya yang ada.

3) Perencanaan kapasitas hendaknya disusun untuk jangka waktu cukup panjang yakni dalam kurun waktu 5 (lima) tahun dan selalu diperbarui untuk mengakomodir perubahan yang ada.
4) Kebutuhan dalam perencanaan kapasitas mengacu kepada dokumen Rencana Strategis Teknologi Informasi (*IT Master Plan*).
5) Dalam perencanaan kapasitas harus dilakukan analisis dari faktor internal maupun faktor eksternal yang dapat mempengaruhi kebutuhan Kementerian PPN/Bappenas.

b. Monitoring Kapasitas
1) Penggunaan sumber daya TI harus diawasi dan dilakukan perkiraan kebutuhan kapasitas di masa mendatang untuk memastikan tercapainya kinerja sistem yang dibutuhkan.
2) Pengawasan terhadap kapasitas sumber daya TI harus dilakukan secara rutin dan didokumentasikan dengan melihat ambang batas yang telah ditentukan.
3) Pengawasan kapasitas yang dilakukan tidak terbatas pada kapasitas penyimpanan, utilisasi server dan utilisasi jaringan.
4) Monitoring kapasitas harus dilakukan secara rutin dan didokumentasikan.
5) Hasil monitoring kapasitas harus disetujui oleh Koordinator Tim Manajemen TIK.

5. *System Planning dan Acceptance*
a. Koordinator manajemen aplikasi di Kementerian PPN/Bappenas memantau dan mengatur penggunaan sumber daya informasi seperti bandwidth, server, storage, kecepatan prosesor, lisensi software dan merencanakan kebutuhan ke depan untuk menjamin kinerja sistem pada tingkat yang diharapkan.
b. Setiap sistem TI baru, *upgrade* atau berubah versi harus memenuhi kriteria penerimaan yang ditetapkan Koordinator Manajemen TIK di Kementerian PPN/Bappenas, sebelum dapat dioperasikan di lingkungan operasional. Kriteria penerimaan meliputi, tetapi tidak terbatas pada:
1) Kesesuaian dengan spesifikasi dan kebutuhan Kementerian PPN/Bappenas;
2) Penerapan kendali keamanan yang diperlukan;

3) Kecukupan teknis: persyaratan kinerja dan kapasitas komputer;
4) Tersedianya prosedur *error recovery* and *fallback arrangement*;
5) Telah menjalani serangkaian pengujian yang komprehensif;
6) Tersedianya *user manual* dan/ atau operator manual; dan
7) Diberikannya pelatihan untuk mengoperasikan sistem tersebut.

6. Perlindungan terhadap *Virus/Malware*
   a. *Software anti-virus* harus dipasang dan diperbarui secara reguler untuk mencegah dan mendeteksi adanya virus ke dalam lingkungan komputer.
   b. Setiap komputer yang terinfeksi virus harus segera diisolasi atau diputuskan sambungannya dari jaringan komputer. Komputer tersebut tidak akan disambung ke jaringan kembali sebelum virus dapat dihilangkan.
   c. Pengguna harus melaporkan ke Petugas HelpDesk Pusdatinrenbang bila mendeteksi adanya virus, mengalami atau melihat terjadinya perubahan konfigurasi secara tiba-tiba, atau adanya perilaku aplikasi atau komputer yang tidak wajar.
7. *Backup* dan *Restore*
   a. Pusdatinrenbang di Kementerian PPN/Bappenas bertanggung jawab menyediakan *File Server* atau NAS sebagai tempat menyimpan file pekerjaan dan backup data; dan melakukan *backup* data yang tersimpan pada komputer server secara berkala.
   b. Pemilik data bertanggungjawab untuk menentukan jenis data/informasi dan masa retensinya yang akan disimpan pada *File Server*.
   c. Pemilik data bertanggung jawab untuk melakukan *backup* yang sudah ditentukan dan menghapusnya setelah masa retensi berakhir.
   d. Jika diperlukan sesuai kebutuhan Kementerian PPN/Bappenas, data yang dianggap tidak digunakan lagi, dapat dilakukan proses archive oleh Pusdatinrenbang Kementerian PPN/Bappenas.
   e. Data hasil *backup* (data operasional, sistem, perangkat lunak) harus dilakukan pengujian (*restore*) oleh Tim Manajemen TIK Kementerian PPN/Bappenas untuk

memastikan *backup* tersebut dapat digunakan sesuai aslinya.

f. Media hasil backup harus disimpan pada lokasi yang terpisah dari lokasi operasional Kementerian PPN/Bappenas (jangan menyimpan pada Pusat Pengelolaan Teknologi Informasi) dan aman ketika terjadi keadaan yang tidak diinginkan (*force majeure*).

g. Pelaksanaan *Backup* data dilakukan oleh pegawai yang telah terkualifikasi.

h. Selama masa retensi, Tim Manajemen TIK di Kementerian PPN/Bappenas harus menjamin ketersediaan data yang dibackup di komputer server kapanpun dibutuhkan Pengguna.

i. Hasil *Backup*, *Archive*, dan *Restore* harus didokumentasikan.

8. Penanganan Media (*Media Handling*)

a. Media penyimpan informasi yang sudah tidak digunakan lagi harus segera dihancurkan agar tidak berpotensi penyalahgunaan informasi atau akses secara tidak berwenang.

b. Penghancuran media penyimpan informasi harus dilakukan hanya dengan metode penghancuran yang teruji.

c. Sistem dokumentasi yang mengandung informasi Rahasia Tercatat, Rahasia Terbatas, dan Rahasia harus dibatasi akses dan distribusinya, disimpan di tempat yang aman, dan dihancurkan jika tidak lagi digunakan.

d. Setiap penggunaan *removable media* harus dilakukan identifikasi dan dicatat sesuai dengan aliran proses yang berlaku.

e. Tidak menggunakan *removable media* (misal, DVD, HDD external atau USB) yang tidak diketahui pemiliknya ke perangkat pengguna.

f. Review pencatatan penggunaan dan pengakhiran *removable media* dapat dilakukan minimal 3 (tiga) bulan sekali.

g. Setiap pengakhiran penggunaan *removable media* harus dilakukan identifikasi dan dicatat sesuai dengan aliran proses yang berlaku.

9. Pertukaran Informasi

a. Pertukaran informasi dan software antara Kementerian PPN/Bappenas dengan pihak ketiga harus disertai perjanjian tertulis yang menetapkan syarat-syarat pertukaran secara aman.

b. Seluruh informasi Rahasia Tercatat, Rahasia Terbatas, dan Rahasia yang dikirim melalui email harus dipastikan alamat penerimanya tepat, tidak salah dan harus diberi kata sandi atau enkripsi.
c. Informasi yang disediakan bagi publik harus melalui proses verifikasi pemilik informasi, disetujui unit kerja yang berwenang, dan dilindungi keutuhannya dari modifikasi secara tidak berwenang

10. Layanan Aplikasi
    a. Layanan Aplikasi harus diberi perlindungan keamanan yang memadai dengan menerapkan metode pengamanan, antara lain:
        1) Menerapkan kombinasi sekurang-kurangnya 2 faktor otentikasi (*two factors authentication*) dengan penggunaan kata sandi, kartu chip magnetik, token, atau *digital signature*.
        2) Pemblokiran akses aplikasi jika Pengguna salah memasukkan kata sandi 3 (tiga) kali berturut-turut.
    b. Kementerian PPN/Bappenas harus memastikan penerapan prinsip kehati-hatian dalam penggunaan metode pengujian keaslian yang meliputi:
        1) Pengamanan pembuatan, validasi enkripsi kata sandi, dan metode pengujian keaslian lainnya.
        2) Pengamanan database pengujian keaslian aplikasi dari gangguan dan kerusakan secara sengaja ataupun tidak.
        3) Penambahan, penghapusan atau perubahan database pengujian keaslian harus diotorisasi oleh pihak yang berwenang.
11. Monitoring
    a. Audit log untuk server aplikasi harus diaktifkan dan hasil-hasilnya dipelihara selama periode waktu tertentu sebagai bukti atau rekaman penggunaan.
    b. Aktivitas *system administrator* dan operator juga harus di log. *System Administrator* dilarang menghapus atau menonaktifkan log aktivitasnya tanpa persetujuan dari Koordinator Keamanan Informasi.
    c. Informasi hasil log aktivitas harus dibatasi aksesnya dan disimpan dengan aman, baik dengan memberi kata sandi atau enkripsi.
    d. Pemantauan penggunaan sistem pengolah informasi harus dilakukan secara periodik untuk menjamin agar aktivitas

yang tidak berwenang tidak terjadi. Kegiatan ini harus menjamin pemeriksaan untuk:

1) Kegagalan akses (*access failures*).
2) Alokasi dan penggunaan hak akses khusus (*privileged access capability*).
3) Penelusuran aktivitas pada aplikasi.
4) Penggunaan sumber daya sensitif.

e. Sinkronisasi waktu seluruh server di Pusat Pengelolaan Teknologi Informasi dilakukan secara periodik dengan sumber waktu yang akurat dan disepakati (*time validation*).

12. Manajemen konfigurasi

a. Kementerian PPN/Bappenas harus mendefinisikan dan mengimplementasikan proses dan alat untuk menegakkan konfigurasi yang ditentukan (termasuk konfigurasi keamanan) untuk perangkat keras, perangkat lunak, layanan (misalnya layanan *cloud*) dan jaringan, untuk sistem yang baru dipasang serta untuk sistem operasional selama masa pakainya.
b. Peran, tanggung jawab, dan prosedur harus ada untuk memastikan kontrol yang memuaskan bagi semua perubahan konfigurasi.
c. Dimana template standar untuk konfigurasi perangkat keras, perangkat lunak, layanan, dan jaringan yang aman harus didefinisikan sebagai berikut:
    1) Menggunakan panduan yang tersedia untuk umum (mis. templat yang telah ditentukan sebelumnya dari vendor dan dari independen organisasi keamanan);
    2) Mempertimbangkan tingkat perlindungan yang diperlukan untuk menentukan tingkat keamanan yang memadai;
    3) Mendukung kebijakan keamanan informasi Kementerian PPN/Bappenas, kebijakan khusus topik, standar dan persyaratan keamanan lainnya;
    4) Mempertimbangkan kelayakan dan penerapan konfigurasi keamanan dalam konteks Kementerian PPN/Bappenas.
d. Template tersebut harus ditinjau secara berkala dan diperbarui saat dibutuhkan ancaman atau kerentanan baru untuk ditangani, atau ketika versi perangkat lunak atau perangkat keras baru diperkenalkan.

e. Berikut ini harus dipertimbangkan untuk membuat template standar untuk konfigurasi aman perangkat keras, perangkat lunak, layanan, dan jaringan:
   1) Meminimalkan jumlah identitas dengan hak akses tingkat istimewa atau administrator;
   2) Menonaktifkan identitas yang tidak perlu, tidak terpakai atau tidak aman;
   3) Menonaktifkan atau membatasi fungsi dan layanan yang tidak perlu;
   4) Membatasi akses ke program utilitas yang kuat dan pengaturan parameter *host*;
   5) Melakukan sinkronisasi jam;
   6) Mengubah informasi otentikasi *default* vendor seperti kata sandi default segera setelahnya instalasi dan meninjau parameter terkait keamanan *default* penting lainnya;
   7) Mengaktifkan fasilitas *time-out* yang secara otomatis mematikan perangkat komputasi setelah waktu yang ditentukan sebelumnya periode tidak aktif;
   8) Memverifikasi bahwa persyaratan lisensi telah dipenuhi.
f. Dimana Konfigurasi perangkat keras, perangkat lunak, layanan, dan jaringan yang telah ditetapkan harus dicatat dan hasil pencatatan harus dipertahankan dari semua perubahan konfigurasi, dimana catatan-catatan ini harus disimpan dengan aman. Ini bisa dicapai dengan berbagai cara, seperti database konfigurasi atau *template* konfigurasi. Pada saat adanya perubahan pada konfigurasi harus mengikuti proses manajemen perubahan.
g. Dalam melakukan pencatatan konfigurasi dapat berisi hal-hal yang relevan sebagai berikut:
   1) Pemilik terkini atau informasi kontak untuk aset;
   2) Tanggal perubahan konfigurasi terakhir;
   3) Versi template konfigurasi; dan
   4) Kaitannya dengan konfigurasi aset lainnya.
h. Konfigurasi harus dipantau dengan seperangkat alat manajemen sistem yang komprehensif (mis. utilitas pemeliharaan, dukungan jarak jauh, alat manajemen Organisasi, perangkat lunak pencadangan dan pemulihan) dan harus ditinjau secara berkala untuk memverifikasi pengaturan konfigurasi, mengevaluasi kekuatan kata sandi dan menilai kegiatan yang dilakukan. Konfigurasi aktual

dapat dibandingkan dengan target yang ditentukan template. Setiap penyimpangan harus diatasi, baik dengan penegakan otomatis dari target yang ditentukan konfigurasi atau dengan analisis manual penyimpangan diikuti dengan tindakan korektif.

13. Penghapusan informasi
    a. Informasi sensitif tidak boleh disimpan lebih lama dari yang diperlukan untuk mengurangi risiko yang tidak diinginkan penyingkapan. Dimana Saat menghapus informasi tentang sistem, aplikasi, dan layanan, hal-hal berikut harus dipertimbangkan:
        1) Memilih metode penghapusan (misalnya penimpaan elektronik atau penghapusan kriptografi) yang sesuai dengan persyaratan kementerian PPN/Bappenas dan mempertimbangkan hukum dan peraturan yang relevan;
        2) Membukukan hasil penghapusan sebagai bukti;
        3) Saat menggunakan penyedia layanan penghapusan informasi, memperoleh bukti penghapusan informasi dari mereka.
    b. Jika pihak ketiga menyimpan informasi Kementerian PPN/Bappenas atas namanya, Kementerian PPN/Bappenas harus mempertimbangkannya pencantuman persyaratan penghapusan informasi ke dalam perjanjian pihak ketiga untuk menegakkannya selama dan setelah penghentian layanan tersebut.
    c. Terkait dengan penyimpanan data dengan mempetimbangkan undang-undang dan peraturan yang relevan, informasi sensitif harus dihapus ketika tidak ada dibutuhkan lagi, dengan:
        1) Mengkonfigurasi sistem untuk memusnahkan informasi dengan aman saat tidak lagi diperlukan (mis periode tunduk pada kebijakan khusus topik tentang penyimpanan data atau dengan permintaan akses subjek);
        2) Menghapus versi usang, salinan, dan file sementara di mana pun mereka berada;
        3) Menggunakan perangkat lunak penghapusan aman yang disetujui untuk menghapus informasi secara permanen untuk membantu memastikan informasi tidak dapat dipulihkan dengan menggunakan pemulihan spesialis atau alat forensik;

4) Menggunakan penyedia layanan pembuangan aman yang disetujui dan bersertifikat;
5) Menggunakan mekanisme pembuangan yang sesuai untuk jenis media penyimpanan yang dibuang (mis. *degaussing hard disk drive* dan media penyimpanan magnetik lainnya).

14. Penyamaran data
    a. Perlindungan data sensitif (misalnya data pribadi) menjadi perhatian, organisasi harus mempertimbangkan untuk menyembunyikannya data tersebut dengan menggunakan teknik seperti penyamaran data, nama samaran, atau anonimisasi. Dimana teknik pseudonimisasi atau anonimisasi dapat menyembunyikan data pribadi, menyamarkan identitas sebenarnya dari yang mengakses atau mengolah data pribadi dan informasi sensitif lainnya. Hal ini dalam memutus hubungan antara data pribadi dan identitas prinsipal atau hubungan antara informasi sensitif lainnya.
    b. Saat menggunakan teknik pseudonimisasi atau anonimisasi, harus diverifikasi bahwa data telah cukup disamarkan atau dianonimkan. Anonimisasi data harus mempertimbangkan semua elemen informasi sensitif menjadi efektif. Sebagai contoh, jika tidak diperhatikan dengan baik, seseorang bisa diidentifikasi bahkan jika data yang dapat secara langsung mengidentifikasi orang tersebut dianonimkan, dengan adanya data lebih lanjut yang memungkinkan orang tersebut untuk diidentifikasi secara tidak langsung. Berikut adalah teknik tambahan untuk penyembunyian data meliputi:
        1) Enkripsi (mengharuskan pengguna yang berwenang untuk memiliki kunci);
        2) Meniadakan atau menghapus karakter (mencegah pengguna yang tidak berwenang melihat pesan lengkap);
        3) Nomor dan tanggal yang bervariasi;
        4) Substitusi (mengubah satu nilai ke nilai lain untuk menyembunyikan data sensitif);
        5) Mengganti nilai dengan hash mereka.
    c. Dimana hal-hal berikut harus dipertimbangkan saat menerapkan teknik penyembunyian data:
        1) Tidak memberikan semua pengguna akses ke semua data, oleh karena itu merancang *query* untuk

ditampilkan hanya data minimum yang diperlukan untuk pengguna;

2) Ada kasus di mana beberapa data tidak boleh terlihat oleh pengguna untuk beberapa record dari kumpulan data, dimana dalam merancang dan menerapkan mekanisme penyamaran data (contoh jika seorang pasien tidak ingin staf rumah sakit dapat melihat semua catatan mereka, bahkan dalam keadaan darurat, maka staf rumah sakit disajikan dengan data yang dikaburkan sebagian dan data hanya dapat diakses oleh staf dengan peran khusus jika mengandung informasi yang berguna untuk pengobatan yang tepat);
3) Ketika data disamarkan, memberikan kemungkinan kepada pengelola data pribadi untuk meminta agar pengguna tidak dapat melihatnya data dikaburkan (*obfuscation of the obfuscation*);
4) Persyaratan hukum atau peraturan apa pun (contoh mewajibkan penyembunyian informasi data pribadi ketika dalam proses input, pemrosesan penyimpanannya).

d. Hal-hal berikut harus dipertimbangkan saat menggunakan penyembunyian data, nama samaran, atau anonimisasi:
1) Tingkat kekuatan penyembunyian data, nama samaran atau anonimisasi menurut penggunaan data yang diproses;
2) Kontrol akses ke data yang diproses;
3) Perjanjian atau pembatasan penggunaan data yang diproses;
4) Melarang penggabungan data yang diproses dengan informasi lain untuk mengidentifikasi pengelola data pribadi;
5) Melacak penyediaan dan penerimaan data yang diproses.

15. Pencegahan Kebocoran Data
a. Kementerian PPN/Bappenas harus mempertimbangkan hal berikut untuk mengurangi risiko kebocoran data:
1) Mengidentifikasi dan mengklasifikasikan informasi untuk melindungi dari kebocoran (misalnya informasi pribadi, model penetapan harga dan desain produk);
2) Sarana komunikasi yang digunakan perlu dipantau dari risiko kebocoran data (misalnya email, transfer file,

perangkat seluler, dan penyimpanan portabel perangkat);

3) Bertindak untuk mencegah kebocoran informasi (misalnya karantina email yang berisi informasi sensitif).

b. Kementerian PPN/Bappenas dapat mempertimbangkan alat pencegahan kebocoran yang dapat digunakan digunakan untuk:

1) Mengidentifikasi dan memantau informasi sensitif yang berisiko diungkapkan secara tidak sah (misalnya data pada sistem pengguna);
2) Mendeteksi pengungkapan informasi sensitif (misalnya saat informasi diunggah ke layanan cloud pihak ketiga yang tidak terpercaya atau dikirim melalui email);
3) Memblokir tindakan pengguna atau transmisi jaringan yang mengekspos informasi sensitif (misalnya mencegah menyalin entri basis data ke dalam *spreadsheet*).

16. Pemantauan Aktivitas

a. Ruang lingkup dan tingkat pemantauan harus ditentukan sesuai dengan ketentuan yang berlaku di Kementerian PPN/Bappenas dan informasi persyaratan keamanan dan dengan mempertimbangkan hukum dan peraturan yang relevan. Catatan pemantauan harus dipertahankan untuk periode retensi yang ditentukan.

b. Berikut ini harus dipertimbangkan untuk dimasukkan dalam sistem pemantauan:

1) Jaringan keluar dan masuk, lalu lintas sistem dan aplikasi;
2) Akses ke sistem, server, peralatan jaringan, sistem pemantauan, aplikasi penting, dll.;
3) Sistem tingkat kritis atau admin dan file konfigurasi jaringan;
4) Log dari alat keamanan [misalnya antivirus, IDS, sistem pencegahan intrusi (IPS), filter web, firewall, pencegahan kebocoran data];
5) Log peristiwa yang berkaitan dengan aktivitas sistem dan jaringan;
6) Memeriksa bahwa kode yang sedang dieksekusi diotorisasi untuk berjalan di sistem dan belum dirusak (misalnya dengan kompilasi ulang untuk menambahkan kode tambahan yang tidak diinginkan);

7) Penggunaan sumber daya (misalnya CPU, hard disk, memori, bandwidth) dan kinerjanya.

c. Kementerian PPN/Bappenas harus menetapkan standar perilaku normal dan memantau standar ini jika ada anomali. Saat menetapkan standar, hal-hal berikut harus dipertimbangkan:
   1) Meninjau pemanfaatan sistem pada periode normal dan puncak;
   2) Waktu akses yang biasa, lokasi akses, frekuensi akses untuk setiap pengguna atau kelompok pengguna.

d. Sistem pemantauan harus dikonfigurasi terhadap standar yang ditetapkan untuk mengidentifikasi anomali perilaku, seperti:
   1) Penghentian proses atau aplikasi yang tidak direncanakan;
   2) Aktivitas yang biasanya terkait dengan malware atau lalu lintas yang berasal dari alamat IP berbahaya yang diketahui atau domain jaringan (misalnya yang terkait dengan perintah botnet dan server kontrol);
   3) Karakteristik serangan yang diketahui (misalnya *denial of service* dan *buffer overflows*);
   4) Perilaku sistem yang tidak biasa (misalnya *keystroke logging*, proses injeksi dan penyimpangan dalam penggunaan protokol standar);
   5) Kemacetan dan kelebihan beban (misalnya antrian jaringan dan tingkat latensi);
   6) Akses tidak sah (aktual atau dicoba) ke sistem atau informasi;
   7) Pemindaian aplikasi, sistem, dan jaringan Kementerian PPN/Bappenas yang tidak sah;
   8) Upaya yang berhasil dan tidak berhasil untuk mengakses sumber daya yang dilindungi (misalnya server DNS, portal web dan sistem file);
   9) Perilaku pengguna dan sistem yang tidak biasa dalam kaitannya dengan perilaku yang diharapkan.

17. Penyaringan Web
    a. Kementerian PPN/Bappenas harus mengurangi risiko dari akses situs web yang mengandung informasi ilegal atau diketahui mengandung virus atau materi phishing. Dengan melakukan blokir lamat IP atau domain situs web yang bersangkutan. Beberapa browser dan anti-malware

teknologi dapat melakukan ini dengan otomatis atau dengan melakukan konfigurasi pada browser.

b. Kementerian PPN/Bappenas mengidentifikasi jenis situs web yang tidak boleh diakses oleh pegawai. Kementerian PPN/Bappenas harus mempertimbangkan untuk memblokir akses ke jenis situs web berikut:
   1) Situs web yang memiliki fungsi pengunggahan informasi kecuali diizinkan untuk alasan Kementerian PPN/Bappenas yang sah;
   2) Situs web berbahaya yang diketahui atau dicurigai (mis. situs web yang mendistribusikan malware atau konten *phishing*);
   3) Server komando dan kontrol;
   4) Situs web berbahaya yang diperoleh dari intelijen ancaman;
   5) Situs web berbagi konten ilegal.

J. Keamanan Komunikasi
   1. Akses ke jaringan komunikasi harus dikelola dan dipantau untuk mengoptimalkan layanan Kementerian PPN/Bappenas secara konsisten.
   2. Fitur-fitur keamanan, tingkat layanan, dan persyaratan manajemen terhadap seluruh layanan jaringan komunikasi harus diidentifikasi dan dicakup dalam perjanjian tingkat layanan (*Service Level Agreement*), baik dilayani secara internal maupun oleh pihak eksternal.
   3. Pemisahan jaringan/sub jaringan berdasarkan kelompok layanan informasi, pengguna atau sistem informasi.

K. Akuisisi, Pengembangan, dan Pemeliharaan Sistem
   1. Persyaratan Pengadaan Sistem Informasi
      a. Sebelum pengadaan sistem informasi/software/aplikasi baru atau pengembangan yang sudah ada, Kementerian PPN/Bappenas menetapkan Tim yang bertugas menetapkan spesifikasi dan persyaratan keamanan yang relevan. Persyaratan Keamanan Sistem Informasi merupakan bagian yang terintegrasi dengan persyaratan lain yang ditetapkan bagi pihak ketiga.
      b. Seluruh software/aplikasi yang dikembangkan secara *in-house* harus menerapkan metode pengembangan aplikasi yang ditetapkan oleh Kementerian PPN/Bappenas.
      c. Selama tersedia sumber dayanya, sistem produksi harus dipisahkan dari sistem pengembangan dan pengujian. Pegawai yang bertanggungjawab dalam pengembangan dan

pengujian tidak boleh memiliki akses ke sistem produksi tanpa persetujuan dan pengawasan dari Koordinator Tim Aplikasi dan Koordinator Tim Manajemen TIK atau penanggung jawab sistem produksi yang ditetapkan.

2. Keamanan File Sistem
   a. Sistem operasi dan aplikasi hanya boleh diimplementasikan setelah melalui serangkaian pengujian dan pengoperasiannya di lingkungan produksi (*production*) harus mendapat persetujuan penanggung jawab lingkungan produksi (*production*) yang ditetapkn.
   b. Instalasi atau update seluruh software operasional, sistem aplikasi, dan program library hanya boleh dilakukan oleh pegawai Koordinator Manajemen TIK Kementerian PPN/Bappenas yang ditetapkan.
   c. Konfigurasi sistem operasional (*hardware* maupun *software*) tidak boleh diubah tanpa melalui proses manajemen perubahan (*IT Change Management*) yang ditetapkan.
   d. Data pengujian harus disimpan di lokasi yang aman dan tidak boleh diakses oleh pengguna kecuali yang berwenang.
   e. Jika pengembang memerlukan akses ke sistem produksi untuk keperluan pengujian atau pengembangan sistem baru, maka hanya akses "*read*" dan "*copy*" yang diberikan. Akses ini hanya diizinkan selama durasi pengujian dan aktivitas pengembangan yang terkait, dan harus segera dicabut setelah aktivitas tersebut berhasil dengan baik.
   f. Staff operasional komputer (*Service Support*) tidak boleh diberikan akses ke data produksi (*production*), *source code*, atau sistem operasi diluar yang diperlukan untuk mengerjakan tugasnya
3. Keamanan dalam Proses Pengembangan
   Setiap perubahan terhadap sistem dan aset informasi Kementerian PPN/Bappenas seperti: sistem operasi, hardware komputer, network, dan aplikasi harus mengikuti prosedur manajemen perubahan yang berlaku di Kementerian PPN/Bappenas.
4. Pengembangan Software oleh Pihak Ketiga (*Outsourcing*)
   Persyaratan keamanan informasi harus secara jelas didefinisikan dalam setiap kontrak tentang pengembangan aplikasi yang dikerjakan oleh pihak ketiga. Kontrak harus menetapkan antara lain, tetapi tidak terbatas pada:

1. Syarat dan ketentuan untuk menjamin seluruh pihak yang terlibat memiliki tanggungjawab terhadap keamanan informasi.
2. Cara memelihara kerahasiaan, keutuhan dan ketersediaan aset TI dan informasi terkait dipelihara dan diuji.
3. Cara mematuhi perundang-undangan dan regulasi yang berlaku.
4. Kontrol fisik dan *logic* yang harus diterapkan untuk menjamin agar akses informasi Kementerian PPN/Bappenas hanya dapat dilakukan oleh pegawai yang berwenang.
5. Cara memelihara layanan pada saat terjadinya bencana.
6. Hak untuk melakukan audit kepada pihak ketiga.

5. *Vulnerability Assessment*
   a. *Vulnerability Assessment* dilakukan sebelum perangkat lunak dan perangkat keras masuk ke dalam lingkungan production (*go live*).
   b. Untuk proses *Vulnerability Assessment* yang dilakukan oleh internal dengan objek aplikasi dan objek server berada di *cloud* maka dilakukan bersamaan pada saat proses pengembangan.
   c. Kegiatan *penetration test* (*pentest*) dilakukan secara rutin minimal 1 (satu) tahun sekali dan/atau berdasarkan permintaan dari manajemen dengan menentukan objek dan metode pengujian (*White Box*, *Black Box*, dan *Grey Box*) dan mitigasi temuan *pentest* dilakukan dan dimonitor oleh Tim Manajemen Aplikasi dan Tim Keamanan Informasi Pusdatinrenbang.
   d. Hasil temuan dari *Vulnerability Assessment* harus dilakukan remediasi atau perbaikan oleh pemohon.
   e. Hasil remediasi harus dilakukan verifikasi terlebih dahulu sebelum hasil temuan dari *Vulnerability Assessment* selesai.
   f. Pemohon membuat Nota Dinas/Memo permohonan *Vulnerability Assessment* dan melampirkan *Pre-Vulnerability Assessment Form*.
   g. Pemohon harus melakukan remediasi atas temuan-temuan dari *Vulnerability Assessment*.
   h. Hasil remediasi harus dilakukan verifikasi dan dipastikan semua temuan sudah ditutup, dimana apabila ada temuan yang apabila ditutup dapat mengganggu operasional Kementerian PPN/Bappenas harus diberi keterangan bahwa risiko diterima (*Risk Acceptance*).

i. Laporan hasil *Vulnerability Assessment* dan laporan hasil verifikasi harus di-*review* terlebih dahulu oleh Koordinator Keamanan Informasi dan apabila *Vulnerability Assessment* dilakukan oleh pihak ketiga, Laporan hasil *Vulnerability Assessment* dan Laporan hasil verifikasi harus direview terlebih dahulu oleh Koordinator Keamanan Informasi.

j. Laporan hasil *Vulnerability Assessment* bersifat rahasia dan tidak boleh diinformasikan kepada pihak yang tidak berkepentingan.

k. Pihak ketiga yang melaksanakan *Vulnerability Assessment* harus menandatangani *Non-Disclosure Agreement* terlebih dahulu dan dibuatkan kontrak pekerjaan sesuai dengan objek yang akan diuji.

6. Pengkodean yang aman

a. Kementerian PPN/Bappenas harus menetapkan proses di seluruh Kementerian PPN/Bappenas untuk memberikan tata kelola yang baik demi keamanan *coding*, dimana garis dasar minimum yang aman harus ditetapkan dan diterapkan. Selain itu, proses dan tata kelola harus diperluas untuk mencakup komponen perangkat lunak dari pihak ketiga dan sumber terbuka dari perangkat lunak.

b. Kementerian PPN/Bappenas harus memantau ancaman serta informasi terbaru tentang kerentanan perangkat lunak untuk memastikan standar pengkodean aman.

c. Dimana Ini dapat membantu memastikan praktik pengkodean aman yang efektif diterapkan untuk memerangi lanskap ancaman yang berubah dengan cepat.

d. Dalam melakukan perencanaan coding prinsip pengkodean yang aman harus digunakan baik untuk pengembangan baru maupun dalam skenario penggunaan kembali. Prinsip ini harus diterapkan pada kegiatan pengembangan baik di dalam Kementerian PPN/Bappenas maupun untuk produk dan jasa yang diberikan oleh Kementerian PPN/Bappenas kepada orang lain. Perencanaan dan prasyarat sebelum *coding* harus termasuk:

1) Ekspektasi khusus Kementerian PPN/Bappenas dan prinsip yang disetujui untuk pengkodean aman yang akan digunakan untuk keduanya pengembangan kode *in-house* dan *outsourcing*;

2) Pengecekan terhadap bug pada pemograman yang mengarah pada kerentanan keamanan informasi;

3) Mengonfigurasi alat pengembangan, seperti lingkungan pengembangan terintegrasi (IDE), untuk membantu menegakkan pembuatan kode aman;
4) Mengikuti panduan yang dikeluarkan oleh penyedia alat pengembangan dan lingkungan pelaksanaan sebagaimana berlaku;
5) Pemeliharaan dan penggunaan alat pengembangan yang diperbarui (misalnya kompiler);
6) Kualifikasi pengembang dalam menulis kode keamanan;
7) Desain dan arsitektur yang aman, termasuk pemodelan ancaman;
8) Standar pengkodean yang aman dan jika relevan mengamanatkan penggunaannya;
9) Penggunaan lingkungan terkendali untuk pembangunan.

e. Dimana pertimbangan selama pengkodean harus mencakup sebagai berikut:
1) Praktik pengkodean yang aman khusus untuk bahasa dan teknik pemrograman yang digunakan;
2) Menggunakan teknik pemrograman yang aman, seperti *pair programming*, *refactoring*, *peer review*, iterasi keamanan dan pengembangan berbasis pengujian;
3) Menggunakan teknik pemrograman terstruktur;
4) Mendokumentasikan kode dan menghapus cacat pemrograman, yang memungkinkan keamanan informasi kerentanan untuk dieksploitasi;
5) Melarang penggunaan teknik desain yang tidak aman (misalnya penggunaan *hard-coded passwords*, *unapproved* contoh kode dan layanan web yang tidak diautentikasi).

f. Dimana proses pengujian harus dilakukan selama dan setelah pengembangan dimana pengujian keamanan aplikasi statis proses dapat mengidentifikasi kerentanan keamanan dalam perangkat lunak. Dimana setelah pengujian dilaksanakan dan sebelum perangkat lunak dibuat operasional, terdapat hal-hal yang harus dievaluasi sebagai berikut:
1) Permukaan serangan dan prinsip hak istimewa terkecil;
2) Melakukan analisis terhadap kesalahan pemrograman yang paling umum dan mendokumentasikannya telah dimitigasi.

g. Setelah kode dibuat operasional perlu dilakukan proses pemantauan dan pemeliharaan yang mana berikut hal-hal yang harus diperhatikan:
   1) Pembaruan harus dikemas dan disebarkan dengan aman;
   2) Kerentanan keamanan informasi yang dilaporkan harus ditangani;
   3) Kesalahan dan dugaan serangan harus dicatat dan catatan ditinjau secara teratur untuk melakukan penyesuaian kode seperlunya;
   4) Kode sumber harus dilindungi dari akses yang tidak sah dan gangguan (misalnya dengan menggunakan alat manajemen konfigurasi, yang biasanya menyediakan fitur seperti kontrol akses dan kontrol versi).

h. Jika menggunakan alat dan platform pengembangan aplikasi eksternal, organisasi harus mempertimbangkan:
   1) Memastikan bahwa perpustakaan eksternal dikelola (misalnya dengan memelihara inventarisasi perpustakaan yang digunakan dan versinya) dan diperbarui secara berkala dengan siklus rilis;
   2) Pemilihan, otorisasi, dan penggunaan kembali komponen yang diperiksa dengan baik, terutama otentikasi dan komponen kriptografi;
   3) Lisensi, keamanan dan riwayat komponen eksternal;
   4) Memastikan bahwa perangkat lunak dapat dipelihara, dilacak, dan berasal dari sumber yang terbukti dan memiliki reputasi baik; dan
   5) Ketersediaan sumber daya dan Platform pengembangan aplikasi yang cukup untuk jangka panjang.

i. Jika paket perangkat lunak perlu dimodifikasi, hal-hal berikut harus dipertimbangkan:
   1) Risiko kontrol bawaan dan proses integritas disusupi;
   2) Apakah akan memperoleh persetujuan dari vendor;
   3) Kemungkinan memperoleh perubahan yang diperlukan dari vendor sebagai pembaruan program standar;
   4) Dampak jika Kementerian PPN/Bappenas menjadi bertanggung jawab atas pemeliharaan perangkat lunak di masa mendatang sebagai hasil perubahan;
   5) Kompatibilitas dengan perangkat lunak lain yang digunakan.

L. Hubungan Pemasok

1. Kinerja penyediaan layanan oleh penyedia jasa TI akan dipantau dan di-*review* secara periodik. Pemantauan akan meliputi, tetapi tidak terbatas pada:
   a. Kinerja kesesuaian layanan penyedia jasa TI terhadap perjanjian atau *Service Level Agreement* (SLA) yang disepakati.
   b. Laporan penggunaan layanan yang dibuat penyedia jasa TI.
   c. Laporan masalah yang terjadi dalam penggunaan layanan dan status tindak lanjutnya.
   d. Rekaman insiden dicatat oleh penyedia jasa TI.
   e. Laporan penyelesaian masalah.
2. Perubahan penyediaan layanan penyedia jasa TI, termasuk pemeliharaan dan peningkatan kebijakan keamanan informasi, prosedur, dan kontrol yang ada, akan dikelola dengan memperhitungkan kekritisan sistem Kementerian PPN/Bappenas, proses yang terlibat, dan mengkaji ulang risikonya.
3. Kementerian PPN/Bappenas melakukan identifikasi terhadap proses atau aktivitas yang dialihdayakan (*outsource*) yang berkaitan langsung maupun tidak langsung yang dapat mempengaruhi keamanan informasi di Kementerian PPN/Bappenas, dijelaskan lebih lanjut dalam lampiran dokumen Kebijakan Keamanan Informasi ini.

M. Manajemen Insiden Keamanan Informasi

1. Seluruh pegawai harus melaporkan sesegera mungkin kepada Petugas *HelpDesk* Pusdatinrenbang Kementerian PPN/Bappenas bila mendapati adanya suatu kelemahan atau insiden keamanan informasi.
2. Pihak ketiga harus melaporkan kelemahan atau insiden keamanan siber dan/atau keamanan informasi ke Tim CSIRT Kementerian PPN/Bappenas.
3. Untuk menjamin kecepatan, ketepatan, dan efektivitas respon terhadap insiden keamanan informasi, Kementerian PPN/Bappenas menetapkan Prosedur Pengelolaan Insiden keamanan informasi.
4. Jika diperlukan tindakan hukum terhadap pegawai atau pihak yang secara sengaja menjadi penyebab insiden keamanan siber dan/atau keamanan informasi, maka bukti-bukti yang diperlukan bagi proses hukum harus dihimpun secara lengkap.
5. Laporan insiden keamanan informasi didapatkan dari *ticketing system*.

6. Terdapat klasifikasi atas kejadian insiden keamanan informasi, sebagai berikut:
   a. *Crisis*: Insiden yang berdampak sangat serius pada aspek keamanan informasi (*Confidentiality, Integrity,* dan *Availability*) dan kontinuitas operasional Kementerian PPN/Bappenas
   b. *Major*: Insiden yang berdampak pada aspek keamanan informasi (*Confidentiality, Integrity,* dan *Availability*) dari perangkat *non-core* namun berdampak langsung pada pelayanan kepada pengguna internal dan eksternal.
   c. *Minor*: Insiden yang berdampak pada aspek keamanan informasi (*Confidentiality, Integrity,* dan *Availability*) dan tidak dapat diabaikan walaupun dampaknya tidak mengganggu operasional sistem lainnya atau keseluruhan sistem.
   d. *Negligible*: Insiden yang berdampak pada aspek keamanan informasi (*Confidentiality, Integrity,* dan *Availability*), akibat dari insiden ini dapat diabaikan karena tidak mengakibatkan kerusakan yang berarti, seperti terputusnya jalur komunikasi data sesaat, dari salah satu ISP, kerusakan salah satu perangkat network yang redundan, terputusnya aliran listrik dari PLN namun *Uninterruptible Power Supply* (UPS) dan genset dapat segera mengambil alih sebagai pemasok listrik pengganti PLN.
7. Setiap insiden keamanan informasi yang terjadi harus dicatat dan didokumentasikan dengan tertib serta dilaporkan secara eskalasi ke atas disesuaikan dengan klasifikasinya.
8. Ketika terjadi insiden keamanan informasi, maka penyedia jasa TI yang telah memiliki kontrak kerjasama dapat dihubungi oleh Kementerian PPN/Bappenas dalam melakukan penanganan insiden tersebut.
9. Ketika keadaan darurat terjadi atau ada gangguan pada sistem informasi dengan klasifikasi mengacu pada poin (6) maka tim yang terorganisir oleh Tim CSIRT Kementerian PPN/Bappenas yang akan merespons sesuai dengan rencana yang ditetapkan.
10. Manajemen insiden keamanan informasi memasukkan kegiatan pemantauan dan deteksi peristiwa keamanan di komputer atau jaringan komputer, dan pelaksanaan respons yang tepat terhadap peristiwa tersebut.
11. Investigasi kejadian insiden dilakukan untuk menentukan dampak atau keadaan setelah terjadinya insiden tersebut. Setiap kejadian insiden memerlukan penelusuran *root caused.* Namun,

sumber daya investigasi seperti alat forensik, jaringan karantina, dan konsultasi dengan penegak hukum mungkin diperlukan untuk penyelesaian insiden yang efektif dan cepat.

12. Tim CSIRT Kementerian PPN/Bappenas akan menyusun *lesson learned* dan mendokumentasikan final laporan penanganan insiden keamanan siber dan/atau keamanan informasi.
13. Pelapor insiden keamanan informasi yang melakukan *open ticket* melalui *ticketing system*, maka Petugas *HelpDesk* Pusdatinrenbang yang akan *close ticket* insiden keamanan informasi di *ticketing system*.

N. Aspek Keamanan Informasi dalam *Business Continuity Management*

1. Ketentuan Umum
   a. Kementerian PPN/Bappenas harus menyusun satu kerangka kerja *Business Continuity Plan* (BCP) terkait dengan ketersediaan sistem TI untuk menjamin kelangsungan operasional Kementerian PPN/Bappenas.
   b. Kerangka kerja BCP akan memfasilitasi proses koordinasi lintas unit kerja, dan mencakup antara lain:
      1) Proses eskalasi.
      2) Proses mobilisasi internal dan sosialisasi untuk menjamin agar seluruh pegawai dan pihak ketiga mendapatkan penjelasan yang memadai.
      3) Proses darurat dan kembali ke kondisi normal.
      4) Proses pengujian dan tindak lanjutnya.
      5) Peningkatan pelatihan dan sosialisasi.
   c. Tujuan implementasi BCP harus sejalan dengan tujuan Kementerian PPN/Bappenas.
   d. BCP harus memenuhi seluruh persyaratan legal yang tepat untuk kebutuhan pemenuhan compliance dari Kementerian PPN/Bappenas.
   e. Layanan TI yang harus dijamin ketersediaanya adalah layanan yang terkait dengan kegiatan organisasi vital dari Kementerian PPN/Bappenas.
   f. Layanan TI yang disebutkan pada poin 5 harus memiliki sistem *backup* dan *restore*.
   g. Layanan TI sebaiknya memiliki sistem redundansi baik dari sisi aplikasi maupun database.
   h. Jika dijalankan menggunakan *Cloud Service*, infrastruktur Layanan TI tersebut dijalankan dengan memanfaatkan fitur *High Availability*.

i. Jika dijalankan menggunakan *On Premise*, infrastruktur Layanan TI tersebut sebaiknya dijalankan dengan memanfaatkan fitur *High Availability* atau sistem DC-DRC.

j. Kriteria suatu kejadian dinyatakan sebagai Bencana adalah:
   1) Kerusakan besar yang disebabkan oleh alam.
   2) Pusat Pengelolaan Teknologi Informasi tidak beroperasi selama lebih dari 1 hari.
   3) Jaringan terputus selama lebih dari 1 hari.
   4) Kebakaran dalam gedung Kementerian PPN/Bappenas.
   5) Pencurian/perampokan.
   6) Banjir.
   7) Wabah penyakit.

k. Rekaman pelaksanaan dan hasil pengujian BCP akan didokumentasikan, dianalisis dan direviu untuk peningkatan secara terus menerus.

2. Ketentuan Analisis Dampak organisasi

a. Analisis dampak organisasi harus disusun dan diupdate minimal 1 (satu) tahun sekali, untuk memastikan dampak baru yang disebabkan oleh perubahan proses Kementerian PPN/Bappenas. Output dari analisis dampak Kementerian PPN/Bappenas ini adalah dokumen BIA (*Business Impact Analysis*).

b. Lebih spesifik lagi analisis dampak organisasi ini dilakukan untuk mengetahui dampak dari suatu bencana terhadap proses organisasi yang diakibatkan tidak tersedianya (*availability*) operasional teknologi informasi.

c. Perlu ditetapkan Batas Waktu Kritikal (*Critical Time Frame*) sebagai referensi untuk Kesepakatan Tingkat Layanan (*Service Level Agreements*) dari Rencana Pemulihan setelah Bencana (*Disaster Recovery Plan*) sebagai berikut:
   1) Batas Waktu *Maksimum Downtime*/ MTD (*Maximum Tolerable Downtime*). Merupakan toleransi periode waktu yang ditentukan oleh Organisasi terhadap tidak berjalannya suatu proses Kementerian PPN/Bappenas sebelum dampaknya mencapai tingkat yang tidak dapat diterima oleh Kementerian PPN/Bappenas.
   2) Batas Waktu Pemulihan/ RTO (*Recovery Time Objective*). Merupakan periode waktu yang tersedia untuk memulihkan sumber daya teknologi informasi apabila suatu proses Kementerian PPN/Bappenas tidak berjalan.
   3) Nilai RTO tidak boleh lebih lama dari MTD.

d. Perlu ditetapkan pernyataan dampak layanan yang merupakan output dari analisis dampak organisasi. Kategori dampak layanan ditetapkan adalah:
   1) Tinggi: Terganggunya layanan mempengaruhi >75% kegiatan operasional Teknologi Informasi.
   2) Menengah: Terganggunya layanan mempengaruhi 25-75% kegiatan operasional Teknologi Informasi.
   3) Rendah: Terganggunya layanan mempengaruhi <25% kegiatan operasional Teknologi Informasi.

3. Ketentuan terkait Strategi Keberlangsungan Teknologi Informasi.
   a. Ketentuan dalam Strategi Pemulihan adalah sebagai berikut:
      1) Perlu ditetapkan strategi pemulihan pasca Bencana sebagai acuan Tim Manajemen Insiden dan Kelangsungan Kementerian PPN/Bappenas dalam menjalankan proses pemulihan Bencana tersebut.
      2) Perlu ditetapkan skenario-skenario dalam strategi pemulihan. Skenario pemulihan pasca bencana dikelompokan menjadi 3 (tiga) kondisi, sebagai berikut:
         i. Skenario 1: Bencana yang menyebabkan ketiadaan SDM untuk menjalankan operasional.
         ii. Skenario 2: Bencana yang menyebabkan ketiadaan premises untuk melakukan operasional seperti gedung & fasilitas pendukung, perangkat hardware.
         iii. Skenario 3: Bencana yang menyebabkan ketiadaan akses untuk melakukan operasional seperti akses layanan aplikasi, akses sistem, akses Data, akses database dan lain-lain.
   b. Dalam menentukan strategi pemulihan harus dilakukan pemetaan antara risiko-risiko yang teridentifikasi dengan skenario pemulihan Bencana.
   c. Ketentuan dalam Strategi Relokasi dan Alternatif Lokasi.
   d. Menetapkan strategi dalam menentukan lokasi dan alternatif lokasi pada proses BCP untuk menjamin proses pelaksanaan BCP dapat berjalan dengan baik sesuai skenario yang sudah ditetapkan.
   e. Penetapan Strategi Relokasi disesuaikan dengan kesiapan dan kondisi yang sudah tersedia. Strategi Relokasi dan Alternatif Relokasi ditetapkan sebagai berikut:
      1) *On-site*: Lokasi *on-site* di kantor Kementerian PPN/Bappenas (Jl. Taman Suropati No.2, Menteng, Kec.

Menteng, Kota Jakarta Pusat) dapat dipilih jika fasilitas dan server produksi (*production*) dapat diakses dan pemulihan sistem pasca bencana dapat dilakukan di tempat tersebut, umumnya lebih sederhana, lebih efisien, dan lebih kecil risikonya dibanding pemulihan *off-site*.

2) Off-site:

i. Lokasi *off-site* di tempat selain kantor Kementerian PPN/Bappenas, dipilih jika fasilitas kerja dan server produksi tidak dapat diakses dan pemulihan sistem pasca Bencana tak dapat dilakukan di Kantor Kementerian PPN/Bappenas. Lokasi ini biasa disebut sebagai *Disaster Recovery Center* (DRC).

ii. Lokasi *off-site* oleh Pihak Ketiga, dipilih jika fasilitas dan server produksi (*Production Server*/*Production Area*) merupakan bentuk layanan yang diberikan oleh pihak ketiga.

iii. Dalam penetapan kategori kesiapan operasional fasilitas pemulihan atau Relokasi atau lokasi alternatif dapat dikategorikan berdasarkan kebutuhan sebagai berikut:

a) *Cold Site* adalah DRC dengan ketentuan bahwa di lokasi ini belum diisi dengan fasilitas TI. Dibutuhkan waktu yang cukup lama antara 2 - 3 minggu untuk pengadaan, pemasangan dan konfigurasi peralatan.

b) *Warm Site* adalah DRC sudah dilengkapi dengan fasilitas TI yang siap pakai, terdiri dari sejumlah hardware, software, network dan peralatan komunikasi yang sudah terpasang. Pengaktifan sistem/layanan TIK memerlukan instalasi dan konfigurasi sistem aplikasi serta restorasi data aplikasi. Sistem DRC ini akan siap dalam beberapa hari.

c) *Hot Site* adalah DRC sudah dilengkapi dengan sistem komputer berupa hardware, software dan jaringan. Sistem operasi dan sistem aplikasi sudah terpasang dengan konfigurasi yang sama seperti fasilitas di Pusat Pengelolaan Teknologi Informasi. Pengaktifan layanan TI memerlukan restorasi data.

Fasilitas Hot site ini umumnya siap beroperasi dalam waktu beberapa jam.

4. Ketentuan Aspek keamanan informasi
   a. Aspek keamanan informasi dan keamanan siber (*Cyber Security*) merupakan hal yang harus diperhatikan dalam proses BCP.
   b. Beberapa ketentuan terkait aspek terkait keamanan informasi dan keamanan siber (*Cyber Security*) adalah:
      1) Pusat Pengelolaan Teknologi Informasi alternatif harus selalu dalam keadaan terkunci dan hanya dapat diakses pegawai tertentu dan sesuai SOP keluar masuk area Pusat Pengelolaan Teknologi Informasi.
      2) Anti-virus di area Pusat Pengelolaan Teknologi Informasi alternatif sudah diaktifkan dan dalam kondisi terkini.
      3) Memastikan area Pusat Pengelolaan Teknologi Informasi utama saat terjadi bencana/setelah terjadi bencana diberikan perlindungan fisik.
      4) Selain perlindungan fisik harus proteksi dengan perangkat keamanan baik berupa *hardware* maupun *software* seperti Firewall dan fitur *security* lainnya (IDS dan IPS).
5. Ketentuan terkait Peran dan Tanggung jawab Tim *IT Disaster Recovery*
   a. Perlu ditetapkan dan dibentuk organisasi, wewenang dan tanggung jawab Tim *IT Disaster Recovery* Kementerian PPN/Bappenas. Untuk menjamin ketersediaan Tim saat dibutuhkan pada saat terjadi Bencana.
   b. Wewenang dan Tanggung jawab Tim *IT Disaster Recovery*
      1) Tugas dan tanggung jawab Tim *IT Disaster Recovery* secara umum:
         i. Bertanggung jawab sebagai koordinator utama dalam inisiasi respon pada terjadinya bencana, terfokus kepada perlindungan aset teknologi informasi.
         ii. Melaksanakan pengujian Disaster Recovery Plan, baik secara teknis, logistik, administratif, prosedural, operasional, sistem dan sumber daya manusia.
         iii. Melaksanakan pemeliharaan infrastruktur Disaster Recovery Plan, baik secara berkala maupun berdasarkan kejadian/ perubahan yang

mempengaruhi Kementerian PPN/Bappenas dan berdampak pada *Disaster Recovery Plan*.

iv. Melaksanakan review *Disaster Recovery Plan*, baik dilakukan oleh pihak internal maupun dengan bantuan pihak independen.

v. Setelah proses pengujian DRP, dilakukan evaluasi sebagai bahan tindakan perbaikan dan/atau rencana peningkatan efektifitas DRP secara berkelanjutan (Continual Improvement).

vi. Menyusun laporan hasil proses pengujian, pemeliharaan dan *review Disaster Recovery Plan*.

vii. IT Disaster Infrastruktur bertugas melakukan analisis dampak bencana terhadap infrastruktur serta bertanggung jawab atas pemulihan infrastruktur.

viii. IT Disaster Network bertugas melakukan analisis dampak bencana terhadap sistem network serta bertanggung jawab atas pemulihan network.

ix. IT Disaster Aplikasi bertugas melakukan analisis dampak bencana terhadap aplikasi yang digunakan di Kementerian PPN/Bappenas serta bertanggung jawab atas pemulihan sistem aplikasi.

2) Tugas dan tanggung jawab Penanggung Jawab TI:

i. Menyediakan fasilitas DRC sebagai solusi backup layanan TI kritikal.

ii. Melakukan pengaktifan rencana pemulihan (*Disaster Recovery Plan*) dan tim *IT Disaster Recovery*.

iii. Melakukan pengambilan keputusan tingkat tinggi termasuk memutuskan untuk menyatakan bencana di TI.

iv. Mengarahkan seluruh proses tanggap darurat, pemulihan dan restorasi di lingkungan TI.

v. Bertindak sebagai penghubung utama di TI kepada pimpinan Kementerian PPN/Bappenas, para pemangku kepentingan (*stakeholder*) dan mitra TI selama pemulihan TI, dengan tanggung jawab sebagai berikut:

a) Menyampaikan status bencana di IT dan kegiatan pemulihan yang sedang berjalan kepada pimpinan Kementerian

PPN/Bappenas dan para pemangku kepentingan.

b) Melakukan koordinasi dengan pimpinan Kementerian PPN/Bappenas dan unit kerja lain di Kementerian PPN/Bappenas serta para pemangku kepentingan, termasuk kepada pihak terkait yang dibutuhkan, dalam melakukan asesmen awal dampak bencana TI, respon terhadap bencana TI, penanganan bencana TI dan pemulihan TI.

vi. Membatalkan/mengakhiri pelaksanaan rencana pemulihan (*Disaster Recovery Plan*) dan tim IT Disaster Recovery.

vii. Mengadakan dan menjaga keberadaan catatan terkait peristiwa/bencana dan tindakan yang dilakukan selama pemulihan, untuk mengetahui bila terjadi penyimpangan dari rencana pemulihan.

6. Ketentuan tahapan rencana pemulihan

Berikut adalah Ketentuan dalam tahapan rencana pemulihan yang harus didefinisikan oleh Kementerian PPN/Bappenas:

1. Ketentuan respon terhadap kondisi darurat.
2. Pelaksanaan pemulihan dan normalisasi Pusat Pengelolaan Teknologi Informasi.
3. Aktivasi DRC.
4. Akuisisi/pembangunan Pusat Pengelolaan Teknologi Informasi.
5. Pengembalian ke kondisi normal.

7. Ketentuan Pemeliharaan *Disaster Recovery Plan*

a. Pengujian *Disaster Recovery Plan*

1) Pengujian DRP harus dilakukan rutin agar pelaksanaan DRP sesuai tujuannya yaitu:

a) Menentukan efektivitas dari prosedur perencanaan.

b) Menentukan kesiapsiagaan dan kemampuan anggota tim yang telah ditunjuk, dalam melaksanakan tugas dalam tanggung jawabnya.

c) Menentukan apakah *Disaster Recovery Plan* membutuhkan modifikasi atau update untuk memastikan *recovery* dalam batas waktu kritikal (*Critical Time Frame*) yang ditetapkan dapat diterima oleh Kementerian PPN/Bappenas.

2) Pengujian dilakukan paling tidak 1 (satu) kali dalam 1 (satu) tahun dengan cara minimal melakukan restore data atau melakukan *switch* pada area DRC. Selain itu pengujian dapat pula dilakukan dengan metode *table-top exercise* (jika diperlukan).
3) Sebelum atau setelah pelaksanaan pengujian DRP dilakukan proses pemeliharaan terhadap dokumen *Disaster Recovery Plan* dari Kementerian PPN/Bappenas agar terjaga kemutakhirannya.
4) Hasil pengujian akan dilakukan evaluasi untuk dijadikan bahan rekomendasi perbaikan.
5) Menyusun laporan hasil pengujian DRP yang berisi laporan evaluasi pelaksanaan dan hasil pengujian rencana pemulihan bencana.

b. Pemeliharaan *Disaster Recovery Plan*
1) Pemeliharaan DRP dapat dilakukan secara berkala agar tetap sesuai dengan keadaan Kementerian PPN/Bappenas maupun dilakukan saat terdapat perubahan yang mempengaruhi Kementerian PPN/Bappenas.
2) Pemeliharaan DRP dilakukan secara organisasi, skenario, isi dokumen secara menyeluruh paling tidak 1 (satu) kali dalam 1 (satu) tahun.

c. Review *Disaster Recovery Plan*
1) Review DRP dapat dilakukan oleh pihak internal atau dapat dilakukan oleh pihak independen paling tidak 1 (satu) kali dalam 1 (satu) tahun.
2) Review DRP dilakukan dengan memeriksa hal sebagai berikut:
i. Seluruh fungsi proses organisasi utama Kementerian PPN/Bappenas beserta proses-proses kritikal dan sumber dayanya telah teridentifikasi dan dipertimbangkan dalam penentuan strategi pada DRP.
ii. DRP telah mencerminkan prioritas dan kebutuhannya secara jelas dan akurat.
iii. Kompetensi, kapabilitas, dan solusi pada DRP dinilai efektif berdasarkan evaluasi uji coba ataupun kejadian bencana sebenarnya.
iv. Program pengujian dan pemeliharaan telah diimplementasikan dengan efektif.

v. DRP telah mengakomodir perbaikan-perbaikan yang diidentifikasikan pada saat uji coba ataupun kejadian bencana sebenarnya.
vi. Sosialisasi dan pelatihan pada DRP dilakukan secara berkesinambungan.
vii. DRP telah dikomunikasikan secara efektif untuk memastikan pemahaman terhadap tugas, peran, tanggung jawab, dan wewenang dari setiap pegawai terkait.

8. Kesiapan TI untuk kelangsungan organisasi
   a. Kesiapan TI untuk kelangsungan organisasi merupakan komponen penting dalam manajemen kelangsungan organisasi dan manajemen keamanan informasi untuk memastikan bahwa tujuan organisasi dapat terus berlanjut bertemu selama gangguan. Dimana persyaratan kesinambungan TI adalah hasil dari analisis dampak organisasi atau BIA adalah untuk mengidentifikasi proses bisnis kritikal dan membuat peringkat/urutan prioritas proses dan kegiatan kritikal. BIA kemudian harus menentukan sumber daya mana yang dibutuhkan untuk mendukung prioritas kegiatan.
   b. BIA yang melibatkan layanan TI dapat diperluas untuk menentukan persyaratan kinerja dan kapasitas Sistem TI dan tujuan titik pemulihan atau RPO informasi yang diperlukan untuk mendukung kegiatan selama gangguan. Berdasarkan keluaran dari BIA dan penilaian risiko yang melibatkan layanan TIK, organisasi harus mengidentifikasi dan memilih strategi kesinambungan TIK yang mempertimbangkan opsi sebelum, selama, dan setelah gangguan. Strategi kelangsungan organisasi dapat terdiri dari satu atau lebih solusi. Berdasarkan strategi, rencana harus dikembangkan, diimplementasikan dan diuji untuk memenuhi tingkat ketersediaan layanan TIK yang dibutuhkan dan dalam kerangka waktu yang diperlukan setelah gangguan, atau kegagalan, proses kritis. Dimana dalam melakukan kesiapan TI untuk kelangsungan organisasi organisasi harus memastikan bahwa:
      1) Tersedia struktur organisasi yang memadai untuk mempersiapkan, melakukan mitigasi, dan menanggapi gangguan didukung oleh pegawai yang memiliki tanggung jawab, wewenang dan kompetensi yang diperlukan;

2) Rencana kesinambungan TIK, termasuk prosedur tanggapan dan pemulihan yang merinci bagaimana organisasi berencana untuk mengelola gangguan layanan TIK, adalah:
   a) Dievaluasi secara berkala melalui latihan dan pengujian;
   b) Disetujui oleh manajemen;
3) Rencana kesinambungan TIK mencakup informasi kesinambungan TIK berikut:
   i. Spesifikasi kinerja dan kapasitas untuk memenuhi persyaratan kelangsungan organisasi dan tujuan sebagaimana ditentukan dalam *Business Impact Analysis*;
   ii. *Recovery Time Objective* dari setiap layanan TIK yang diprioritaskan dan prosedur pemulihan komponen tersebut;
   iii. *Recovery Point Objective* sumber daya TIK yang diprioritaskan didefinisikan sebagai informasi dan prosedur untuk memulihkan informasi.

O. Kepatuhan
1. Kementerian PPN/Bappenas menetapkan daftar *software* standar dan akan menyediakan lisensi *software* dalam jumlah yang memadai untuk memungkinkan pegawai bekerja secara aman dan mematuhi ketentuan lisensi *software*.
2. *Systems administrator* berhak menghapus *software* dari komputer yang digunakan Pengguna jika Pengguna tidak dapat membuktikan lisensi *software* yang dipasangnya atau jika *software* tidak diperlukan bagi tujuan organisasi atau menimbulkan masalah di komputer milik Kementerian PPN/Bappenas.
3. Setiap *software* yang dikembangkan oleh pegawai selama bekerja di dan/atau dengan menggunakan sumber daya Kementerian PPN/Bappenas menjadi hak milik Kementerian PPN/Bappenas.
4. Lisensi *software* yang disediakan oleh Kementerian PPN/Bappenas tidak boleh digunakan atau dipasang di peralatan komputer selain milik Kementerian PPN/Bappenas. Instalasi *software* harus dilakukan dan/atau dipantau oleh Tim Teknis Pusdatinrenbang Kementerian PPN/Bappenas.
5. Akses terhadap *audit tool* tidak boleh diberikan kecuali kepada pegawai yang kompeten dan berwenang untuk mencegah risiko

terjadinya gangguan terhadap sistem atau kemungkinan penyalahgunaan.

P. Audit Internal SMKI

1. Persiapan Audit Internal SMKI
   a. Tim Audit Internal SMKI akan membuat program audit tahunan sesuai dengan standar ISO/IEC 27001. Dokumen program audit ini harus disahkan oleh Ketua Tim SMKI.
   b. Tim Audit Internal SMKI akan mengirimkan dokumen program audit yang akan disahkan oleh Ketua Tim SMKI.
   c. Ketua Tim SMKI akan menganalisis dan memeriksa ketepatan program audit. Apabila sudah sesuai, maka penandatanganan program audit tahunan dilakukan.
   d. Ketua Tim SMKI akan menyetujui atau tidak menyetujui program audit yang diajukan oleh Tim Audit Internal SMKI.
   e. Apabila dokumen program audit disetujui Ketua Tim SMKI, maka dokumen program audit yang sudah disahkan dikembalikan kepada Tim Audit Internal SMKI.
   f. Tim Audit Internal SMKI akan melakukan persiapan-persiapan audit yang diperlukan sebelum aktivitas program audit dilaksanakan diantaranya:
      1) Melakukan persiapan audit seperti penyusunan jadwal.
      2) Memastikan ketersediaan tim Audit Internal, memberikan arahan kepada tim Audit Internal.
      3) Memastikan ketersediaan ~~ruangan dan~~ sumber daya lainnya yang diperlukan untuk pelaksanaan audit.
      4) Memastikan bahwa *checklist* audit telah dibuat.
   g. Tim Audit Internal SMKI mengkonfirmasikan dan menginformasi terkait jadwal audit kepada Auditee.
2. Pelaksanaan Audit Internal SMKI
   a. Tim Audit Internal SMKI memulai pelaksanaan audit dengan melakukan acara pembukaan (*opening meeting*). Agenda acara pembukaan, antara lain minimal mencakup kegiatan sebagai berikut:
      1) Perkenalan.
      2) Penjelasan tujuan dan ruang lingkup audit.
      3) Konfirmasi audit *plan*.
      4) Penjelasan tata cara audit.
      5) Penjelasan kategori ketidaksesuaian.
      6) Penjelasan metode pelaporan; dan
      7) Tanya jawab.

b. Tim Audit Internal SMKI akan melaksanakan Audit Internal SMKI sesuai dengan ruang lingkup dan jadwal yang telah ditentukan.
c. Tim Audit Internal SMKI akan meminta informasi yang dibutuhkan berkaitan dengan ruang lingkup audit kepada Auditee.
d. Auditee akan memberikan informasi mengenai hal-hal yang diminta oleh Tim Audit Internal SMKI. Penyampaian informasi dapat berupa wawancara, observasi maupun penyerahan dokumen.
e. Setelah semua informasi yang dibutuhkan Tim Audit Internal SMKI akan mencatat temuan, rekomendasi, dan memberikan kertas kerja yang berisi informasi tersebut kepada Auditee.
f. Auditee akan menerima dan menganalisis kertas kerja yang diberikan oleh Tim Audit Internal SMKI.
g. Auditee dan Tim Audit Internal SMKI akan menentukan tanggal perbaikan hasil temuan serta menandatangani kertas kerja audit.
h. Tim Audit Internal SMKI menerima kertas kerja yang telah ditandatangani oleh Auditee. Kertas kerja ini kemudian digandakan dan didistribusikan dengan ketentuan sebagai berikut:
    1) Kertas kerja asli diserahkan kepada Auditor Internal SMKI.
    2) Salinan kertas kerja diberikan kepada Auditee; dan
    3) Salinan kertas kerja disimpan oleh anggota tim Audit Internal SMKI.
i. Setelah keseluruhan audit selesai, Tim Audit Internal SMKI akan memimpin rapat penutupan (*closing meeting*) yang dihadiri oleh seluruh tim Audit Internal SMKI dan Auditee. Agenda rapat penutupan minimal mencakup:
    1) Ucapan terima kasih.
    2) Presentasi terhadap temuan (jika ada) serta meminta tanggapan dari auditee dan melakukan pembahasan rencana tindak lanjut temuan audit; dan
    3) Tanya Jawab.

3. Pemantauan Tindakan Perbaikan Audit Internal SMKI
    a. Auditee melaksanakan tindakan perbaikan atas temuan yang didapat selama Audit Internal SMKI.

b. Perbaikan disesuaikan dengan usulan rekomendasi yang diberikan di kertas kerja. Setelah perbaikan dilakukan, hasil perbaikan dilaporkan kepada Tim Audit Internal SMKI.
c. Tim Audit Internal SMKI memonitor tindak lanjut perbaikan yang dilaksanakan oleh Auditee. Auditee harus melaporkan status tindak lanjut kepada Auditor Internal SMKI.
d. Tim Audit Internal SMKI akan memutuskan apakah tindakan perbaikan memadai.
e. Tim Audit Internal SMKI akan memantau status tindak lanjut perbaikan dalam status log laporan audit.
f. Tim Audit Internal SMKI menyimpan semua dokumentasi yang berkaitan dengan Audit Internal SMKI.
g. Tim audit internal harus mengikuti perkembangan TIK.

BAB III
PENUTUP

Dengan adanya Kebijakan Pengamanan Informasi Sistem Manajemen Keamanan Informasi Kementerian PPN/Bappenas ini, diharapkan dapat menghasilkan implementasi keamanan informasi yang dapat menjaga kerahasiaan, ketersediaan, dan keakuratan Kementerian PPN/Bappenas.

Kebijakan Pengamanan Informasi Sistem Manajemen Keamanan Informasi Kementerian PPN/Bappenas ini agar dapat digunakan dan dipatuhi oleh para pihak baik pegawai di internal Kementerian PPN/Bappenas maupun pihak lain yang bekerja sama dengan Kementerian PPN/Bappenas.

Hal-hal lain yang belum tertuang dalam Kebijakan Pengamanan Informasi ini, karena adanya perubahan petunjuk pelaksanaan eksternal ataupun internal maka akan diadakan penyesuaian lebih lanjut dan merupakan bagian yang tidak terpisahkan dengan petunjuk pelaksanaan ini.

Hal-hal lain yang bersifat teknis dituangkan dalam prosedur yang merupakan dokumen terpisah yang menjadi satu kesatuan dengan Kebijakan Keamanan Informasi ini.

Kebijakan Pengamanan Informasi ini mulai berlaku sejak ditetapkan, dan berlaku surut sejak tanggal 2 Januari 2024.

SEKRETARIS KEMENTERIAN PERENCANAAN PEMBANGUNAN NASIONAL/SEKRETARIS UTAMA BADAN PERENCANAAN PEMBANGUNAN NASIONAL

TENI WIDURIYANTI