BADAN POM

BADAN PENGAWAS OBAT DAN MAKANAN

Jl. Percetakan Negara No. 23 Jakarta Pusat 10560 Indonesia
Telp. (021) 4244691, 4209221, 4263333, 4244755, 4241781, 4244819, Fax : 4245139
Email : halobpom@pom.go.id ; Website : www.pom.go.id

KEPUTUSAN KEPALA BADAN PENGAWAS OBAT DAN MAKANAN
REPUBLIK INDONESIA
NOMOR HK.04.01.1.22.03.19.1268 TAHUN 2019
TENTANG
KEBIJAKAN PENGELOLAAN KEAMANAN INFORMASI
DI LINGKUNGAN BADAN PENGAWAS OBAT DAN MAKANAN

KEPALA BADAN PENGAWAS OBAT DAN MAKANAN
REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk melindungi kerahasiaan, integritas dan ketersediaan sistem informasi Badan Pengawas Obat dan Makanan dari ancaman keamanan informasi, perlu menetapkan mekanisme pengelolaan keamanan informasi di lingkungan Badan Pengawas Obat dan Makanan;

b. bahwa untuk mekanisme pengelolaan keamanan informasi sebagaimana yang dimaksud pada huruf a, perlu menetapkan kebijakan mengenai pengelolaan keamanan informasi;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b perlu menetapkan Keputusan Kepala Badan Pengawas Obat dan Makanan tentang Kebijakan Pengelolaan Keamanan Informasi di lingkungan Badan Pengawas Obat dan Makanan;

Mengingat : 1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016

Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);

2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
3. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
4. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
5. Peraturan Presiden Nomor 80 Tahun 2017 tentang Badan Pengawas Obat dan Makanan (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 180);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. Peraturan Menteri Komunikasi dan Informatika Nomor 41/PER/MEN.KOMINFO/11/2007 Tahun 2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional;
8. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
9. Peraturan Kepala Badan Pengawas Obat dan Makanan Nomor 6 Tahun 2017 tentang Daftar Informasi Publik yang Dikecualikan di Lingkungan Badan Pengawas Obat dan Makanan (Berita Negara Republik Indonesia Tahun 2017 Nomor 542)

10. Peraturan Badan Pengawas Obat dan Makanan Nomor 26 Tahun 2017 tentang Organisasi dan Tata Kerja Badan Pengawas Obat dan Makanan (Berita Negara Republik Indonesia Tahun 2017 Nomor 1745);
11. Peraturan Badan Pengawas Obat dan Makanan Nomor 12 Tahun 2018 tentang Organisasi dan Tata Kerja Unit Pelaksana Teknis di Lingkungan Badan Pengawas Obat dan Makanan (Berita Negara Republik Indonesia Tahun 2018 Nomor 784);
12. Peraturan Badan Pengawas Obat dan Makanan Nomor 27 Tahun 2018 tentang Standar Pelayanan Publik di Lingkungan Badan Pengawas Obat dan Makanan (Berita Negara Republik Indonesia Tahun 2018 Nomor 1132);
13. Keputusan Kepala Badan Pengawas Obat dan Makanan Nomor HK.00.06.74.3496 Tahun 2009 tentang Kebijakan Teknologi Informasi dan Komunikasi Terintegrasi di Lingkungan Badan Pengawas Obat dan Makanan;

MEMUTUSKAN:

Menetapkan : KEPUTUSAN KEPALA BADAN PENGAWAS OBAT DAN MAKANAN TENTANG KEBIJAKAN PENGELOLAAN KEAMANAN INFORMASI DI LINGKUNGAN BADAN PENGAWAS OBAT DAN MAKANAN.

Kesatu : Menetapkan dan memberlakukan Kebijakan Pengelolaan Keamanan Informasi di Lingkungan Badan Pengawas Obat dan Makanan sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan ini.

Kedua : Kebijakan Pengelolaan Keamanan Informasi sebagaimana dimaksud dalam diktum Kesatu merupakan acuan bagi seluruh pegawai dalam mengelola keamanan informasi di lingkungan satuan kerja atau unit kerja di Lingkungan Badan Pengawas Obat dan Makanan.

Ketiga : Unit Kerja di lingkungan Badan Pengawas Obat dan Makanan wajib melindungi dan menjaga kerahasiaan data dan informasi yang berada dalam penguasaannya.

Keempat : Pimpinan Unit Kerja di lingkungan Badan Pengawas Obat dan Makanan bertanggung jawab atas terlaksananya kontrol keamanan informasi untuk memastikan perlindungan terhadap data dan informasi yang dikelola.

Kelima : Dalam pelaksanaan kebijakan pengelolaan keamanan informasi sebagaimana dimaksud dalam diktum kesatu, Kepala Pusat data dan Informasi Obat dan Makanan sebagai koordinator untuk melakukan pengawasan penyelenggaraan proses keamanan informasi.

Keenam : Dalam melaksanakan kebijakan pengelolaan keamanan informasi sebagaimana dimaksud dalam diktum kesatu, Unit Kerja harus menyediakan sumber daya yang dibutuhkan untuk membentuk, implementasi, pemeliharaan dan peningkatan secara berkesinambungan.

Ketujuh : Pada saat Keputusan ini mulai berlaku, Keputusan Kepala Badan Pengawas Obat dan Makanan Nomor HK.04.1.74.01.13.111 Tahun 2013 tentang Kebijakan Pengelolaan Keamanan Informasi Data Center Badan Pengawas Obat dan Makanan sebagaimana telah diubah dengan Keputusan Kepala Badan Pengawas Obat dan Makanan Nomor HK.04.1.74.02.14.0859 Tahun 2014 tentang Perubahan atas Keputusan Kepala Badan Pengawas Obat dan Makanan Nomor HK.04.1.74.01.13.111 Tahun 2013 tentang Kebijakan Pengelolaan Keamanan Informasi Data Center Badan Pengawas Obat dan Makanan, dicabut dan dinyatakan tidak berlaku.

BADAN POM

BADAN PENGAWAS OBAT DAN MAKANAN

Jl. Percetakan Negara No. 23 Jakarta Pusat 10560 Indonesia

Telp. (021) 4244691, 4209221, 4263333, 4244755, 4241781, 4244819, Fax : 4245139

Email : halobpom@pom.go.id ; Website : www.pom.go.id

Kedelapan : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta

Pada tanggal 28 Maret 2019

KEPALA BADAN PENGAWAS OBAT DAN MAKANAN,

REPUBLIK INDONESIA.



ttd.

PENNY K. LUKITO

LAMPIRAN
KEPUTUSAN KEPALA BADAN PENGAWAS OBAT DAN MAKANAN
REPUBLIK INDONESIA
NOMOR HK.04.01.1.22.03.19.1268 TAHUN 2019
TENTANG
KEBIJAKAN PENGELOLAAN KEAMANAN INFORMASI
DI LINGKUNGAN BADAN PENGAWAS OBAT DAN MAKANAN

KEBIJAKAN PENGELOLAAN KEAMANAN INFORMASI DI LINGKUNGAN BADAN PENGAWAS OBAT DAN MAKANAN

BAB I
PENGENDALIAN UMUM

1.1. Pendahuluan

Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik mengingat peran TIK yang semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik (*Good Corporate Governance*). Dalam penyelenggaraan tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama tata kelola TIK mengalami masalah keamanan informasi. Ada 3 (tiga) aspek utama dalam keamanan informasi.

1. *Confidentiality* yaitu suatu aspek yang memastikan data atau informasi dapat diakses sesuai dengan kewenangan yang diberikan dan menjaga informasi dari akses oleh pihak yang tidak berkepentingan.
2. *Integrity* yaitu suatu aspek yang memastikan bahwa data atau informasi tidak boleh berubah tanpa seizin pemilik data sehingga terjaga akurasi dan kelengkapannya.
3. *Availability* yaitu suatu aspek yang menjamin data dan informasi dapat tersedia dan diakses kapanpun pada saat dibutuhkan.

Data yang disimpan oleh Badan POM merupakan data yang memiliki nilai bagi organisasi, sehingga diperlukan suatu kontrol untuk pelakukan perlindungan terhadap data tersebut. Ketiga aspek dari keamanan informasi menjadi dasar untuk melakukan pengamanan terhadap sistem atau data.

1.2. Tujuan

Agar aset informasi yang dikelola Badan POM dapat terlindungi dengan baik, perlu pengamanan yang menyeluruh dan terintegrasi pada setiap aspek yang

ada. Untuk menerapkan proses pengamanan informasi di lingkungan Badan POM diperlukan beberapa proses dan kontrol yang diperlukan untuk menjaga dan melindungi aset informasi yang dikelola. Lampiran ini menjadi pedoman bagi unit kerja di lingkungan Badan POM dalam penerapan suatu sistem manajemen keamanan informasi.

Tujuan dari implementasi sistem pengelolaan keamanan informasi ini adalah:

1. Mendukung Badan POM dalam proses kerja penyelenggaraan dan pengelolaan data dan informasi yang mendukung tugas pokok dan fungsi Badan POM.
2. Melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi yang tersimpan di Badan POM dari segala bentuk gangguan dan ancaman baik dari dalam maupun luar, yang dilakukan secara sengaja atau tidak
3. Sebagai panduan dalam penerapan tatakelola keamanan informasi secara efektif, efisien, dan konsisten dengan pendekatan berbasis risiko.
4. Menumbuhkan dan meningkatkan kepercayaan para pihak yang terkait dan berkepentingan terhadap pengelolaan informasi di Badan POM

1.3. Sasaran Penyelenggaraan Keamanan Informasi adalah:

a. terselenggaranya layanan sistem elektronik yang memperhatikan tingkat keamanan sistem dan informasi
b. terlaksananya peningkatan proses keamanan informasi di lingkungan Organisasi Badan POM untuk menghasilkan pelayanan publik yang optimal
c. terlaksananya maksud dan tujuan pengelolaan keamanan informasi dalam hal perencanaan, pengelolaan dan pemanfaatan teknologi informasi
d. terwujudnya prinsip aksesibilitas terhadap pengelolaan dan penggunaan teknologi informasi

1.4. Ruang Lingkup

Kebijakan ini berlaku untuk pengelolaan pengamanan seluruh aset informasi Badan POM dan dilaksanakan oleh seluruh unit kerja, pegawai Badan POM baik sebagai pengguna maupun pengelola Teknologi Informasi dan Komunikasi (TIK), dan pihak ketiga di lingkungan Badan POM. Ruang lingkup dalam Keputusan Kepala Badan ini adalah :

a. Tanggung Jawab pengendalian Keamanan Informasi
b. Perencanaan Proses Keamanan Informasi
c. Penerapan Pengendalian Keamanan Informasi.

d. Evaluasi dan Perbaikan Proses Keamanan Informasi.
e. Pengawasan Proses Keamanan Informasi

1.5. Definisi

Berikut ini adalah definisi dari beberapa istilah yang digunakan di dalam dokumen kebijakan pengelolaan keamanan informasi ini yaitu:

a. Aset Badan POM adalah aset dalam bentuk:
   1. Data/dokumen meliputi: data gaji, data kepegawaian, dokumen penawaran, tender dan kontrak dengan pihak ketiga yang terkait dengan pengamanan data Badan POM, dokumen perjanjian kerahasiaan, kebijakan Badan POM, hasil penelitian, dan dokumentasi sistem manajemen keamanan informasi (misalnya: dokumen kebijakan pengelolaan keamanan infomasi, bahan pelatihan, prosedur operasional, rencana kelangsungan kegiatan, hasil audit dan lain lain)
   2. Perangkat lunak meliputi: perangkat lunak aplikasi, perangkat lunak sistem, dan perangkat lunak pembantu pengembangan sistem
   3. Aset fisik meliputi: perangkat komputer, perangkat jaringan komunikasi (Router, Modem, Switch, Kabel, Firewal), removable media, dan perangkat pendukung (UPS, Genset, *Fire Extinguisher, Access Door Electronic,* HVAC , A/C, CCTV, Sensor Suhu, Sensor Temperatur, Sensor Air)
   4. Aset Personil meliputi: pegawai tetap, honorer, dan pihak ketiga (vendor).

b. Aset Informasi adalah segala sesuatu yang mempunyai nilai bagi Badan POM
c. Informasi meliputi:
   1. Informasi tercetak

      Informasi banyak tertulis dalam bentuk kertas, meskipun mula-mula dihasilkan dari sebuah komputer.Kertas sebagai media penyimpan informasi masih sangat penting dan tinggi penggunaannya mengingat pertimbangan-pertimbangan legal, kebiasaan atau kenyamanan dalam membacanya. Risiko informasi dalam bentuk kertas antara lain: hilang, rusak (tidak bisa dibaca isinya), tercecer dan dibaca oleh orang yang tidak berhak
   2. Informasi elektronik

      Informasi jenis ini disimpan dalam media elektronik, baik dalam kurun waktu pendek atau lama sesuai masa berlakunya.Semula informasi disimpan dalam sebuah hard disk, kemudian disalin (back-up) ke dalam

media lainnya, seperti floppy disk, CD-ROM, flash disk dan tape. Keamanan media-media ini harus dilindungi secara fisik atau logik sesuai tingkat klasifikasi informasinya. Risiko informasi dalam bentuk elektronik: hilang/dihapus, rusak/corrupt (tidak bisa dibaca isinya), tersebar kemana-mana secara tidak sah dan dibaca oleh orang yang tidak berhak.

3. Unit kerja adalah organisasi di lingkungan Badan POM setingkat eselon II, termasuk Unit Pelaksana Teknis.
4. Dokumen adalah rujukan kerja tertulis yang dapat berupa, tetapi tidak terbatas pada, kebijakan, prosedur, standar, atau pedoman yang menjadi bagian dari kerangka kerja. Dokumen bisa berbentuk file elektronik (*softcopy*) atau cetakan (*hardcopy*)
5. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi.
   Catatan: Sifat- sifat informasi yang lain seperti keaslian (*authenticity*), akuntabilitas (*accountability*), non-repudiation dan keandalan (*reliability*) dapat juga dimasukkan sebagai keamanan informasi.
6. Kebijakan Pengelolaan Keamanan Informasi adalah kerangka kerja manajemen pengamanan aset informasi yang menggunakan pendekatan berbasis risiko dalam menyusun, menerapkan, melaksanakan, mengawasi, mengkaji, memelihara dan meningkatkan kinerja keamanan informasi
7. Pemilik Aset Informasi adalah pihak yang secara hukum ditunjuk sebagai penanggung jawab aset informasi atau proses kerja di Badan POM /pimpinan unit organisasi dimana data/ informasi itu dibuat.
8. Pejabat Keamanan Informasi adalah pejabat setingkat Eselon II yang ditunjuk oleh Kepala Badan POM untuk mengkoordinasikan dan mengarahkan kegiatan penerapan kebijakan dan prosedur keamanan informasi di lingkungan Badan POM .
9. Petugas Keamanan Informasi adalah personil setingkat Eselon IV yang ditunjuk oleh Kepala Unit kerja atau setingkat eselon II di Badan POM untuk melaksanakan kegiatan penerapan kebijakan dan prosedur keamanan informasi di lingkungan Badan POM tempat dia ditugaskan. Petugas bekerja dibawah pengawasan dan pengarahan Pejabat Keamanan Informasi.
10. Hak Akses adalah kewenangan terkait penggunaan suatu aset informasi yang jenis dan tingkatannya disesuaikan dengan kebutuhan kerja dan

risiko keamanan informasi. Hak ini, tergantung dari jenis asetnya secara formal diberikan atau disahkan oleh pemilik aset atau atasan langsung.

11. Kajian Risiko adalah keseluruhan proses analisa dan evaluasi risiko.
12. Evaluasi Risiko adalah proses yang membandingkan estimasi besaran suatu risiko dengan kriteria yang sudah terdefinisi untuk menetapkan tingkatan risiko.
13. Komite Pengarah Keamanan Informasi adalah suatu badan yang memberikan arahan terhadap masukan proyek TI dan penanganan masalah atau risiko-risiko yang signifikan dan berdampak pada kegiatan operasional Badan POM.
14. Insiden keamanan informasi adalah kejadian yang tidak diinginkan dan yang melanggar kebijakan atau prosedur Sistem Manajemen Keamanan Informasi (SMKI) sehingga menimbulkan ancaman terhadap kondisi keamanan aset informasi atau mengakibatkan gangguan terhadap proses kerja organisasi.
15. *Mobile Computing* adalah penggunaan perangkat komputasi jinjing (portabel) seperti notebook dan smart phone untuk melakukan akses, pengolahan data dan penyimpanannya.
16. *Teleworking* adalah penggunaan teknologi telekomunikasi untuk memungkinkan karyawan bekerja di suatu lokasi yang jauh dari kantor.
17. Kelemahan (*vulnerability*) adalah kerentanan suatu aset atau kontrol yang dapat dimanfaatkan untuk menimbulkan ancaman (*threat*).
18. Panduan adalah rekomendasi tindakan yang dianjurkan dapat dilakukan untuk mencapai suatu sasaran.
19. Prosedur adalah urutan kegiatan dari suatu proses yang melibatkan satu atau beberapa unit kerja dalam suatu organisasi
20. Rekaman adalah dokumen yang menyatakan hasil yang dicapai atau memberi bukti suatu aktivitas dilakukan.
21. Sasaran Kontrol (*Control Objective*) adalah pernyataan yang menggambarkan apa yang harus dicapai sebagai hasil dari penerapan kontrol.
22. Sistem Manajemen Keamanan Informasi (SMKI) adalah bagian dari keseluruhan sistem manajemen organisasi untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara dan meningkatkan keamanan informasi. SMKI dibangun dengan pendekatan risiko.

23. Pihak ketiga yang dimaksud adalah seluruh pihak yang terkait dan berkepentingan yang berada di luar struktur organisasi Badan POM.
24. Pengguna adalah pihak atau personil yang dapat mengakses sistem informasi berdasarkan user *account* yang telah diberikan.
25. Hak akses khusus adalah izin atau hak istimewa yang diberikan kepada pengguna, program atau *workstation* untuk membuat, mengubah, menghapus atau melihat data dan file dalam sebuah sistem.

1.6. Prinsip Pengelolaan Keamanan Informasi

Kebijakan Pengelolaan Keamanan Informasi didasarkan pada prinsip-prinsip sistem manajemen keamanan informasi sesuai dengan pesyaratan standard dan peraturan perundang-undangan yang berlaku.

Adapun Prinsip Umum Kebijakan Pengelolaan Keamanan Informasi sebagai berikut:

a. Pengelolaan keamanan Badan POM merupakan faktor penting dalam meningkatkan kinerja Badan POM dan menjadi salah satu pendorong untuk mencapai visi, misi, tujuan, strategis, indikator kinerja utama dan program sesuai tugas dan fungsi Badan POM.
b. Penerapan *Good IT Governance* dimana para pemangku kepentingan memiliki kesepakatan untuk bekerjasama dalam melakukan perencanaan, pengadaan, penerapan dan pengawasan terhadap sumber daya TIK, yang terdiri dari informasi, aplikasi, infrastruktur dan sumber daya manusia.
c. Data milik Badan POM merupakan aset yang dikelola dengan prinsip TRUST (*complete*/ lengkap, *Reliable*/ handal, *Up to date*/ terkini, *Secure*/ aman, *accurate*/ akurat)
d. Pemanfaatan data sesuai klasifikasinya harus:
    1. mendukung aspek kepentingan Badan POM secara menyeluruh dalam bentuk kolaborasi antar unit pengguna layanan.
    2. secara proaktif membantu proses pengambilan kebijakan dan keputusan oleh pimpinan.
    3. mendukung terwujudnya transparansi informasi kepada publik.
e. Badan POM menetapkan standar TIK dengan mengadopsi teknologi yang telah mapan, legal dan diterima di pasar, dengan tujuan mendukung penerapan keamanan pada aset informasi.
f. Badan POM membuat rencana pemulihan bencana (*Disaster Recovery Plan*) yang teruji dalam mengatasi dampak bencana untuk menjamin kelangsungan kegiatan Badan POM.

1.7. Standar Acuan

Standar yang digunakan sebagai acuan di dalam pembuatan kebijakan pengelolaan keamanan informasi ini adalah:

a. SNI ISO/IEC 27001:2013 dan SNI ISO/IEC 27002:2013
   Standard SNI ISO 27001 adalah suatu standar khusus yang terstruktur tentang pengamanan informasi melalui Sistem Manajemen Keamanan Informasi (SMKI) yang memberikan gambaran secara umum mengenai kontrol keamanan saja yang harus dilakukan oleh sebuah organisasi dalam usaha mereka untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi di organisasi dalam pengamanan informasi.
b. kerja dan melakukan peninjauan secara berkala terkait kemampuan unit kerja untuk menerapkan pada seluruh proses bisnis.

2.1. Kepemimpinan

Pimpinan Unit Kerja harus memastikan tanggung jawab dalam penerapan sistem manajemen keamanan melalui :

a. Komitmen seluruh personil di unit kerja dalam:
   1. Penerapan kebijakan dan pencapaian keamanan informasi.
   2. Pengelolaan ketersediaan dari sumber daya yang dibutuhkan dalam rangka implementasi keamanan informasi.
   3. Memastikan koordinasi implementasi kontrol keamanan informasi terhadap data dan informasi yang dikelola telah dilakukan secara berkala.
   4. Peningkatan yang berkesinambungan yang dijabarkan dalam program aktivitas SMKI.
   5. Bertanggung jawab atas terlaksananya kontrol keamanan informasi untuk memastikan perlindungan terhadap data dan informasi yang dikelola.
   6. Berkerjasama dengan pejabat keamanan informasi untuk memastikan perlindungan terhadap asset Informasi.
b. Menetapkan dan menjalankan tugas dan tanggung jawab yang ditentukan terkait pengelolaan kontrol keamanan informasi di Unit Kerja.

2.2. Perencanaan Kontrol Keamanan Informasi

Berikut ini adalah gambaran umum proses manajemen risiko yang digunakan oleh Unit kerja di dalam pengelolaan risikonya:

a. Unit kerja di lingkungan Badan POM harus mendefinisikan kerangka pengelolaan risiko yang sesuai dengan Kebijakan Pengelolaan Keamanan Informasi, hukum, undang-undang serta peraturan berlaku dan kegiatan terkait.
b. Badan POM akan melakukan kajian risiko (*risk assessment*) secara periodik terhadap aset-aset informasi yang tercatat untuk menemukan ancaman (*threat*) dan kelemahan (*vulnerability*) keamanannya serta dampak risiko yang mungkin ditimbulkannya. Tingkat kedalaman kajian risiko akan disesuaikan berdasarkan tingkat kerahasian dan tingkat kerawanan informasi.
c. Metode-metode penanganan risiko dan kontrol-kontrol keamanan informasi akan diterapkan untuk mencegah atau mengurangi dampak risiko yangditemukan.
d. Proses manajemen risiko keamanan informasi diterapkan dengan menghasilkan output sebagai berikut:
    1. Profil risiko keamanan informasi di unit Kerja yang mencakup aset penting terkait keamanan informasi.
    2. Rencana peningkatan tindakan pengendalian risiko (*risk treatment plan*) keamanan informasi di unit Kerja.
e. Proses pelaksanaan manajemen risiko harus dilakukan minimal satu kali dalam satu tahun dan keluaran (output) dari proses manajemen risiko harus mendapat persetujuan manajemen pimpinan unit kerja sebelum dapat diterapkan.
f. Proses manajemen risiko dilakukan melalui proses iteratif yang mencakup aktivitas penilaian risiko, penanganan risiko, penerimaan risiko dan pengkomunikasian risiko.
g. Proses penilaian risiko yang dilakukan dengan memepertimbangkan aktivitas sebagai berikut:
    1. Identifikasi risiko keamanan informasi yang meliputi penerapan proses penilaian risiko terkait kritikalitas atas tingkat kerahasiaan, integritas dan ketersediaan informasi.
    2. Analisis tiap risiko keamanan informasi, mencakup:
        a. menilai konsekuensi potensial yang akan terjadi.
        b. menilai kemungkinan realistis terjadinya risiko yang teridentifikasi
        c. menentukan tingkat risiko.
        d. menentukan pemilik risiko (*risk owner*) dalam masing-masing risiko yang teridentifikasi.

3. Mengevaluasi tiap risiko keamanan informasi, mencakup:
   a. Membandingkan hasil analisis risiko dengan kriteria risiko dan
   b. Memberikan prioritas risiko yang telah dianalisis untuk tiap penanganan risiko.

h. Sedangkan proses pengendalian risiko memperhatikan aktivitas sebagai berikut :
   1. Memilih opsi penanganan risiko yang memadai dengan mempertimbangkan hasil penilaian risiko.
   2. menentukan kontrol risiko yang dibutuhkan untuk implementasi dari opsi penanganan risiko keamanan informasi yang dipilih. Pemilihan dari kontrol tersebut dapat memperhatikan kontrol keamanan informasi berdasarkan standar ISO 27001:2013 atau kontrol lainnya pada peraturan perundang-undangan yang berlaku.
   3. merencanakan penanganan risiko keamanan informasi yang tertuang dalam rencana penanganan risiko.

i. Untuk memastikan efektifitas dari penerapan kontrol keamanan informasi maka unit kerja perlu menetapkan sasaran keamanan informasi untuk mengevaluasi kinerja keamanan informasi dengan mempertimbangkan:
   1. Konsisten dengan penetapan kontrol dalam kebijakan pengelolaan keamanan informasi yang tertuang dalam dokumen ini.
   2. Dapat diukur.
   3. Mempertimbangkan terkait persyaratan keamanan informasi dan hasil dari penilaian dan pengendalian risiko.
   4. Harus dikomunikasikan ke pihak terkait.
   5. Secara berkala dievaluasi dan dilakukan pengkinian sesuai perubahan tujuan keamanan inforamsi dari unit kerja.

j. Penetapan sasaran keamanan informasi harus mencakup penentuan dari:
   1. Tujuan yang perlu diperhatikan.
   2. sumber daya yang dibutuhkan.
   3. penanggung jawab dari pelaksanaan sasaran tersebut.
   4. target penyelesaian.
   5. bagaimana sasaran tersebut dievaluasi hasilnya.

2.3. Dukungan Keamanan Informasi

Dukungan terhadap penerapan keamanan informasi perlu dilakukan melalui :

a. penentuan dan penyediaan sumber daya yang dibutuhkan untuk membentuk, implementasi, pemeliharaan dan peningkatan secara

berkesinambungan dari penerapan sistem manajemen keamanan informasi yang mencakup:

1. Sumber daya dengan kompetensi dan pemahaman yang memadai, dokumentasi, proses dan solusi teknis, baik berupa perangkat keras maupun perangkat lunak.
2. Perencanaan sumber daya SMKI dapat dilakukan bersamaan dengan proses perencanaan dan penyusunan anggaran tahunan di unit kerja.

b. Unit kerja secara kontinu melakukan sosialisasi dan pelatihan mengenai SMKI ke seluruh pegawai. Sosialisasi dapat dilakukan dengan berbagai cara, seperti:
   1) Tatap muka di dalam kelas
   2) Penyampaian brosur, *leaflet*, spanduk untuk meningkatkan kepedulian karyawan
   3) Penggunaan email, nota dinas, portal atau majalah internal
   4) Media komunikasi lainnya
c. Bukti sosialisasi dan pelatihan baik berupa materi, daftar hadir, hasil *pre/post test*, laporan evaluasi pelatihan ataupun sertifikat harus disimpan dan dipelihara.
d. Komunikasi yang relevan dengan SMKI, baik internal maupun eksternal, harus dikendalikan dan dikoordinasikan untuk memastikan:
   1) Efektivitas alur pertukaran informasi dalam organisasi SMKI dan/atau dari dan ke pihak eksternal
   2) Jalur komunikasi SMKI mencakup:
      i. Komunikasi tatap muka
      ii. Surat dan memo internal
      iii. Email
      iv. Website Badan POM
      v. Pengumuman
      vi. Material cetak
e. Informasi terkait dengan keamanan informasi yang berasal dari sumber eksternal harus ditinjau dan didistribusikan kepada pihak yang relevan dalam SMKI organisasi. Hal ini mencakup:
   1) Penerbitan peraturan hukum dan perundangan yang baru maupun perubahan terhadap peraturan lama;
   2) Usulan perubahan terhadap prasyarat keamanan informasi;
   3) Teknologi, ancaman dan kelemahan baru terkait keamanan informasi.

2.4. Dokumentasi Keamanan Informasi

Proses dokumentasi pengelolaan keamanan informasi yang harus dijadikan panduan oleh unit kerja yang meliputi :

a. Unit kerja perlu untuk mengembangkan dan memelihara dokumentasi pengelolaan keamanan informasi yang terdiri dari :
   1) Pedoman Sistem Manajemen Keamanan Informasi, menjelaskan uraian singkat sistem manajemen keamanan informasi dan kebijakan keamanan informasi di lingkup Unit Kerja serta kesesuaiannya dengan standar SNI ISO/IEC 27001:2013.
   2) Prosedur, menjelaskan rincian metode dan cara kerja pelaksanaan proses/sistem manajemen keamanan informasi di Unit Kerja.
   3) Metodologi Risk Assessment, menjelaskan metode pelaksanaan penilaian risiko dan termasuk di dalamnya daftar risiko dan rencana penanganan risiko terkait pengamanan informasi.
   4) Dokumen Statement of Applicability, menjelaskan kontrol – kontrol pengamanan informasi sesuai dengan SNI ISO/IEC 27001:2013 yang diimplementasikan di Unit Kerja.
   5) Dokumen Pendukung, sebagai penunjang pelaksanaan Prosedur dan Instruksi Kerja yang dibuat, dapat berupa formulir, catatan hasil kegiatan serta dokumen lainnya.
b. Dokumentasi pengelolaan keamanan informasi harus tersedia di seluruh area operasional dan mudah diakses oleh pengguna yang memerlukan, dikelola secara efektif dan dikendalikan penggunaannya, dipelihara kemutakhirannya serta dilindungi dari penggunaan yang tidak berwenang.
c. Pengendalian dokumen pengelolaan keamanan informasi dilakukan demi menjaga efektivitas pelaksanaan operasionalnya, menghindarkan dari segala jenis kerusakan dan mencegah akses oleh yang tidak berwenang.
d. Pengendalian catatan penerapan dan pelaksanaan kebijakan keamanan informasi bertujuan untuk menjamin agar catatan tersebut dapat tersedia,terpelihara dan terkendali.
e. Catatan digunakan untuk mengukur kepatuhan dan efektivitas penerapan Kebijakan Pengelolaan Keamanan Informasi.
f. Semua dokumentasi SMKI harus ditinjau paling sedikit satu kali dalam 1 (satu) tahun atau apabila terdapat perubahan dalam SMKI dan/atau organisasi untuk menjamin kesesuaian dan kecukupannya

2.5. Operasional Keamanan Informasi

Unit kerja harus menetapkan proses perencanaan dan pengendalian operasional sistem manajemen keamanan informasi yang mencakup :

a. Proses perencanaan operasional SMKI harus dilakukan secara tahunan serta dokumentasikan dan dikomunikasikan kepada pihak yang terkait dengan pihak yang terkait dengan SMKI.
b. Proses pengendalian operasional SMKI adalah proses yang dilakukan untuk memastikan pelaksanaan operasional SMKI unit kerja telah sesuai dengan perencanaan yang telah dibuat. Proses pengendaliaan ini dapat mencakup aktifitas rapat peninjauan dan harus dilakukan paling sedikit satu kali dalam tiga bulan serta melibatkan personil yang terlibat di unit kerja.
c. Untuk menunjang penyelenggaraan sistem elektronik, Setiap Organisasi Badan POM penyelenggara Sistem Elektronik harus merencanakan proses keamanan informasi dalam penyelenggaraan Teknologi Informasi.
d. Perencanaan proses Keamanan Informasi yang mencakup penetapan kebijakan dan sasaran sistem manajemen keamanan informasi.
e. Pimpinan Organisasi Badan POM harus memastikan tingkat pemahaman terkait proses keamanan informasi kepada seluruh pegawai di lingkungan Organisasi Badan POMnya.

2.6. Evaluasi Pengelolaan Keamanan Informasi

Unit Kerja harus melakukan aktivitas pelaksanaan evaluasi SMKI untuk melihat kinerja dan mengevaluasi efektifitas pelaksanaan pengelolaan keamanan informasi:

a. Unit kerja harus melakukan evaluasi pengelolaan keamanan informasi untuk melihat kinerja dan efektifitas pelaksanaan Kebijakan Pengelolaan Keamanan Informasi. Pengkajian dilakukan secara berkala minimum sekali setahun.
b. Penetapan evaluasi kinerja kontrol keamanan mencakup :
    1) Pendefinsian parameter dan indikator yang perlu dipantau dan diukur, termasuk proses dan kontrol keamanan informasi
    2) Penentuan metode untuk pemantauan, pengukuran, analisis dan evaluasi untuk memastikan hasil yang valid
    3) Penentapan periode dan penanggung jawab pelaksana pemantauan dan pengukuran yang ditetapkan melalui ketetapan pimpinan
    4) Parameter pengukuran yang telah ditentukan harus memungkinkan evaluasi dari pencapaian sasaran SMKI

c. Proses pengukuran harus dilakukan minimal satu kali dalam satu tahun terutama untuk mengukur pencapaian dari sasaran SMKI.
d. Hasil dari evaluasi harus didokumentasikan secara jelas, dipelihara dan ditindaklanjuti.
e. Unit Kerja dapat melakukan proses audit internal dengan ketentuan sebagai berikut:
    1) Audit internal SMKI harus dilaksanakan minimal satu kali dalam satu tahun dan harus mencakup seluruh ruang lingkup SMKI
    2) Audit internal harus dilakukan oleh auditor yang memiliki kompetensi yang memadai berupa sertifikasi di bidang auditor keamanan informasi serta memiliki objektifitas dan inedependen terhadap proses audit dan ditunjuk secara formal oleh pimpinan unit kerja
    3) Sebuah program audit tahunan harus ditetapkan oleh koordinator audit internal SMKI dan harus dikomunikasikan kepada Pimpinan Unit Kerja yang mencakup jadual, metode, kriteria dan ruang lingkup, tanggung jawab serta prasyarat pelaporan dari audit
    4) Proses audit harus dilakukan sesuai dengan program audit yang telah ditetapkan secara formal
    5) Setiap ketidaksesuaian dan/atau peluang untuk perbaikan yang ditemukan dalam proses audit harus dicatat secara formal oleh auditor dan ditentukan jangka waktu yang disepakati oleh auditee dengan cara merencanakan dan melaksanakan koreksi dan tindakan korektif
    6) Laporan audit harus dilaporkan kepada pimpinan unit kerja dan dikomunikasikan kepada seluruh pegawai unit kerja
    7) Pejabat Keamanan Informasi dan auditor internal SMKI bertanggung jawab untuk memantau dan memverifikasi koreksi, tindakan korektif maupun peningkatan terkait ketidaksesuaian yang ditemukan dalam audit
f. Pimpinan Unit Kerja wajib untuk melaksanakan tinjauan manajemen SMKI minimal satu kali dalam satu tahun untuk menjamin terjaganya kesesuaian, kecukupan dan efektivitas dari SMKI dengan ketentuan sebagai berikut:
    1) Tinjauan manajemen SMKI harus dihadiri oleh:
        i. Pimpinan Unit Kerja
        ii. Pejabat Keamanan informasi di Unit kerja

iii. Petugas keamanan informasi di Unit Kerja

iv. Apabila dibutuhkan, tinjauan manajemen dapat dihadiri oleh Pemangku kepentingan yang relevan dan Subject matter expert yang memadai.

2) Tinjauan manajemen SMKI harus mencakup masukan sebagai berikut:

i. Status dari tindakan yang diputuskan pada tinjauan manajemen terdahulu

ii. Perubahan baik internal maupun eksternal yang terkait SMKI

iii. Masukan terkait kinerja keamanan informasi yang mencakup trend pada:

1) Ketidaksesuaian dan tindakan korektif

2) Hasil pemantauan dan pengukuran

3) Hasil audit, baik internal maupun eksternal

4) Pemenuhan dari sasaran keamanan informasi

iv. Masukan dari pihak terkait

v. Hasil dari assessment risiko dan status rencana penanganan risiko

vi. Peluang untuk peningkatan secara berkesinambungan.

3) Berdasarkan dari masukan tersebut, tinjauan manajemen SMKI harus menghasilkan keluaran sebagai berikut:

i. Keputusan terkait peningkatan SMKI secara berkesinambungan

ii. Peluang dan kebutuhan untuk perubahan SMKI.

4) Setiap keluaran dari tinjauan manajemen SMKI harus digunakan sebagai dasar bagi peningkatan dan perencanaan tahunan SMKI

2.7. Peningkatan Pengelolaan Keamanan Informasi

Unit Kerja harus memastikan adanya upaya berkelanjutan dari Badan POM untuk meningkatkan kinerja dan efektifitas pengelolaan keamanan informasi:

1. meningkatkan efektivitas Kebijakan Pengelolaan Keamanan Informasi secara terus-menerus melalui penyempurnaan kebijakan dan sasaran keamanan informasi, hasil-hasil audit, hasil analisa terhadap gangguan/insiden keamanan informasi, tindakan koreksi dan pencegahan serta evaluasi manajemen keamanan informasi.
2. melakukan tindakan perbaikan terhadap terjadinya pelanggaran keamanan informasi dan melakukan pencegahan agar pelanggaran keamanan informasi tidak terjadi. Tindakan perbaikan dan pencegahan

dilakukan berdasarkan hasil analisa masalah-masalah keamanan informasi yang terjadi.

3. Untuk setiap ketidaksesuaian, evaluasi harus dilakukan untuk mengevaluasi kebutuhan untuk mengambil tindakan korektif untuk menghilangkan penyebab dari ketidaksesuaian supaya ketidaksesuaian tersebut tidak terjadi lagi atau terjadi ditempat lain.
4. Setelah koreksi dan tindakan korektif telah diambil, sebuah peninjauan harus dilakukan untuk menjamin efektifitasnya dalam mencegah terjadinya kembali atau terjadinya ketidaksesuaian tersebut.
5. Inisiatif peningkatan harus secara formal diidentifikasi, direncanakan, diimplementasikan dan ditinjau
6. Identifikasi dari peningkatan harus dilakukan berdasarkan log, laporan dan hasil dari:
7. Proses pengelolaan insiden keamanan informasi
8. Peninjauan internal SMKI
9. Proses audit internal SMKI
    a. Proses pemantauan dan pengukuran SMKI
    b. Peninjauan dan/atau proses audit eksternal terhadap SMKI
    c. Laporan dan masukan dari stakeholder yang terkait
    d. Perencanaan dan implementasi dari inisiatif peningkatan harus ditinjau untuk memastikan bahwa inisiatif tersebut dapat mencapai tujuannya
10. Dokumentasi yang relevan dengan proses peningkatan secara berkesinambungan harus dibuat dan dipelihara

BAB III
PENGENDALIAN ORGANISASI KEAMANAN INFORMASI

Bab ini bertujuan memberikan pedoman dalam membentuk organisasi fungsional keamanan informasi yang bertanggung jawab untuk mengelola keamanan informasi dan perangkat pengolah informasi di lingkungan Badan POM termasuk hubungan dengan pihak luar.

3.1. Organisasi Internal

3.1.1. Struktur Organisasi Tim Pengelola Keamanan Informasi Beserta Tanggung Jawabnya

Berikut ini adalah struktur organisasi tim pengelola keamanan informasi di Badan POM:

a. Kepala Badan POM memastikan tanggung jawab terkait proses keamanan informasi pada masing-masing peranan dalam struktur organisasi SMKI di lingkungan Badan POM.
b. Tanggung jawab dan kewenangan dari Organisasi Keamanan Informasi di Badan POM mencakup:
    1. Kepala Badan POM

        Fungsi Kepala Badan POM adalah mengawasi implementasi kebijakan keamanan informasi dalam penerapan sistem manajemen keamanan informasi. Tanggung jawab mencakup antara lain:

        a. mengarahkan, memantau dan mengevaluasi Rencana Strategis TI dan kebijakan penyelenggaraan TI
        b. melakukan pemantauan dan mengevaluasi kesesuaian antara kebijakan dengan penerapan manajemen risiko dalam penggunaan TI
        c. mereview, menyetujui dan memantau proyek-proyek teknologi yang berdampak secara signifikan terhadap operasional dan kondisi Badan POM
        d. Mengkoordinasikan perumusan dan penyempurnaan Kebijakan dan Standar Pengelolaan Keamanan Informasi di lingkungan Badan POM
        e. melakukan evaluasi terhadap pengelolaan pengamanan yang andal dan efektif atas TI guna menjamin ketersediaan, kerahasiaan, keakuratan informasi.

2. Pimpinan Unit Kerja

Wewenang dan tanggung jawab keamanan informasi bagi Pimpinan unit Kerja mencakup :

a. menetapkan Rencana pelaksanaan/pengembangan TI jangka pendek yang sejalan dengan rencana strategis TI di Badan POM
b. menetapkan kebijakan dan prosedur terkait penyelenggaraan keamanan informasi yang memadai dan mengkomunikasikannya secara efektif, baik pada unit kerja penyelenggara maupun pengguna TI
c. Menetapkan target keamanan informasi setiap tahunnya dan menyusun rencana kerja untuk Badan POM
d. Memonitor penerapan proses manajemen risiko dalam penggunaan TI yang dilaksanakan secara efektif dan memadai antara lain dengan:
    1) menumbuhkan risk awareness kepada seluruh pegawai
    2) memiliki dan mengkomunikasikan pemahaman yang jelas mengenai kriteria dan tingkat risiko yang dapat diterima oleh organisasi
    3) mengkomunikasikan risiko signifikan secara transparan kepada pegawai yang menghadapi risiko tersebut
    4) mengembangkan struktur organisasi beserta uraian tugas dan tanggung jawab yang dapat mengelola risiko yang dihadapi Unit Kerja secara komprehensif, sistematis dan terintegrasi.
e. Memastikan peningkatan kesadaran, kepedulian, dan kepatuhan seluruh pegawai terhadap Kebijakan dan Standar Pengelolaan Keamanan Informasi
f. terdapat sistem pengukuran kinerja proses penyelenggaraan keamanan informasi yang paling kurang dapat meningkatkan kinerja proses penyelenggaraan TI dan kualitas layanan
g. Memastikan langkah-langkah perbaikan sudah dilakukan berdasarkan saran dan rekomendasi yang diberikan dalam pelaksanaan evaluasi dan atau audit penerapan Kebijakan dan Standar Pengelolaan Keamanan Informasi.

3.Komite Pengarah Keamanan Informasi

Badan POM wajib memiliki Komite Pengarah Keamanan Informasi yang bertujuan untuk membantu Kepala Badan POM dalam mengawasi tindakan perbaikan dan peningkatan terkait keamanan informasi. Komite sekurang- kurangnya terdiri dari:

a. Pimpinan Unit Kerja yang membawahi fungsi Teknologi Informasi
b. Pimpinan Unit Kerja yang membawahi fungsi Manajemen Risiko
c. Pimpinan Unit Kerja yang membawahi fungsi audit
d. Pejabat Pelaksana Keamanan Informasi dari unit kerja yang membawahi unit kerja pengelola Infrastruktur dan TIK

Wewenang dan tanggung jawab Komite Pengarah keamanan informasi adalah memberikan rekomendasi kepada Kepala Badan POM yang paling kurang mencakup:

a. kesesuaian proyek-proyek TI yang disetujui dengan Rencana Strategis TI di Badan POM. Komite juga menetapkan status prioritas proyek TI yang bersifat kritikal (berdampak signifikan terhadap kegiatan Badan POM) misalnya pergantian sistem application utama;
b. Menentukan langkah-langkah dalam mitigasi risiko yang mempengaruhi kinerja dan reputasi Badan POM;
c. upaya penyelesaian berbagai masalah terkait TI, yang tidak dapat diselesaikan oleh unit kerja pengguna dan unit kerja penyelenggara. Komite dapat memfasilitasi hubungan antara kedua Unit kerja tersebut;

b. Unit kerja juga membentuk tim pengelolaan keamanan informasi untuk memastikan penerapan kontrol keamanan informasi di Unit kerja yang mencakup dan tidak terbatas pada:

1. Pejabat Pelaksana Keamanan Informasi

Tugas dan wewenang Pejabat Pelaksana Keamanan Informasi adalah sebagai berikut :

a. Memelihara dan mengendalikan penerapan Kebijakan dan Standar Pengelolaan Keamanan Informasi di seluruh area yang menjadi tujuan/ sasaran pengendalian.
b. Mengkoordinasikan pelaksanaan proses manajemen risiko SMKI di unit kerja.

c. Mengkoordinasikan pelaksanaan aktifitas SMKI serta pengamanan informasi di unit kerja dan peninjauan secara berkala terhadap implementasi SMKI di unit kerja.
d. Mendefinisikan kebutuhan, merekomendasikan, dan mengupayakan penyelenggaraan pendidikan dan pelatihan keamanan informasi bagi pegawai.
e. Mengkoordinasikan proses pengukuran efektivitas SMKI dan kontrol keamanan informasi di unit keerja.
f. Memastikan efektifitas dan konsistensi penerapan Kebijakan dan Standar Pengelolaan Keamanan Informasi di lingkungan unit kerja dan mengukur kinerja keseluruhan.
g. Memastikan terlaksananya audit internal terhadap penerapan Kebijakan dan Standar Pengelolaan Keamanan Informasi di unit kerja
h. Memberikan laporan secara berkala terkait kondisi SMKI dan keamanan informasi kepada pimpinan unit kerja terkait.

2. Petugas Pelaksana Keamanan Informasi

Tugas dan wewenang Petugas Pelaksana Keamanan Informasi adalah sebagai berikut :

a. Mengelola data inventaris aset pemrosesan dan penyimpan informasi yang digunakan dalam pelaksanaan proses transaksi informasi.
b. Melaksanakan dan mengawasi penerapan Kebijakan dan Standar Pengelolaan Keamanan Informasi di unit kerja.
c. Memastikan Kebijakan dan Standar Pengelolaan Keamanan Informasi di unit kerja diterapkan secara efektif.
d. memantau pengukuran efektivitas kontrol implementasi SMKI.
e. melakukan pemantauan dan pengkinian terhadap daftar risiko (risk register) terkait perkembangan ancaman pada proses bisnis.
f. Memberi panduan dan/ atau bantuan penyelesaian masalah-masalah keamanan informasi.
g. Melaporkan kinerja penerapan Kebijakan dan Standar Pengelolaan Keamanan Informasi di unt kerja sesuai ruang lingkup dan tanggung jawabnya kepada Pejabat Pengelola Keamanan Informasi yang akan digunakan sebagai dasar peningkatan keamanan informasi.

3. Tim pengelolaan standard, kebijakan, dan risiko

   Tugas dan wewenang Tim pengelolaan standard, kebijakan, dan risiko adalah sebagai berikut :

   a. Mengidentifikasi dan mendokumentasikan peraturan perundang-undangan dan kewajiban kontrak yang relevan dengan SMKI dan keamanan informasi.
   b. Menyusun dan mengevaluasi terlaksananya kebijakan dan prosedur keamanan informasi.
   c. Melakukan pemantauan berkala terhadap kepatuhan SMKI organisasi dengan prasyarat dari kebijakan dan prosedur SMKI organisasi serta peraturan peraturan perundang-undangan dan kewajiban kontrak yang relevan dengan SMKI dan keamanan informasi.
   d. Melakukan peninjauan terkait proses keamanan informasi berdasarkan berdasarkan peraturan perundang-undangan, kebijakan dan prosedur SMKI.
   e. Menyusun dan mengkoordinasikan aktivitas proses pengelolaan manajemen risiko SMKI di unit kerja.
   f. Mengkoordinasikan proses registrasi dan pengkinian secara rutin terhadap risiko SMKI di unit kerja.
   g. Menyusun dan memelihara dokumen risk profile dan risk treatment plan SMKI organisasi.

4. Tim Penanganan insiden keamanan informasi dan pemulihan kelangsungan bisnis

   Tugas dan wewenang Tim Penanganan insiden keamanan informasi dan pemulihan kelangsungan bisnis adalah sebagai berikut :

   a. Memantau, mencatat dan menguraikan secara jelas gangguan keamanan informasi yang diketahui atau laporan yang diterima, dan menindaklanjuti laporan tersebut sesuai prosedur penanganan insiden dan pelaporan gangguan keamanan informasi.
   b. Mengkoordinasikan dan memantau tindakan perbaikan terhadap insiden keamanan informasi dan peninjauan terhadap peningkatan perbaikan proses.
   c. Mengkoordinasikan dan memantau pengelolaan manajemen kelangsungan bisnis di unit kerja berdasarkan skenario bencana yang telah ditetapkan.

d. Memastikan terjaganya aspek keamanan informasi dalam proses manajemen kelangsungan bisnis.

5. Tim pengendali dokumen.

Tugas dan wewenang Tim pengendali dokumen adalah sebagai berikut :

a. Mengkoordinasikan dan memantau proses pengelolaan dokumentasi terkait SMKI. Hal ini mencakup kebijakan dan prosedur terkait SMKI unit kerja.
b. Menyusun dan mengkoordinasikan pelaksanaan program security awareness bagi personil organisasi.
c. Mendokumentasikan hasil pengukuran efektivitas SMKI dan kontrol keamanan informasi.

3.1.2. Pemisahan Tugas dan Tanggung Jawab

a. Pimpinan Unit Kerja menjamin dilakukannya pemisahan tugas pada proses-proses kerja yang melibatkan informasi kritikal agar tidak ada pegawai yang memiliki kontrol menyeluruh terhadap semua aset informasi.
b. Pemisahan tugas tanggung jawab meliputi pembagian terhadap kewenangan terkait penginputan, validasi, persetujuan dan lainnya terhadap transaksi informasi yang dilakukan.

3.1.3. Hubungan dengan Pihak Berwenang

Unit Kerja harus mengidentifikasi dan menjalin kerjasama dengan pihak-pihak berwenang di luar Badan POM yang terkait dengan keamanan informasi.

3.1.4. Hubungan dengan Komunitas Keamanan Informasi

a. Unit Kerja harus menjalin kerjasama dengan komunitas keamanan informasi di luar Badan POM yang terkait dengan keamanan informasi.
b. Tujuan dari keikutsertaan komunitas keamanan informasi untuk mendapatkan informasi mengenai pengkinian teknologi dan referensi keamanan informasi, ancaman yang sedang terjadi, dan informasi solusi terhadap penanganan kejadian keamanan informasi. Informasi tersebut harus dikomunikasikan ke pihak yang terkait di lingkungan unit kerja dan Badan POM.

c. Unit kerja di Badan POM harus menyimpan *emergency contact number, mailing list, contact number* dari pihak – pihak yang dibutuhkan saat terjadi isu di keamanan informasi seperti PLN, Petugas Keamanan, Kepolisian, pihak ketiga pengelola infrastruktur, dan para ahli di bidang Keamanan Informasi.

3.1.5. Keamanan Informasi dalam Manajemen Proyek

a. Unit kerja di Badan POM mempertimbangkan aspek keamanan informasi dalam manajemen proyek yang dilaksanakan di Badan POM.
b. Setiap informasi yang diakses selama pelaksanaan proyek yang terkait dengan Badan POM harus memperhatikan aspek perlindungan dari kerahasiaan informasi di dalam pengelolaannya untuk mencegah kebocoran data.

3.2. Penggunaan Perangkat Mobile dan Teleworking

3.2.1. Aturan penggunaan perangkat mobile

a. Penggunaan perangkat mobile, baik milik pribadi atau milik institusi untuk mengakses dan/atau menyimpan informasi yang dikelola unit kerja harus sangat dibatasi sesuai dengan kebutuhan pekerjaan dengan mempertimbangkan prinsip kehati-hatian saat menggunakan perangkat mobile dengan menghindari meninggalkan perangkat tanpa pengawasan.
b. Perangkat mobile harus mengaktifkan fitur otentikasi pengguna, seperti penggunaan user name dan password, sesuai dengan kebijakan terkait pengendalian akses.
c. Informasi sensitif milik Unit Kerja yang disimpan pada perangkat mobile device harus di-backup secara berkala untuk menghindari hilangnya aspek ketersediaan dari informasi.

3.2.2. Teleworking

a. Aktivitas teleworking sebagai sarana pegawai untuk bekerja dari lokasi di luar area kerja Badan POM dengan mengakses jaringan internal secara remote melalui jaringan internet diperbolehkan namun sangat dibatasi hanya untuk personil yang diberi izin berdasarkan kebutuhan pekerjaannya

b. Akses ke jaringan internal Badan POM dari jaringan internet harus menggunakan koneksi aman dengan menggunakan antara lain teknologi VPN

c. Fitur teknologi yang diperbolehkan untuk digunakan dalam pelaksanaan teleworking sebagai berikut:

   1) perangkat akses (misalnya notebook) yang digunakan untuk teleworking harus terinstalasi *firewall* dan antivirus

   2) mekanisme akses terhadap sistem atau aplikasi disesuaikan dengan klasifikasi aset informasi:

      i. informasi publik : dapat diakses langsung.

      ii. informasi rahasia :

         a. harus menggunakan protokol HTTPS atau SSH

         b. harus menggunakan VPN, sebelum kemudian mengakses melalui protokol HTTPS atau SSH.

BAB IV
PENGENDALIAN KEAMANAN SUMBER DAYA MANUSIA

Keamanan sumber daya manusia bertujuan memastikan bahwa seluruh pegawai dan pihak ketiga di lingkungan Badan POM memahami tanggung jawabnya masing-masing, sadar atas ancaman keamanan informasi serta mengetahui proses terkait keamanan informasi sebelum, selama, dan setelah bertugas.

4.1 Sebelum Menjadi Karyawan Badan POM

4.1.1 Skrining Pegawai

a. Seluruh pegawai yang akan bekerja di Unit Kerja harus diperiksa data pribadinya sesuai dengan peraturan perundang-undangan yang berlaku.
b. Fungsi kepegawaian di Unit kerja akan melakukan penelitian dan pemeriksaan pada data pribadi dan keterangan pekerjaan sebelumnya yang diberikan oleh pegawai baru, atau mitra kerja sesuai dengan kebijakan penerimaan pegawai/mitra kerja yang berlaku.
c. Pemeriksaan latar belakang calon pegawai dan pihak ketiga harus memperhitungkan privasi, perlindungan data pribadi dan/ atau pekerjaan berdasarkan undang-undang, meliputi:
    1) Ketersediaan referensi
    2) Pemeriksaan kelengkapan dan ketepatan dari riwayat hidup pemohon
    3) Konfirmasi kualifikasi akademik dan profesional yang diklaim
    4) Pemeriksaan independen identitas (paspor atau dokumen yang sama)
    5) Pemeriksaan lebih rinci seperti pemeriksaan kredit atau pemeriksaan dari catatan kriminal

4.1.2 Syarat dan Kondisi Pekerjaan

a. Seluruh pegawai yang bekerja di Unit kerja, mitra dan pihak ketiga lainnya harus mematuhi kebijakan dan prosedur keamanan informasi yang berlaku di Badan POM
b. Pegawai, mitra kerja, dan pihak ketiga lainnya yang akan menggunakan aset informasi yang tergolong RAHASIA dan SANGAT RAHASIA harus menyetujui dan menandatangani perjanjian

Kesepakatan Kewajiban Menjaga Rahasia *(Non-Disclosure Agreement/ NDA)* dan ketentuan lainnya sebelum mulai bekerja.

c. Peran dan tanggung jawab pegawai, mitra kerja, dan pihak ketiga lainnya terhadap keamanan informasi didefinisikan, didokumentasikan dan dikomunikasikan kepada yang bersangkutan sebelum penugasan.

d. Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menjadi bagian dari penjabaran tugas pokok dan fungsi, khususnya bagi mereka yang memiliki akses terhadap aset informasi yang bersifat rahasia, berharga (mempunyai nilai nominal tertentu dan merupakan hasil dari pembelanjaan APBN), dan rawan (mempunyai aspek nilai intangible atau terkait risiko keamanan terhadap aset informasi lainnya).

e. Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menyertakan persyaratan untuk:
   1) Melaksanakan dan bertindak sesuai dengan organisasi keamanan informasi
   2) Melindungi aset dari akses yang tidak sah, penyingkapan, modifikasi, kerusakan atau gangguan
   3) Melaksanakan proses keamanan atau kegiatan keamanan informasi sesuai dengan peran dan tanggung jawabnya; dan
   4) Melaporkan kejadian, potensi kejadian, atau risiko keamanan informasi sesuai dengan Kebijakan dan Standar Pengelolaan Keamanan Informasi di lingkungan Badan POM.

4.2 Saat Menjadi Karyawan Badan POM

4.2.1 Tanggung Jawab Manajemen

a. Pejabat Keamanan Informasi menyusun daftar tenaga ahli kunci di lingkungannya, yang perlu mendapat perhatian khusus pada saat yang bersangkutan akan mengalami penghentian, pemutusan hubungan kerja atau mutasi.

b. Pejabat Keamanan Informasi bertanggung jawab untuk memastikan bahwa pegawai berkeahlian khusus atau yang berada di posisi kunci telah memiliki pengganti atau yang bisa menggantikan saat yang bersangkutan akan berhenti, putus hubungan kerja atau dimutasikan. Pimpinan dari pegawai berkeahlian khusus atau yang berada di posisi kunci (key person) harus memastikan ketersediaan pengganti pegawai

tersebut dengan kompetensi yang setara apabila pegawai yang bersangkutan mutasi/ berhenti.

c. Pegawai berkeahlian khusus atau yang berada di posisi kunci harus didorong agar melakukan alih keahlian dan pengetahuannya kepada rekan kerja sebelum mereka meninggalkan Badan POM.

4.2.2 Pendidikan, Pelatihan untuk Meningkatkan Kesadaran Terkait Keamanan Informasi

a. Seluruh pegawai yang bekerja di unit kerja harus mendapatkan pendidikan, pelatihan, dan sosialisasi sistem keamanan informasi secara berkala sesuai tingkat tanggung jawabnya.

b. Mitra dan pihak ketiga lainnya, jika diperlukan, mendapatkan sosialisasi untuk meningkatkan kepedulian terhadap keamanan informasi melalui proses induksi atau metode lain yang tepat.

4.2.3 Proses pendisiplinan

a. Seluruh pegawai, mitra dan pihak ketiga lainnya yang melanggar kebijakan dan standar pengelolaan keamanan informasi yang berlaku di lingkungan Badan POM akan dikenai sanksi atau tindakan disiplin sesuai ketentuan yang berlaku.

b. Kepatuhan pegawai terhadap Kebijakan Pengelolaan Keamanan Informasi Badan POM harus dievaluasi secara berkala oleh atasan masing-masing dan menjadi bagian dari penilaian kinerja pegawai.

4.3 Pemutusan dan Perubahan Hubungan Kerja

4.3.1 Pemutusan atau perubahan tanggung jawab pekerjaan

a. Seluruh pegawai yang berhenti bekerja atau mutasi harus mengembalikan seluruh aset informasi yang dipergunakan selama bekerja sesuai dengan ketentuan yang berlaku.

b. Pegawai, mitra kerja, dan pihak ketiga yang telah berhenti bekerja atau habis masa kontrak kerjanya harus mengembalikan seluruh aset yang dipergunakan selama bekerja di unit kerja.

c. Unit kerja menghentikan hak penggunaan aset informasi bagi pegawai yang sedang menjalani pemeriksaan yang terkait dengan dugaan adanya pelanggaran kebijakan dan standar pengelolaan keamanan informasi di lingkungan unit kerja dan/ atau yang sedang menjalani proses hukum

d. Unit kerja mencabut Hak akses terhadap sistem informasi yang dimiliki pegawai, mitra kerja dan pihak ketiga lainnya apabila yang bersangkutan tidak lagi bekerja di unit kerja.
e. Sebelum penghentian, pemutusan hubungan kerja atau mutasi efektif berlaku, unit kerja wajib mengingatkan hak dan kewajiban pegawai, mitra kerja dan pihak ketiga untuk tetap mematuhi kebijakan dan aturan keamanan informasi yang berlaku di Badan POM terutama yang terkait dengan kewajiban menjaga kerahasiaan

BAB V

PENGENDALIAN PENGELOLAAN ASET

Pengelolaan aset informasi bertujuan memberikan pedoman dalam mengelola aset informasi di lingkungan Badan POM untuk melindungi dan menjamin keamanan informasi.

5.1 Tanggung Jawab terhadap Aset Informasi

5.1.1 Inventarisasi Aset

a. Unit kerja harus mengidentifikasi aset informasi dan mendokumentasikannya dalam Daftar Inventaris Aset Informasi yang berisikan seluruh aset informasi utama.

b. Aset informasi yang diinventaris adalah aset dalam bentuk:

1) Perangkat keras, meliputi perangkat keras yang digunakan untuk mengolah dan menyimpan informasi dalam bentuk fisik maupun elektronik, yang mencakup namun tidak terbatas pada komputer, notebook, server, harddisk drive, USB disk.

2) Perangkat lunak, meliputi perangkat lunak yang digunakan untuk mengolah informasi dalam bentuk elektronik, yang mencakup namun tidak terbatas pada sistem operasi, aplikasi, dan database.

3) Perangkat jaringan, meliputi perangkat keras dan lunak yang digunakan untuk membentuk dan infrastruktur jaringan telekomunikasi, yang mencakup namun tidak terbatas pada hub, switch, router, firewall, IDS, IPS, dan network monitoring tools.

4) Informasi, meliputi data-data yang telah diolah dan dilakukan pemrosesan informasi yang mencakup namun tidak terbatas pada database, laporan, catatan atau informasi yang bersifat hardcopy maupun softcopy.

5) Perangkat pendukung meliputi perangkat digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan informasi yang mencakup namun tidak terbatas pada genset, UPS, AC, rak server, lemari penyimpanan informasi dan CCTV.

6) Sumber daya manusia meliputi personil baik internal maupun eksternal yang terlibat dalam pengolahan dan penyimpanan informasi.

c. Daftar Inventaris harus secara jelas mengidentifikasi setiap aset, pemilik aset, dan lokasinya.

d. Daftar Inventaris Aset Informasi ini dipelihara dan dikelola perubahannya oleh Penanggung Jawab Pengendalian Dokumen.

5.1.2 Kepemilikan Aset

a. Pejabat pelaksana keamanan informasi Informasi menetapkan Pemilik Aset di unit kerja yang bertanggung jawab dalam memantau perlindungan terhadap aset.
b. Pemilik aset informasi bertanggung jawab terhadap perlindungan keamanan seluruh aset informasi yang berada dibawah pengawasannya.
c. Pemilik aset informasi menetapkan aturan penggunaan aset informasi yang berada di bawah pengawasannya.
d. Pemilik aset informasi menetapkan dan mengkaji secara berkala klasifikasi aset informasi dan jenis perlindungan keamanannya.
e. Pemilik aset informasi menetapkan pihak yang berwenang untuk mengakses aset informasi

5.1.3 Penggunaan Aset yang Diperbolehkan

a. Kepala BPOM sebagai induk organisasi Badan POM menetapkan kebijakan dan aturan penggunaan aset-aset informasi bagi pegawai, mitra, dan pihak ketiga lainnya.
b. Seluruh pengguna aset informasi, tanpa kecuali, wajib mematuhi kebijakan dan aturan yang telah ditetapkan dan harus melaporkan kepada penanggung jawab keamanan informasi setempat bila melihat terjadinya pelanggaran terhadap kebijakan ini.

5.2 Pengklasifikasian aset informasi

5.2.1 Klasifikasi Informasi

a. Klasifikasi aset informasi dilakukan oleh pemilik aset informasi dan disetujui oleh pimpinan unit kerja. Aset informasi diklasifikasikan sesuai tingkat kerahasiaan, nilai, ketentuan/kebutuhan kegiatan yang menggunakannya, tingkat kerahasiaan, tingkat kritikalitas serta aspek hukumnya.
b. Aset informasi yang diterima dari pihak ketiga, harus memuat dan mencantumkan klasifikasinya atau dilakukan penggolongan ulang sesuai skema yang ditetapkan Badan POM.
c. Badan POM menetapkan 3 (tiga) golongan aset informasi sebagai berikut:

1) RAHASIA yaitu aset informasi yang sangat peka dan berisiko tinggi yang pembocoran atau penyalahgunaan akses terhadapnya bisa mengganggu kelancaran kegiatan Badan POM atau mengganggu citra dan reputasi Badan POM. Informasi ini hanya bisa diakses secara terbatas oleh pihak ketiga, untuk kepentingan, atau karena kewajiban dan kebutuhan Badan POM, melalui serah terima resmi dengan syarat Pihak ketiga dan pegawai pihak ketiga menandatangani Kesepakatan Kewajiban Menjaga Rahasia/*Non-Disclosure Agreement.*

   Contoh: IP address, password komputer, bahan/materi pelatihan, rencanaanggaran atau pengadaan, data gaji dan penilaian kinerja pegawai, dan data kesehatan pribadi yang secara legal harus dilindungi.

2) TERBATAS (hanya untuk penggunaan internal) yaitu aset informasi yang telah terdistribusi secara luas di lingkungan internal Badan POM yang penyebarannya secara internal tidak lagi memerlukan ijin dari pemilik informasi dan risiko penyebarannya secara tak berwenang tidak menimbulkan kerugian berarti. Informasi ini dapat diberikan ke pihak ketiga oleh pemiliknya untuk kepentingan dinas melalui prosedur serah terima resmi.

   Contoh: kebijakan Badan POM, panduan kerja, prosedur kerja, instruksi kerja,memo/publikasi internal, informasi yang disediakan dalam intranet, dan data operasional TI lainnya.

3) PUBLIK yaitu aset informasi yang secara sengaja disediakan Badan POM untuk dapat diketahui publik/ masyarakat umum.

   Contoh: brosur, situs publik Badan POM, dan siaran pers (*press release*).

5.2.2 Pelabelan Informasi

a. Pemberian label pada aset informasi harus dilakukan secara konsisten pada segala bentuk aset informasi yang tersimpan di Badan POM, seperti pada hasil cetakan perangkat lunak, laporan, dokumen pedaoman penggunaan sistem, tape, dsb. Untuk itu Badan POM menetapkan prosedur pemberian label dan penanganan aset informasi yang dibuat dan diterapkan sesuai klasifikasi yang ditetapkan.

b. Pemberian label klasifikasi aset informasi hanya khusus untuk informasi yang bersifat rahasia dan diberikan keterangan "RAHASIA" pada dokumen tersebut.

c. Dalam hal data yang tersimpan di dalam media bersifat rahasia, perlu diberikan proteksi kata sandi untuk melindungi data.

5.2.3 Penanganan Aset

a. Penanganan terhadap aset informasi harus mempertimbangkan tingkat klasifikasi yang telah ditetapkan oleh unit kerja.

b. Proses penanganan informasi yang diklasifikasikan memperhatikan dari siklus transaksi informasi sebagai berikut :

Klasifikasi / Tipe	Klasifikasi Rahasia
Dokumen dan catatan (*record*) dalam bentuk non elektronik (*hardcopy*).	Diberi label "*Rahasia*" Apabila terdapat map atau amplop yang didalamnya terdapat informasi Rahasia maka media tersebut harus diberi tanda.
Amplop untuk surat eksternal (ke luar kantor).	• Menggunakan 2 amplop, dimana amplop pertama dimasukkan kedalam amplop kedua; • Pada amplop pertama ditandai "Rahasia", dan pada amplop kedua tidak diberikan tanda apapun.
Dokumen dan catatan (*record*) dalam bentuk elektronik (*softcopy*).	Memberikan label "Rahasia" pada bagian awal dari nama *file* atau pada bagian tertentu dari *file properties*.
Publikasi / Distribusi	• Distribusi kepada pihak eksternal sangat dibatasi untuk kebutuhan kedinasan. • Apabila memungkinkan, infor masi rahasia tidak disalin oleh pihak eksternal (*eyes only*). • Distribusi kepada pihak eksternal perlu seijin pemilik Informasi. • Kerahasiaan terhadap informasi perlu diberitahukan kepada pihak eksternal. • Pihak ketiga harus disertai perjanjian kerahasiaan (NDA - *non disclosure agreement*).
Pencetakan informasi	• Pencetakan hanya pada *printer* organisasi dan diusahakan tidak mencetak menggunakan jasa pencetakan eksternal.

Klasifikasi / Tipe	Klasifikasi Rahasia
Surat menyurat internal (di dalam kantor)	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat internal. • Menginformasikan kepada penerima akan pengiriman informasi tersebut. • Mengkonfirmasi kepada penerima bahwa informasi yang dikirim sudah diterima.
Surat menyurat eksternal (ke luar kantor)	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat eksternal. • • Apabila menggunakan jasa ekspedisi, pengiriman harus tercatat dengan tanda pengiriman. • Menginformasikan kepada penerima akan pengiriman informasi tersebut. • Mengkonfirmasi kepada penerima bahwa informasi yang dikirim sudah diterima.
Pengiriman ke pihak internal melalui *email*	• Pengiriman e-mail harus menggunakan account e-mail institusi • Memberi *password* pada informasi yang dikirim melalui email dan password diinformasikan kepada penerima secara terpisah • Tidak mencantumkan informasi rahasia di *body text* e-mail • Pengiriman informasi, termasuk *forwarding* / meneruskan *email* hanya boleh dilakukan oleh pemilik informasi.
Pengiriman ke pihak eksternal melalui *email*	• Tidak disarankan menggunakan e-mail untuk mengirim informasi dengan klasifikasi ini. • Pengiriman e-mail harus menggunakan *account* e-mail institusi • Pastikan alamat email tujuan sudah benar. • Memberi *password* pada informasi yang dikirim melalui email dan password diinformasikan kepada penerima secara terpisah
Penyimpanan informasi *hardcopy*	Disimpan secara aman dalam tempat penyimpanan yang terkunci.

Klasifikasi / Tipe	Klasifikasi Rahasia
Penyimpanan informasi *softcopy*	• Penyimpanan pada komputer atau media penyimpanan harus yang menggunakan *password.* • *File* yang disimpan harus diberi *password.* • Media penyimpanan eksternal (*externalharddisk,* atau *flashdisk*) harus disimpan pada tempat penyimpanan yang terkunci.
Penyimpanan pada pihak ketiga	Harus disertai dengan perjanjian kerahasiaan (*non disclosure agreement* - NDA).
Penghancuran (*disposal*)	• Memperhatikan masa retensi informasi yang disetujui oleh pemilik informasi • Dihancurkan dengan metode pemusnahan dan informasi tidak dapat diakses kembali (dihancurkan secara fisik atau *secure format*).

c. Untuk informasi yang bersifat terbatas dan publik tidak terdapat perlakuan khusus dan penanganan terhadap informasi tersebut ditentukan oleh unit kerja pemilik informasi.

d. Perangkat pendukung yang didalamnya terdapat informasi yang terklasifikasi maka unit kerja harus memperhatikan perlindungan terhadap aset tersebut.

5.2.4 Pengembalian Aset

Setiap pengguna harus mengembalikan sumber daya informasi milik Badan POM yang digunakannya segera setelah penugasannya berakhir, atau sumber daya informasi tersebut tidak lagi digunakan untuk bekerja di Unit Kerja.

5.3 Penanganan Media

5.3.1 Pengelolaan *Removable Media*

Dokumentasi dari sistem, baik yang tercetak ataupun yang berupa dokumen elektronik, digolongkan sebagai dokumen RAHASIA dan harus disimpan secara aman dan hanya disediakan bagi mereka yang memerlukannya. Yang termasuk dokumentasi dari sistem antara lain struktur data, struktur jaringan, proses-proses otorisasi, dsb.

5.3.2 Pengelolaan Internet

a. Unit kerja yang membidangi infrastruktur dan TIK berkewajiban memastikan akses internet kepada Unit kerja di lingkungan Badan POM berjalan secara aman khususnya apabila terkoneksi dengan sistem di Data Center

b. Ketentuan dalam pengguaan internet adalah sebagai berikut:

1) Pengguna dilarang menggunakan akses internet Badan POM untuk kegiatan melanggar hukum dan aktifitas yang dapat membahayakan keamanan jaringan Badan POM;

2) Pengguna dilarang untuk menggunakan akses internet Badan POM untuk mengakses, mendistribusikan, mengunggah dan/atau mengunduh:

Materi pornografi :

i. Perangkat lunak tidak berlisensi atau yang berbahaya.

ii. Materi yang bersifat SARA.

iii. Situs yang dapat menimbulkan risiko serangan malware, penyusupan atau hacking ke jaringan Badan POM.

3) Pengguna disarankan untuk tidak membagi informasi Badan POM melalui situs internet atau media sosial.

5.3.3 Pembuangan Media

a. Informasi yang terkandung dalam media penyimpan informasi yang bisa dipakai ulang dan digunakan sebagai media transit (seperti disket dan USB flash disk) harus dihapus jika tidak lagi diperlukan dan harus dipastikan bahwa salinan asli informasi tersebut masih tersedia.

b. Seluruh media penyimpan informasi mudah jinjing (removable) harus diformat ulang dengan teknik tertentu sehingga data tidak bisa dikembalikan. Tetapi jika hal itu tidak bisa dilakukan, media tersebut harus dihancurkan.

c. Media kertas (termasuk carbon copies, cetakan printer) yang mengandung informasi RAHASIA dihancurkan dengan menggunakan alat penghancur kertas atau dibakar.

d. Media lain, seperti disket, tape, CD, DVD, USB flash disk, dan lain-lain harus dirusak secara fisik sehingga isinya tidak bisa diakses oleh pihak yang tidak berwenang.

5.3.4 Transfer Media secara Fisik

a. Pertukaran informasi antara Badan POM dengan pihak ketiga hanya akan dilakukan atas persetujuan tertulis kedua belah pihak. Pertukaran informasi digital harus disetujui oleh Pimpinan Unit Kerja.

b. Unit Kerja harus menjamin bahwa pertukaran informasi penting dan rawan hanya dilakukan setelah melalui suatu pengkajian risiko yang memadai dan penetapan ketentuan-ketentuan keamanan informasi dalam perjanjian pertukaran informasi antara pihak yang terkait.

c. Aset informasi yang dikirim dengan menggunakan jasa layanan kurir atau pos rawan diakses oleh pihak yang tidak berwenang selama pengiriman. Unit Kerja menerapkan alat kendali berikut :

   1) Mencatat secara lengkap dan jelas identitas kurir yang digunakan.
   2) Mengemas aset informasi dalam kemasan yang baik dan kuat yang mampu melindungi kandungannya dari kerusakan fisik selama pengiriman.
   3) Informasi internal Badan POM yang disediakan bagi masyarakat umum harus disetujui oleh pemilik aset informasi dan dilindungi keutuhannya dari modifikasi oleh pihak yang tidak berwenang.

BAB VI

PENGENDALIAN HAK AKSES

Pengendalian akses bertujuan untuk memastikan otorisasi akses pengguna dan mencegah akses pihak yang tidak berwenang terhadap aset informasi khususnya perangkat pengolah informasi.

6.1 Persyaratan Bisnis untuk Pengendalian Akses

6.1.1 Kebijakan Pengendalian Hak Akses

a. Pemilik sistem informasi harus menyusun, mendokumentasikan, dan mengkaji ketentuan hak akses ke aset informasi berdasarkan kebutuhan organisasi dan persyaratan keamanan.
b. Ketentuan hak akses harus didokumentasikan dalam bentuk matriks hak akses.
c. Hak penggunaan/akses terhadap aset-aset informasi diberikan sesuai dengan kebutuhan fungsi dan tugas pengguna dan diberikan berdasarkan prinsip minimum/seperlunya, yaitu cukup untuk memenuhi kebutuhan user dalam menjalankan tugasnya.
d. Persyaratan untuk pengendalian hak akses mencakup:
    1) Pengembangan aturan pemberian akses perlu mempertimbangkan:
        a. Klasifikasi dari informasi
        b. Kritikalitas dari aset yang digunakan untuk mendukung operasional bisnis
        c. Prasyarat hukum perundang-undangan, kontraktual serta keamanan yang relevan
        d. Didasarkan atas prinsip *need to know* dan *need to use*, yaitu disesuaikan dengan kebutuhan pekerjaan dan operasional dalam lingkungan Badan POM
    2) Pemisahan peran pengendalian akses, seperti administrasi akses dan otorisasi akses

6.1.2 Kebijakan Penggunaan Layanan Jaringan

a. Unit kerja yang mengelola Infrastruktur dan TIK mengatur akses pengguna dalam mengakses jaringan internal Badan POM sesuai peruntukannya.
b. Unit kerja yang mengelola Infrastruktur dan TIK menerapkan proses otorisasi pengguna untuk setiap akses ke dalam jaringan internal melalui koneksi eksternal (*remote access*).

c. Unit kerja yang mengelola Infrastruktur dan TIK melakukan isolasi layanan jaringan pada area jaringan yang mengalami gangguan keamanan informasi
d. Akses ke jaringan milik Badan POM hanya diberikan kepada user yang berwenang saja.
e. Untuk menghindarkan akses oleh pihak yang tidak berwenang, pemberian akses dilakukan melalui proses logon yang aman.
f. Proses logon tidak boleh mengungkapkan informasi apapun tentang sistem, yang dapat dimanfaatkan oleh pihak yang tidak berwenang untuk mendapatkan akses ke jaringan.
g. Akses secara remote ke jaringan internal Badan POM dari jaringan publik harus sangat dibatasi baik dari perangkat yang digunakan maupun waktu untuk kebutuhan troubleshooting dan harus dilakukan melalui secure channel, antara lain dengan menggunakan teknologi VPN
h. Unit kerja yang mengelola Infrastruktur dan TIK harus mempertimbangkan pemisahan jaringan antara lain:
    1) Jaringan komunikasi dalam lingkungan Badan POM harus dipisahkan kedalam domain jaringan yang terpisah sesuai dengan kebutuhan bisnis dan operasional, dalam rangka untuk mengamankan jaringan internal dan aset di jaringan tersebut;
    2) Pemberian akses jaringan kepada tamu, hanya dapat diberikan akses terbatas misalnya internet dan/ atau surat elektronik tanpa bisa terhubung ke jaringan internal Badan POM

6.2 Pengelolaan Hak Akses Pengguna Aset Informasi

6.2.1 Registrasi dan de-Registrasi Pengguna

a. Unit kerja pemilik sistem informasi harus mengembangkan mekanisme pemberian hak akses yang dikelola secara formal pada seluruh siklusnya, mulai dari proses pengajuan, persetujuan serta pencabutan, serta dilaksanakan oleh para pihak terkait sesuai jenjang kewenangannya;
b. Setiap permintaan registrasi dari pengguna harus disertai surat permohonan dan harus disetujui oleh pimpinan setingkat Eselon III dari unit kerja pengelola sistem informasi.
c. Identitas pengguna harus diotorisasi secara formal berdasarkan matriks hak akses yang telah ditetapkan. Akses atas sistem dan aplikasi hanya dapat diaktifkan jika proses otorisasi telah selesai.

d. Identitas pengguna pada sistem, seperti user ID, harus bersifat unik untuk memungkinkan mengidentifikasi dan meminta pertanggungjawaban pengguna.

6.2.2 Pengelolaan Hak Akses Khusus (*Privilege Management*)

a. Hak akses khusus (*privileged access rights*) ke sistem informasi termasuk sistem operasi, *storage device, file server*, dan aplikasi – aplikasi dalam lingkungan Badan POM, seperti administrator, *root*, hak akses untuk memodifikasi database atau hak akses untuk membuat, memodifikasi atau mencabut pengguna dalam sistem aplikasi, harus sangat dibatasi kepada personil yang terotorisasi dan terlatih; Hak akses khusus harus disetujui dan didokumentasikan secara formal.
b. Hak akses khusus hanya diberikan kepada pengguna sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu.
c. Pengelolaan proses otorisasi dan catatan seluruh hak akses khusus yang dialokasikan/ diberikan kepada pengguna. Hak akses khusus tidak boleh diberikan sebelum proses otorisasi selesai.
d. Hak akses khusus harus diberikan secara terpisah dari akun yang digunakan untuk kegiatan umum, seperti akun sistem administrator, database administrator, dan *network administrator.*
e. Apabila memungkinkan, hak akses khusus harus dialokasikan secara individual dan tidak di-share. Hal ini dilakukan untuk menjamin akuntabilitas dari pengguna khusus.
f. Jejak audit (log) untuk hak akses khusus pada sistem informasi dalam lingkungan unit kerja pengelola sistem informasi harus diaktifkan.
g. Pencabutan hak akses khusus harus dilakukan setelah penggunaan hak akses tersebut telah selesai dan alokasi dari hak akses khusus harus ditinjau secara berkala dan setiap terdapat perubahan dalam status penggunaan akses tersebut.

6.2.3 Pengelolaan Password (*secret authentication information of users*)

a. Password diberikan secara otomatis oleh Administrator Sistem / Aplikasi dan selanjutnya harus diganti sebelum pengguna dapat memakai lebih lanjut hak aksesnya pada sistem / aset informasi terkait.

b. Password harus dijaga kerahasiaannya :
   1) Tidak boleh dipakai bersama (shared).
   2) Tidak boleh diberitahukan kepada orang lain.
   3) Tidak boleh dituliskan (*hard coded*) dalam perangkat lunak apapun.
   4) Tidak boleh ditulis di media yang diletakkan di tempat yang mudah terlihat orang lain.
c. Pemakaian user ID dan kegiatan yang dilakukan dengan mengatasnamakannya akan dicatat dan direkam untuk tujuan pemantauan dan tindakan terkait.

6.2.4 Kajian Hak Akses Pengguna

a. Unit Kerja memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya.
b. Hasil evaluasi akan dianalisa dan ditindaklanjuti oleh administrator apabila terjadi penyimpangan pada penggunaan maupun aktiviasi user.
c. Setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan menyesuaikan atau menghapus hak akses khusus yang menyimpang.
d. Pemeriksaan hak akses khusus harus dilakukan secara berkala untuk memastikan pemberian hak akses khusus telah diotorisasi.

6.2.5 Penghapusan atau Penyesuaian Hak Akses Pengguna

a. User account akan dihapus setelah pengguna tidak memiliki kewenangan atau otorisasi ke sistem informasi.
b. Hak akses pengguna dihapus atau dinonaktifkan segera setelah user berubah tugas dan/ atau fungsinya, setelah penugasan berakhir atau mutasi.
c. Hak akses pengguna disesuaikan secara berkala tergantung pada kebutuhan.
d. Pemeriksaan, penghapusan serta penonaktifan akun secara berkala dan untuk pengguna yang memiliki lebih dari 1 (satu) akun

6.3 Tanggung Jawab Pengguna

6.3.1 Penggunaan Password (*secret authentication information*)

a. Pengguna harus memastikan perangkat pengolah informasi yang digunakan mendapatkan perlindungan terutama pada saat ditinggalkan melalui penggunaan password pada layar perangkat.

b. Untuk menghindari serangan password maka berikut ini adalah kebijakan yang mengatur mengenai pengelolaan password:

1) Pengguna harus menjaga kerahasiaan dan keamanan password pribadi atau kelompok serta informasi otentikasi rahasia lainnya;

2) *Password* minimum terdiri dari 8 karakter kombinasi angka dan huruf serta tidak boleh menggunakan karakter yang mudah ditebak, serta tidak terdiri dari informasi pribadi seperti ulang tahun pengguna, nama perusahaan atau nama pengguna

3) Pengguna harus mengganti *default password* yang diberikan saat pertama kali mendapatkan hak akses.

4) *Password* tidak boleh:

i. diberitahukan kepada orang lain

ii. ditulis di media yang mudah terlihat orang lain

5) *Password* diganti secara berkala atau segera diganti bila diduga telah diketahui orang lain. Periode penggantian *password* untuk administrator dan pengguna setiap 90 hari

6) Hak akses akan direset atau dinonaktifkan jika tak pernah digunakan selama 90 hari secara berturut-turut.

c. Komputer yang berisikan informasi penting harus dipasangi screen saver yang dilindungi password dan aktif dengan sendirinya setelah komputer tidak digunakan selama 10 (sepuluh) menit.

6.4 Pengendalian Hak Akses ke Sistem dan Aplikasi

6.4.1 Pembatasan Akses Informasi

a. Pengelola sistem informasi mengatur akses pengguna dalam mengakses informasi pada sistem informasi sesuai peruntukannya. Pengelola sistem informasi menjamin bahwa akses terhadap informasi hanya diberikan bagi mereka yang memerlukan akses dalam menjalankan pekerjaannya.

b. Pengelola sistem informasi membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki informasi dengan klasifikasi RAHASIA.

6.4.2 Sistem Pengelolaan Password

a. Pemilik Aset Informasi harus memastikan bahwa sistem dan aplikasi dibawah pengelolaannya memiliki fasilitas manajemen hak akses pengguna, manajemen kata sandi yang baik, serta mekanisme otentikasi pengguna yang aman.
b. Fasilitas manajemen kata sandi harus memastikan dihasilkannya kata sandi yang berkualitas, yaitu:
    1) menegakkan akuntabilitas pengguna melalui penggunaan identitas pengguna tunggal untuk setiap individu.
    2) memberikan fasilitas penggantian kata sandi mandiri.
    3) mewajibkan pengguna untuk mengganti kata sandi pada saat pertama kali login.
    4) mewajibkan pengguna untuk mengganti kata sandi secara berkala.
    5) tidak menampilkan kata sandi saat sedang dimasukkan.
c. Fasilitas *session time out* harus diaktifkan utuk menutup dan mengunci layar komputer aplikasi apabila tidak ada aktifitas pengguna setelah periode tertentu.

6.4.3 Penggunaan *privileged utility programs*

a. Unit kerja pengelola infrastruktur dan TIK membatasi dan mengendalikan penggunaan system utilities pada perangkat server yang tersimpan sistem aplikasi.
b. Penggunaan program utility khusus seperti registry cleaner atau system monitoring yang dapat mengambil alih kendali sistem/aplikasi atau mendapatkan hak akses khusus pada sistem/aplikasi harus sangat dibatasi berdasarkan kebutuhan operasional pengguna;

6.4.4 Kendali akses ke kode sumber program

a. Unit kerja pengelola sistem informasi harus memastikan bahwa source code dikelola dan disimpan secara memadai baik yang dikembangkan oleh internal Unit kerja maupun yang dikembangkan oleh penyedia jasa aplikasi.
b. Apabila source code dari penyedia jasa aplikasi tidak dapat diserahkan kepada pengelola aplikasi, unit kerja bersama penyedia jasa aplikasi tersebut harus mempertimbangkan *escrow aggreeement* untuk memastikan kelangsungan operasional sistem aplikasi jika ada pengembangan selanjutnya.

c. Pengendalian terhadap akses ke source code aplikasi sebagai berikut:

1) Untuk sistem aplikasi yang dikembangkan secara internal dan/atau dibeli dengan source code, pengendalian akses harus diimplementasikan untuk mencegah akses tanpa izin ke source code tersebut

2) Pengendalian tersebut mencakup :

i. Tidak menyimpan source code pada sistem operasional

ii. Menyimpan source code pada lokasi fisik yang aman dari ancaman akses tanpa izin maupun ancaman kerusakan karena kondisi lingkungan

iii. Membatasi akses secara fisik maupun logical ke *source code* program hanya kepada pengembang dan personil yang berwenang

iv. Mengimplementasikan metode versioning dan proses manajemen perubahan untuk menjamin integritas dari *source code* aplikasi.

BAB VII

PENGENDALIAN KRIPTOGRAFI

Pengendalian kriptografi bertujuan untuk menjaga supaya aset dan informasi tidak bisa dibaca oleh pihak yang tidak berwenang.

7.1 Pengendalian Kriptografi

a. Unit kerja pengelola sistem informasi harus mengembangkan dan menerapkan sistem kriptografi untuk perlindungan informasi dan membuat rekomendasi yang tepat bagi penerapannya.
b. Unit kerja pengelola sistem informasi harus mengkaji sistem untuk proses enkripsi data dan menyusun standar yang tepat bagi penerapannya.
c. Sistem kriptografi harus digunakan untuk melindungi aset informasi yang memiliki klasifikasi RAHASIA.
d. Kontrol kriptografi dapat mencakup namun tidak terbatas pada:
    1) Enkripsi informasi dan jaringan komunikasi
    2) Pemeriksaan integritas informasi, seperti hashing
    3) Otentikasi identitas
    4) Digital signatures
e. Pemilihan kontrol kriptografi harus mempertimbangkan:
    1) Jenis dari kontrol kriptografi
    2) Kekuatan dari algoritma kriptografi
    3) Panjang dari kunci kriptografi.

BAB VIII

PENGENDALIAN KEAMANAN FISIK DAN LINGKUNGAN

Keamanan fisik dan lingkungan bertujuan untuk mencegah akses fisik oleh pihak yang tidak berwenang, menghindari terjadinya kerusakan pada perangkat pengolah informasi serta gangguan pada aktifitas organisasi

8.1 Pengamanan area

8.1.1 Perimeter Keamanan Fisik

a. Unit Kerja harus menggunakan Perimeter keamanan fisik untuk melindungi daerah-daerah yang berisi informasi dan fasilitas pengolahan informasi.
b. Keseluruhan area di Badan POM dikelompokkan ke dalam 3 (tiga) zona ruang sesuai aktivitas yang dapat dilakukan dalam zona tersebut. Setiap zona ruang memiliki identifikasi dan tingkat kewenangan/otorisasi yang diperlukan bagi pengguna yang akan mengakses suatu area:
    1) Area Publik : area yang dapat dimasuki oleh semua orang yang meliputi area lobby, area resepsionis.
    2) Area Terbatas : area yang hanya diotorisasi bagi pegawai Badan POM dan pihak diluar tersebut harus mendapatkan otorisasi dari pegawai di area tersebut. Contoh area ini adalah area kerja.
    3) Area Tertutup : area yang hanya petugas tertentu yang dapat mengakses area tersebut yang telah diotorisasi oleh pimpinan unit kerja, seperti : ruang Data Center dan DRC, ruang jaringan, Ruang Arsip.
c. Untuk area Data center, disaster recovery center, ruang jaringan dan ruang arsip harus dilindungi dengan menerapkan pengamanan fisik pada perimeter area tersebut dengan kriteria:
    1) Konstruksi dinding, atap dan lantai yang kuat
    2) Pintu akses menuju area harus dilengkapi dengan mekanisme kontrol akses, seperti: access door lock
    3) Pintu dan jendela harus senantiasa dalam kondisi terkunci, khususnya pada saat tanpa penjagaan
    4) Perangkat CCTV perlu terpasang pada sisi eksterior dan interior area
    5) Tidak diperbolehkan menyimpan bahan-bahan berbahaya yang mudah terbakar.

8.1.2 Pengendalian Akses Masuk Fisik

a. Seluruh pegawai, mitra kerja, tamu dan pihak ketiga lainnya yang memasuki lingkungan Badan POM harus mengenakan kartu identitas (ID Card) resmi yang dikeluarkan BADAN POM.
b. Setiap area harus merupakan akses terbatas, dimana akses masuk hanya diberikan bagi personil yang telah mendapatkan otorisasi. Mekanisme pembatasan ini dapat dilakukan aturan penerimaan tamu yang diterapkan berdasarkan kritikalitas area tersebut.
c. Kunjungan ke dalam area tersebut harus disetujui secara formal oleh pengelolaan area tersebut.
d. Selama kunjungan di dalam area tersebut, pengunjung harus senantiasa didampingi oleh personil unit kerja atau petugas keamanan.
e. Kartu identitas pengunjung perlu diverifikasi, disimpan oleh petugas selama kunjungan, dan dikembalikan sesudah selesai kunjungan;
f. Setiap pengunjung ke dalam area harus tercatat, mencakup jam masuk dan keluar.
g. Pengamanan kantor, ruangan dan fasilitas menjadi beberapa level.
    1) Level pertama
       Untuk masuk ke gedung dijaga oleh petugas keamanan.
    2) Level Kedua
       Untuk masuk kedalam area tertutup diperlukan penggunaan tools akses fisik dan kartu akses.

8.1.3 Pengamanan Kantor, Ruangan dan Fasilitas

a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya pencurian, akses oleh pihak yang tidak berwenang, kebakaran, air, debu, dan sebagainya.
b. Aktivitas pada area-area kritikal harus disertai dengan fasilitas CCTV dan dimonitor secara berkala.
c. Penggunaan petugas keamanan harus dipastikan tersedia dalam waktu-waktu yang dianggap rawan berdasarkan analisa risiko dari masing-masing area.

8.1.4 Pengamanan dari Ancaman Eksternal dan Lingkungan

a. Setiap area harus dipastikan terdapat alat pemadam kebakaran kebakaran kecil (APAR). Khusus untuk area tertutup perlu

diperhatikan penggunaan alat pemadam kebakaran yang khusus atau APAR dengan volume yang berisikan powder.

b. Setiap area harus dipasang smoke detector dan dipelihara secara berkala melalui pengujian rutin.
c. Pimpinan unit kerja menunjuk Pegawai di area tersebut untuk diberikan pelatihan mengenai penggunaan alat pemadam api yang tersedia.
d. Area yang digunakan dalam aktivitas pegawai harus diperhatikan suhu dan kelembaban untuk mencegah kerusakan aset.

8.1.5 Bekerja di Area Aman

a. Akses keluar masuk fasilitas Data Centre dan area kerja lainnya yang berisikan aset informasi yang bersifat RAHASIA harus dibatasi dan hanya diberikan kepada pegawai tertentu yang berwenang.
b. Seluruh pegawai, mitra kerja, pihak ketiga lainnya atau tamu yang memasuki fasilitas Data Centre atau area kerja yang berisikan aset informasi yang bersifat RAHASIA harus didampingi pegawai tertentu yang berwenang. Waktu masuk dan keluar serta maksud kedatangan harus dicatat dalam buku catatan keluar masuk ruangan (*log book*).
c. Kantor, ruangan dan fasilitas yang berisikan informasi RAHASIA harus memiliki pengamanan fisik yang memadai.
d. Fasilitas pada area tertutup harus dilengkapi dengan UPS, generator listrik cadangan, perangkat pemadam kebakaran, dan diusahakan terdapat perlindungan kejut listrik (petir, tegangan tidak stabil).
e. Fasilitas area tertutup dilengkapi dengan sistem sensor deteksi asap, air, suhu dan kelembaban, yang dapat terpantau.
f. Parameter temperatur dan kelembaban berikut perlu dijaga untuk fasilitas area tertutup meliputi:
    1) Temperatur antara 18° - 27° celcius
    2) Kelembaban (RH) antara 40% - 60%.
g. Pengambilan gambar di ruang server harus dengan seijin penanggung jawab ruang server.
h. Ruang Server, Data Centre, dan *Disaster Recovery Centre* (DRC) tidak boleh digunakan untuk ruang kerja.
i. Makanan dan minuman dilarang untuk dibawa masuk atau dikonsumsi di dalam ruang area tertutup. Semua area yang digunakan untuk menyimpan aset informasi penting adalah area bebas rokok.

8.1.6 Area Pengiriman dan Pemuatan

a. Area keluar masuk barang dan area lainnya (pengembangan) harus selalu dijaga, diawasi dan dikendalikan, dan jika mungkin diisolasi dari fasilitas pengolah informasi (komputer) untuk menghindari akses oleh pihak yang tidak berwenang.
b. Delivery dari barang harus dilaporkan dan diperiksa sebelum barang tersebut dapat dipindahkan dari area bongkar muat atau penerimaan barang ke data center, *disaster recovery center* dan ruang arsip.

8.2 Pengamanan perangkat

8.2.1 Penempatan dan Pengamanan Perangkat

a. Perangkat pengolah informasi dan perangkat pendukung harus ditempatkan di lokasi yang aman dan diposisikan sedemikian rupa sehingga mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang.
b. Perangkat pengolah informasi harus ditempatkan di lokasi yang tidak selalu dilewati/dilalui oleh tamu atau pihak ketiga.
c. Perangkat pengolah informasi (termasuk mesin faksimili, printer, komputer) yang digunakan untuk memproses informasi RAHASIA harus ditempatkan di lokasi yang aman untuk mencegah penyingkapan informasi tersebut ke pihak yang tidak berwenang.
d. Semua perangkat pengolah informasi harus mendapatkan pasokan daya yang sesuai dengan spesifikasi yang disyaratkan oleh pabrikan perangkat. Untuk setiap lokasi kerja (termasuk ruang Data Centre) tersedia pasokan listrik yang cukup untuk beban maksimal seluruh perangkat (termasuk perangkat pendukung) yang ada di lokasi tersebut.
e. Instalasi jaringan listrik harus sesuai dengan standar keselamatan yang ada.

8.2.2 Utilitas Pendukung

a. Perangkat pendukung harus dipasang untuk menjamin beroperasinya perangkat pengolah informasi dan secara berkala harus diperiksa dan diuji ulang kinerjanya.
b. Pasokan listrik yang digunakan untuk mengoperasikan perangkat pengolah informasi Badan POM harus mempunyai sumber alternatif dengan daya dan jangka waktu ketersediaan (jangka waktu pengoperasian) yang cukup. Pasokan ini minimal berupa perangkat

generator listrik dan perangkat UPS (*Uninterruptible Power Supply*) dengan daya yang cukup dan dengan konfigurasi yang dapat memindahkan pasokan listrik tanpa gangguan terhadap perangkat komputer/server.

8.2.3 Keamanan Pemasangan Kabel

a. Kabel sumber daya listrik harus dilindungi dari kerusakan;
b. Kabel telekomunikasi yang mengalirkan informasi harus dilindungi dari kerusakan dan penyadapan.
c. Konfigurasi jaringan kabel data dan daya harus terekam dalam dokumen resmi yang dimutakhirkan untuk setiap perubahan.
d. Jaringan kabel data harus dipisahkan dari kabel listrik dengan jarak yang cukup untuk menghindari dampak elektromagnet dan dengan pencantuman label yang sesuai.
e. Jaringan kabel data atau koneksi yang menghubungkan perangkat komputer/server penting harus diamankan melalui :
    1) Konstruksi jalur kabel data yang melindungi kabel dari dampak lingkungan atau pihak yang tidak berwenang.
    2) Spesifikasi kabel data yang sesuai dengan ancaman lingkungan (air,suhu/panas, kotoran, radiasi).
    3) Proses inspeksi dan perawatan rutin.
    4) Penempatan yang terlindung dari ancaman sekitar (jalur lintas kendaraan,peralatan berat, pekerjaan konstruksi).

8.2.4 Pemeliharaan Perangkat

a. Perangkat harus dipelihara secara berkala untuk menjamin ketersediaannya, keutuhannya, dan fungsinya.
b. Seluruh perangkat pengolah informasi penting dan peralatan pendukung harus diperiksa dan di-uji-coba efektifitasnya secara teratur/berkala, dirawat dan dibersihkan sesuai dengan spesifikasi pabrikannya.
c. Perawatan dan perbaikan perangkat pengolah informasi hanya dilakukan oleh personil yang berwenang dan mempunyai kompetensi teknis yang sesuai.
d. Pemeliharaan yang dilakukan oleh pihak ketiga, harus dilaksanakan sesuai dengan kesepakatan tingkat layanan (service level agreement/SLA) yang menjabarkan tingkat pemeliharaan dan kinerja yang harus dipenuhi pihak ketiga.

e. Bagi pemeliharaan yang tidak dapat dilakukan di lokasi kantor Badan POM, maka informasi rahasia dan kritikal yang tersimpan dalam peralatan tersebut harus dipindahkan terlebih dahulu.
f. Pemeliharaan perangkat yang mengharuskan dibawa dari luar area harus atas persetujuan pejabat berwenang.

8.2.5 Pemusnahan Aset

a. Perangkat pengolah informasi penyimpan data yang sudah tidak digunakan lagi harus disanitasi sebelum dimusnahkan
b. Perangkat pengolah informasi dimusnahkan menggunakan metode dan prosedur pemusnahan yang mempertimbangkan aspek keamanan informasi agar tidak bisa dibaca dan digunakan lagi oleh pihak yang tidak berwenang

8.2.6 Keamanan Perangkat di luar Area Badan POM

a. Penggunaan perangkat yang dibawa ke luar dari lingkungan Badan POM harus disetujui oleh pejabat yang berwenang.
b. Perlindungan perlu mempertimbangkan risiko dari lokasi *off premises* dan petunjuk dari pembuat
c. Perangkat yang diguanakan pada area diluar Badan POM khususnya di area publik tidak ditinggal tanpa pengawasan

8.2.7 Keamanan Pembuangan dan Penggunaan Kembali Perangkat

a. Perangkat pengolah informasi penyimpan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dihapuskan/ dimusnahkan;
b. Penggunaan kembali perangkat harus memperhatikan tidak adanya informasi yang tersimpan dan telah mendapatkan otorisasi dari pimpinan terkait sebelum digunakan

8.2.8 Perangkat Pengguna yang Tidak Dijaga

Komputer yang tidak terawasi dan ditinggalkan selama lebih dari 30 (tiga puluh) menit harus dengan sendirinya masuk ke dalam status hibernate atau shut down.

Pengendalian Keamanan Operasonal bertujuan Tujuan dari kebijakan keamanan operasional sistem informasi adalah untuk memastikan pengoperasian aset pengolahan dan penyimpanan informasi secara benar

dan aman dan mencegah terjadinya eksploitasi atas kelemahan sistem informasi.

9.1 Tanggung Jawab dan Prosedur Operasional

9.1.1 Dokumentasi Prosedur Operasional

Unit kerja harus menjamin bahwa seluruh prosedur operasional yang terkait dengan penggunaan perangkat pengolah informasi dan komunikasi didokumentasikan, dirawat dan bisa didapatkan dengan mudah oleh pegawai yangmembutuhkannya. Prosedur operasional harus berisikan antara lain:

1) Tatacara pengolahan dan penanganan informasi.
2) Tatacara menangani kesalahan-kesalahan atau kondisi khusus yang terjadi beserta pihak yang harus dihubungi bila mengalami kesulitan teknis.
3) Standar baseline konfigurasi keamanan yang ditetapkan oleh Petugas Keamanan Informasi khusus untuk aset RAHASIA.
4) Cara memfungsikan kembali perangkat dan cara mengembalikan perangkat ke keadaan awal saat terjadi kegagalan sistem.
5) Tatacara backup dan pengelolaan catatan penggunaan (audit *trail*) dan catatan kejadian/kegiatan sistem (*system log*).

9.1.2 Manajemen Perubahan

Seluruh perubahan pada fasilitas pengolahan informasi yang dapat berimplikasi pada keamanan informasi, perlu diperlakukan secara terkendali, mencakup antara lain:

1) menyusun perencanaan mengenai perubahan yang mungkin terjadi serta melakukan pengujian terkait terpenuhinya persyaratan keamanan.
2) melakukan kajian atas implikasi perubahan pada operasional sistem yang mungkin terjadi.
3) mengajukan persetujuan secara formal atas perubahan yang akan dilakukan.
4) mencatat seluruh perubahan yang telah dilakukan.

9.1.3 Manajemen Kapasitas

a. Unit kerja harus memantau penggunaan aset yang dimiliki dan membuat proyeksi kebutuhan ke depan untuk menjamin ketersediaan aset yang diperlukan.
b. Penggunaan sumber daya sistem informasi utama, seperti server data (file server), server surat elektronik (email server) dan sistem lainnya yang kritis bagi kegiatan penggunaan perangkat harus dimonitor sehingga kapasitas tambahan dapat segera disediakan saat diperlukan.
c. Unit kerja harus menentukan threshold untuk masing-masing kapasitas yang diukur untuk dievaluasi tindak lanjut yang diperlukan.

9.1.4 Pemisahan Lingkungan Pengembangan, Pengujian, dan Operasional

a. Untuk mengurangi peluang modifikasi yang tidak berwenang atau kesalahan penggunaan sistem informasi, Unit kerja yang mengelola infrastruktur dan TIK menjamin pemisahan fasilitas pengembangan, tes dan operasional.
b. Untuk menghindari penyalahgunaan akses atau terjadinya perubahan sistem yang tidak dikehendaki, pengembangan dan pengujian perangkat lunak harus dilakukan pada perangkat yang berbeda dari yang digunakan untuk operasional.
c. Jika pengelolaan fasilitas pengolah informasi diserahkan kepada mitra, unit kerja harus menjamin dilakukannya evaluasi terhadap risiko dan ditetapkannya kontrol-kontrol untuk mengurangi setiap potensi kerusakan atau kehilangan data. Kontrol-kontrol ini harus disertakan dalam kontrak kerja.

9.2 Perlindungan dari Malware

9.2.1 Alat Kendali Terhadap Malware

a. Unit Kerja harus mempunyai alat kendali (*control*) untuk mendeteksi dan mencegah masuknya perangkat lunak yang membahayakan ke dalam jaringan komputer. Alat kendali minimum yang harus dimasukkan mencakup :
   1. Pemasangan anti-virus yang dijaga kemutakhirannya secara berkala.

2. Kebijakan yang mewajibkan pengguna (*user*) memeriksa lampiran(*attachment)* surat elektronik (*e-mail*) dan arsip (*file*) yang diambil dari Internet dari kandungan virus sebelum digunakan.
3. Peningkatan kemampuan pengguna melalui pelatihan, sosialisasi, dan tindakan-tindakan praktis untuk mencegah atau menghilangkan virus.

b. Unit kerja yang mengelola infrastruktur dan TIK harus memantau jaringan dari ancaman virus dan dapat mem-block akses ke website yang dapat menimbulkan ancaman kepada sistem informasi;
c. Setiap insiden terkait dengan malware harus dilaporkan kepada Petugas Keamanan Informasi sistem dan dikategorikan sebagai insiden keamanan informasi

9.3 Back Up

9.3.1 Back Up Informasi

a. Seluruh informasi penting dan kritikal yang dikelola unit kerja diback-up secara berkala untuk menjamin keutuhan dan ketersediaannya saat diperlukan.
b. Unit kerja harus menetapkan mekanisme yang mencakup daftar informasi yang perlu dibackup, cara dan media penyimpan backup, serta jadwal pelaksanaan backup berdasarkan kritikalitas informasi yang telah ditetapkan.
c. Informasi yang RAHASIA dan SANGAT RAHASIA harus disimpan di media backup dengan akses yang dibatasi. Hal ini untuk memelihara kerahasiaan, ketersediaan, dan keutuhan informasi serta mengurangi dampak kelemahan keamanan fisik.
d. Unit kerja pengelola infrastruktur dan TIK harus melakukan backup terhadap database dan aplikasi pada infrastruktur pengganti (DRC) berdasarkan kritikalitas sistem yang distujui oleh Komite Pengarah keamanan informasi.
e. Parameter backup berdasarkan klasifikasi sistem kritikal sebagai berikut:
    1. Cakupan Backup : Aplikasi dan database
    2. Frekuensi Backup : Harian
    3. Pengujian Restore : Tahunan
f. Unit kerja pengelola infrastruktur dan TIK bersama – sama dengan unit kerja pemilik sistem informasi menentukan jadwal pengujian restore data dan didokumentasikan.

9.4 Logging dan Monitoring untuk mencatat kejadian dan menghasilkan bukti

9.4.1 Log Kejadian

a. Sistem harus dikonfigurasi untuk melakukan pencatatan (logging) atas seluruh aktivitas pengguna, jaringan, sistem, aplikasi, error yang terjadi (exceptions).
b. Gangguan keamanan informasi yang ditemukan selama pemantauan harus segera dicatat dan dilaporkan ke Pejabat Keamanan Informasi terkait.
c. Pejabat Keamanan Informasi akan melakukan evaluasi mendalam terhadap laporan-laporan hasil pemantauan, khususnya pada penggunaan yang tidak wajar dari aset-aset informasi yang mungkin merupakan penyalahgunaan aset tersebut.

9.4.2 Perlindungan terhadap Informasi Log

a. Log kejadian dan hasil pemantauan adalah aset informasi yang dilindungi keamanan oleh unit kerja pemilik sistem informasi.
b. Fasilitas pencatatan log dan informasi log yang dicatat harus dilindungi dari penghapusan dan akses oleh pihak yang tidak berwenang;

9.4.3 Log administrator dan operator

Sistem informasi harus dapat mencatat seluruh kegiatan system administrator dan system operator dalam log administrator dan log operator yang dilindungi keamanannya

9.4.4 Sinkronisasi Jam

Semua fasilitas pemrosesan informasi yang terhubung ke jaringan internal perlu melakukan sinkronisasi waktu dari semua sistem pemrosesan informasi yang relevan dalam suatu organisasi atau domain keamanan dengan sumber waktu akurat yang sudah disepakati secara berkala.

9.5 Pengendalian terhadap Software yang Operasional

9.5.1 Instalasi Software ke Sistem yang Operasional

a. Proses untuk mengendalikan instalasi perangkat lunak pada sistem operasional harus ditetapkan dan diimplementasikan untuk memastikan terjaganya kerahasiaan, integritas dan keterseiaan informasi;
b. Proses pemutakhiran (update) perangkat lunak operasional hanya akan dilakukan oleh pegawai yang berwenang.

c. Proses pemutakhiran pada perangkat kritikal di Data Center tidak boleh dilakukan terhadap sistem operasional sebelum pengujiannya dinyatakan selesai dan berhasil serta mendapatkan persetujuan dari penanggung jawab sistem tersebut.

d. Salinan versi terkini dari perangkat lunak yang akan dimutakhirkan disimpan ditempat yang aman sebagai antisipasi terhadap keadaan yang tidak dikehendaki.

9.6 Pengelolaan Kerentanan Teknis

9.6.1 Pengelolaan Kerentanan Teknis

a. Pemilik aset informasi wajib melakukan upaya-upaya identifikasi atas kelemahan teknis (*vulnerabilities*) dari seluruh aset informasi dibawah pengelolaannya

b. Tindakan pengendalian yang sesuai untuk meminimalkan resiko atas hilangnya aset informasi berdasarkan evaluasi dan penilaian risiko terhadap kerentanan teknis yang ditemukan dalam sistem informasi. Tindakan pengendalian dapat berupa penonaktifan fitur tertentu, perbaikan/upgrade sistem, aplikasi, atau patching.

9.7 Pertimbangan dalam Audit Sistem Informasi

9.7.1 Alat Kendali Audit Sistem Informasi

a. Setiap sistem informasi di lingkungan Unit kerja dapat dilakukan proses audit yang mencakup proses verifikasi terhadap sistem informasi dan/atau informasi di unit kerja dengan mempertimbangkan sebagai berikut:

   1. harus direncanakan dan dikelola dengan baik untuk meminimalisasi gangguan terhadap proses bisnis
   2. Setiap proses audit yang membutuhkan akses kepada sistem informasi dan/atau informasi unit kerja harus disetujui oleh pemilik dari sistem dan/atau informasi tersebut
   3. Hak akses untuk kebutuhan audit harus dibatasi hanya hak akses *read only*
   4. Instalasi dari tools yang digunakan untuk proses audit hanya dapat dilakukan oleh personil yang berwenang yaitu administrator jaringan dan sistem TI di unit kerja, dan harus segera dihapus setelah proses audit telah selesai dilakukan.

BAB X

PENGENDALIAN KEAMANAN KOMUNIKASI

Pengendalian keamanan komunikasi bertujuan untuk memastikan keamanan jaringan dan keamanan pertukaran informasi.

10.1. Pengelolaan Keamanan Jaringan

10.1.1 Pengendalian Jaringan

a. Unit kerja yang mengelola infrastruktur dan TIK harus mengelola dan mengamankan jaringan internal di Badan POM untuk menjamin:
   1. Pencegahan akses tanpa izin ke jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan
   2. Keamanan dari informasi milik Badan POM yang dikirimkan melalui jaringan
   3. Integritas dan ketersediaan dari layanan jaringan Badan POM.

b. Pengelolaan keamanan jaringan meliputi:
   1. Pemantauan kegiatan pengelolaan jaringan untuk menjamin bahwa perangkat jaringan digunakan secara efektif dan efisien
   2. Pengendalian dan pengaturan tentang penyambungan atau perluasan jaringan internal atau eksternal Badan POM
   3. Pengendalian dan pengaturan akses ke sistem jaringan internal atau eksternal Badan POM
   4. Pencatatan informasi pihak ketiga yang diizinkan mengakses ke jaringan Badan POM dan menerapkan pemantauan serta pencatatan kegiatan selama menggunakan jaringan
   5. Pemutusuan layanan tanpa pemberitahuan sebelumnya jika terjadi gangguan keamanan informasi
   6. Perlindungan jaringan dari akses yang tidak berwenang mencakup:
      a. Penetapan untuk penanggung jawab pengelolaan jaringan dipisahkan dari pengelolaan perangkat pengolah informasi
      b. Penerapan pengendalian khusus untuk melindungi keutuhan informasi yang melewati jaringan umum antara lain dengan penggunaan enkripsi
      c. Pendokumentasian arsitektur jaringan harus dipastikan terkini dan terkendali.

c. Kegiatan jaringan akan dipantau untuk menjamin bahwa sumber daya jaringan digunakan secara efektif dan efisien, dan agar kesalahan pemrosesan tidak terjadi.

d. Akses ke layanan jaringan unit kerja hanya diberikan kepada personil yang terotorisasi berdasarkan prinsip *need to have*.

e. Penyambungan atau perluasan jaringan komputer, akses ke sistem jaringan internal atau eksternal ditentukan berdasarkan kebutuhan kegiatan Badan POM dan dikendalikan serta diatur oleh unit kerja yang mengelola infrastruktur dan TIK. Persetujuan perluasan jaringan Internal, External dan persetujuan perencanaan serta persetujuan pelaksanaan hanya dapat diberikan oleh Kepala Unit kerja yang mengelola infrastruktur dan TIK.

10.1.2 Keamanan Layanan Jaringan

a. Unit kerja yang mengelola infrastruktur dan TIK mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan serta mencantumkannya dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh pihak ketiga

b. Konfigurasi dari jaringan, perangkat aktif dan perangkat keamanan jaringan harus ditinjau secara berkala untuk:
   1) Memastikan kesesuaian dengan kondisi terkini.
   2) Mengidentifikasi kerawanan pada jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan.

c. Jaringan internal Badan POM harus dipisahkan dari jaringan eksternal dengan menggunakan security gateway atau firewall dan harus dikonfigurasikan untuk memfilter traffic tanpa izin maupun *traffic* yang mencurigakan.

d. Koneksi ke *security gateway* atau firewall harus diotentikasikan, diotorisasi dan diamankan dengan metode pengamanan yang sesuai, misalnya dengan virtual private network (VPN), secure shell (SSH) atau metode kriptografi.

e. Akses dari jaringan eksternal yang dilakukan oleh vendor pihak ketiga hanya dapat diberikan untuk kebutuhan *troubleshooting* dan harus secara formal disetujui dan didokumentasikan dan harus dibatasi waktunya sesuai dengan kebutuhan dari akses.

f. Penggunaan pihak ketiga penyedia layanan jaringan harus dimonitor untuk menjamin kesesuaian dengan prasyarat keamanan Badan POM.

g. Mekanisme keamanan, tingkat layanan dan prasyarat pihak ketiga penyedia jaringan harus diidentifikasi dan dimasukkan kedalam perjanjian layanan jaringan.

h. Akses oleh pihak ketiga ke jaringan Badan POM hanya diberikan untuk pelaksanaan kegiatan di lingkungan Badan POM, dan setelah perjanjian kontrak dan kesepakatan Kewajiban Menjaga Rahasia (*Non-Disclosure Agreement/ NDA*) disetujui oleh kedua belah pihak.

i. Pihak ketiga yang diijinkan masuk ke jaringan *Data Center* Badan POM harus dirinci secara jelas hak aksesnya dan kegiatannya selama menggunakan jaringan akan dipantau, diawasi dan dicatat.

10.1.3 Pemisahan dalam Jaringan

a. Jaringan internal perusahaan harus disegmentasi baik secara fisik maupun logical untuk meningkatkan keamanan dan untuk mengendalikan akses dan traffic jaringan berdasarkan kritikalitas dari sistem dalam jaringan Badan POM.

b. Segmentasi jaringan harus ditinjau paling sedikit satu kali dalam tiga bulan untuk menjamin kesesuaian dengan prasyarat keamanan terkini.

10.2. Transfer Informasi

10.2.1 Kebijakan dan Prosedur Transfer Informasi

a. Penyediaan informasi internal Badan POM bagi masyarakat umum harus disetujui oleh pemilik informasi dan dilindungi keutuhannya dari modifikasi oleh pihak yang tidak berwenang

b. Unit Kerja harus menjamin bahwa pertukaran informasi penting dan rawan hanya dilakukan setelah melalui suatu pengkajian risiko yang memadai dan penetapan ketentuan-ketentuan keamanan informasi dalam perjanjian pertukaran informasi antara pihak yang terkait.

c. Aset informasi yang dikirim dengan menggunakan jasa layanan kurir atau pos rawan diakses oleh pihak yang tidak berwenang selama pengiriman. Unit Kerja menerapkan alat kendali berikut :

   1. Mencatat secara lengkap dan jelas identitas kurir yang digunakan.
   2. Mengemas aset informasi dalam kemasan yang baik dan kuat yang mampu melindungi kandungannya dari kerusakan fisik selama pengiriman.

10.2.2 Kesepakatan terkait Transfer Informasi

a. Pertukaran informasi antara Badan POM dengan pihak ketiga hanya akan dilakukan atas persetujuan tertulis kedua belah pihak.
b. Pertukaran informasi digital harus disetujui oleh Pimpinan Unit Kerja.

10.2.3 Pesan Elektronik

a. Prosedur pertukaran informasi bila menggunakan perangkat komunikasi elektronik mencakup :
   1. Perlindungan pertukaran informasi dari pencegatan, penyalinan, modifikasi, miss routing dan perusakan
   2. Pendeteksian dan perlindungan terhadap kode berbahaya yang dapat dikirim melalui penggunaan komunikasi elektronik
   3. Perlindungan informasi elektronik dalam bentuk attachment yang memiliki klasifikasi RAHASIA
b. Ketentuan dalam pengguaan email adalah sebagai berikut:
   1. Tidak mendistribusikan materi yang melecehkan, mendiskriminasikan, yang membakar emosi atau menimbulkan kebencian atau membuat pernyataan palsu atau yang bersifat merusak mengenai orang lain
   2. Pengguna dilarang untuk mendistribusikan informasi Badan POM yang bersifat rahasia tanpa izin dari pemilik informasi
   3. Pesan penyangkalan ini harus dituliskan pada akhir setiap e-mail. *"Pesan ini mungkin berisi informasi rahasia dan hanya ditujukan kepada pihak yang dituju. Apabila anda bukanlah pihak yang dituju, anda dilarang untuk mengungkapkan, menyebarkan atau menyalin isi email ini. Apabila anda mendapatkan email ini tanpa sengaja mohon segera hubungi pengirim email dan hapus email ini segera. Badan POM tidak bertanggung jawab untuk pengiriman informasi ini secara lengkap dan tepat dan juga tidak bertanggung jawab untuk keterlambatan dalam pengiriman email ini."*
c. Unit kerja yang membidangi infrastruktur dan TIK yang mengelola akun email Badan POM berhak untuk mem-block akun email pengguna pada saat terdapat bukti memadai terkait penyalahgunaan dan/atau pelanggaran keamanan

10.2.4 Kerahasiaan atau Non Disclosure Agreement

Akses ke sistem informasi baik oleh pegawai maupun pihak ketiga hanya diberikan untuk pelaksanaan kegiatan di Badan POM, dan setelah perjanjian kontrak dan kesepakatan Kewajiban Menjaga Rahasia (*Non-Disclosure Agreement/ NDA*) disetujui oleh kedua belah pihak.

BAB XI

PENGENDALIAN PENGADAAN, PENGEMBANGAN, DAN PEMELIHARAAN SISTEM

Keamanan informasi dalam pengadaan, pengembangan, dan pemeliharaan sistem informasi bertujuan untuk memastikan bahwa keamanan informasi merupakan bagian yang terintegrasi dengan sistem informasi, mencegah terjadinya kesalahan, kehilangan, serta modifikasi oleh pihak yang tidak berwenang.

11.1. Persyaratan Keamanan dalam Sistem Informasi

11.1.1 Analisa dan Spesifikasi Persyaratan Keamanan

a. Pemilik sistem informasi menetapkan dan mendokumentasikan secara jelas persyaratan-persyaratan keamanan informasi yang relevan sebelum pembangunan, perluasan, atau pengadaan sistem informasi baru.
b. Persyaratan keamanan harus diidentifikasi secara jelas di dalam dokumen persyaratan dan spesifikasi perangkat lunak;
c. Spesifikasi ini harus disetujui baik oleh pemilik aset informasi yang terlibat dan pengembang sistemnya sebelum kegiatan penulisan program dimulai.

11.1.2 Pengamanan Layanan Aplikasi pada jaringan publik

a. Informasi yang digunakan oleh aplikasi Badan POM yang ditransimisikan melalui jaringan publik (internet) harus diamankan dari aktivitas fraud, kemungkinan adanya contract dispute dan pengungkapan dan/atau perubahan informasi tanpa izin.
b. Pengamanan informasi terhadap informasi yang ditransmisikan melalui sistem informasi yang digunakan dapat mencakup namun tidak terbatas pada:
    1. Proses otentikasi dan otorisasi terhadap pengguna aplikasi
    2. Perlindungan untuk memastikan kerahasiaan dan integritas informasi yang dipertukarkan melalui jaringan publik
    3. Perlindungan terhadap session transaksi untuk menghindari duplikasi dan/atau modifikasi
    4. Mengamankan jalur komunikasi antara pihak-pihak yang terlibat

11.2. Keamanan dalam Proses Pengembangan dan Dukungan

11.2.1 Kebijakan Pengembangan yang Aman

a. Unit kerja terkait mengawasi dan memantau pengembangan perangkat lunak yang dilakukan oleh pihak mitra kerja untuk memastikan bahwa proses pengembangannya memenuhi syarat-syarat keamanan informasi yang ditetapkan dalam kontrak.

b. Aturan untuk pengembangan sistem harus ditetapkan dan diimplementasikan untuk proses pengembangan sistem di Badan POM yang mencakup:

   1) Pengamanan dari lingkungan pengembangan, seperti pemisahan lingkungan pengembangan baik secara fisik dan/atau logikal, pengendalian akses, pengelolaan perubahan
   2) Panduan secure coding
   3) Pengedalian versi aplikasi
   4) Penyimpanan dari source code
   5) Metode pengujian untuk mengidentifikasi dan memperbaiki *vulnerability*.

11.2.2 Prosedur Pengendalian Perubahan

a. Pemilik sistem informasi menetapkan prosedur pengendalian perubahan untuk mengelola perubahan pada aplikasi dan sistem operasi melalui prosedur pengendalian perubahan.

b. Perubahan terhadap perangkat lunak, baik perangkat lunak yang dikembangkan sendiri maupun yang dipasok oleh mitra kerja, akan dikontrol dengan membatasi tanggung jawab dan wewenang melakukan perubahan pada pengelola sistem.

c. Perubahan-perubahan terhadap perangkat lunak yang dipasok mitra kerja akan dikelola berdasarkan kontrak perjanjian dengan pemasok.

11.2.3 Kajian Teknis terhadap Aplikasi setelah perubahan platof

Apabila platform operasional, misalnya sistem operasi, database dan/atau middleware, dari sistem informasi Badan POM mengalami perubahan, aplikasi kritikal Badan POM harus ditinjau dan diuji untuk memastikan tidak ada dampak buruk terhadap operasional dan keamanan organisasi

11.2.4 Pembatasan Perubahan terhadap Paket Software

a. Pembelian paket *software* dilaksanakan melalui lima tahap yaitu:
   1. Tahap perencanaan
   2. Tahap pendefinisian kebutuhan (*requirement*)
   3. Tahap pendefinisian detail spesifikasi teknis (diantaranya proses *Proof of Concept*)
   4. Tahap instalasi, konfigurasi, dan uji coba
   5. Tahap implementasi.

11.2.5 Prosedur Pengembangan Sistem

a. Pengembangan aplikasi dilakukan dengan memperhatikan keamanan, kelengkapan, akurasi, dan keutuhan informasi yang akan dihasilkan, serta kerahasiaan informasi yang digunakan.
b. Pengembangan aplikasi yang dilakukan baik secara *in-house* maupun outsource dilaksanakan dengan mengikuti prinsip *Software Development Life Cycle* (SDLC) melalui lima tahap, yaitu:
   1) Tahap perencanaan
   2) Tahap pendefinisian kebutuhan (*requirement*)
   3) Tahap perancangan dan pembangunan
   4) Tahap pengujian
   5) Tahap implementasi.

11.2.6 Lingkungan Pengembangan yang Aman

a. Pemilik sistem informasi menyediakan lingkungan pengembangan yang aman dan terpisah dari server operasional untuk memastikan pengembangan layanan baru tidak menganggu aplikasi yang sedang operasional.
b. Unit kerja pemilik sistem informasi harus menetapkan lingkungan pengembangan yang aman untuk pengembangan dan integrasi sistem Badan POM. Hal ini dapat mencakup namun tidak terbatas pada:
   1) Pemisahan lingkungan pengembangan baik secara fisik dan/atau logikal
   2) Pengendalian akses
   3) Perpindahan data dari dan ke lingkungan pengembangan

11.2.7 Pengembangan oleh Pihak Outsourcing

a. Dalam hal pengembangan aplikasi dilakukan oleh pihak ketiga (*outsource*), tahapan perencanaan dan pendefinisian kebutuhan

dilakukan oleh pihak unit kerja, jika perlu melibatkan pihak ketiga. Sedangkan tahapan kegiatan perancangan, pembangunan aplikasi (*coding*), pengujian, dan implementasi dilakukan oleh pihak ketiga dengan diawasi oleh penanggung jawab pengembangan di Unit kerja.

b. Unit Kerja pemilik sistem informasi harus mengawasi aktivitas pengembangan sistem yang dialihdayakan (*outsourced*). Hal ini dapat mencakup:
   1) Perjanjian terkait lisensi dan kepemilikan sistem
   2) Pengujian penerimaan sistem untuk menguji kualitas dan akurasi dari sistem
   3) Prasyarat dokumentasi untuk sistem
   4) Perjanjian escrow
c. Hak untuk melakukan audit proses pengembangan dan kontrol yang diimplementasikan oleh vendor.
d. Unit kerja pemilik informasi harus memperhatikan kelangsungan pemeliharaan sistem yang mencakup Dokumentasi, masa garansi, dan *Transfer of Knowledge*.

11.2.8 Pengujian Keamanan Sistem

a. Unit Kerja bertanggung jawab untuk membuat perencanaan pengujian aplikasi yang mencakup pendekatan/metode, alur, dan parameter pengujian.
b. Kriteria dan jadwal untuk pengujian penerimaan sistem harus ditetapkan untuk sistem informasi baru, upgrade dan versi baru dari sistem informasi
c. Pengujian terhadap suatu aplikasi dapat dilakukan secara bertingkat mulai dari unit testing, integration testing, system testing, sampai dengan *User Acceptance Testing* (UAT).
d. Unit testing dipersiapkan dan dilakukan oleh masing-masing developer pada lingkungan pengembangan dengan mengacu kepada standar pengujian yang telah ditentukan.
e. Integration testing dipersiapkan dan dilakukan oleh pengembang di lingkungan pengembangan.

11.3. Data Pengujian

11.3.1 Pengamanan Data Pengujian

a. Data yang digunakan dalam pengujian sistem (system test data) harus dilindungi dari kemungkinan rusak, hilang atau perubahan yang dilakukan tanpa ijin.

b. Pengamanan terhadap Data hasil pengujian perlu diperhatikan sebagai berikut:

1) Data untuk pengujian sistem harus dipilih secara hati-hati untuk menghindari pengungkapan atau perubahan informasi sensitif oleh pihak yang tidak berhak, serta melindung dari kemungkinan kerusakan dan kehilangan informasi

2) *Masking* data harus dilakukan apabila data operasional yang sensitif digunakan untuk keperluan pengujian

3) Data operasional yang digunakan untuk keperluan pengujian harus dihapus segera setelah proses pengujian telah selesai dilaksanakan.

BAB XII

PENGENDALIAN HUBUNGAN DENGAN PENYEDIA

Hubungan dengan penyedia produk atau jasa ke Badan POM harus dikendalikan untuk memastikan keamanan informasi organisasi yang dapat diakses oleh penyedia produk/ jasa.

12.1 Keamanan dalam Hubungan dengan Penyedia Produk/ Jasa

12.1.1 Kebijakan Keamanan Informasi yang Berhubungan dengan Penyedia Produk/ Jasa

a. Unit kerja harus mempertimbangkan aspek keamanan Informasi dalam hubungan dengan pemasok mulai dari pemilihan, penunjukan, monitoring, evaluasi,sampai dengan terminasi.
b. Pejabat keamanan informasi menetapkan kebijakan dan aturan penggunaan aset-aset informasi bagi penyedia.
c. Akses terhadap aset informasi di lingkungan Badan POM harus dikontrol secara ketat. Sebelum memberikan akses kepada penyedia produk/ jasa, wajib dideteksi dan dievaluasi risiko-risiko yang mungkin muncul sehubungan dengan pemberian akses dan menerapkan kontrol yang memadai untuk mengurangi dampak atau mencegah terjadinya risiko-risiko tersebut.
d. Pengendalian risiko pemberian akses pada penyedia jasa/ supplier dilakukan antara lain melalui klausul-klausul dalam perjanjian kontrak dan melalui perjanjian Kesepakatan Kewajiban Menjaga Rahasia (*Non-Disclosure Agreement/ NDA*)

12.1.2 Pemuatan Isu Keamanan Informasi dalam Kontrak Kerja dengan Penyedia

a. Dalam perjanjian kontrak dengan Penyedia Produk/ Jasa harus dicantumkan antara lain :
    1) Kewajiban Penyedia Produk/ Jasa untuk mematuhi kebijakan keamanan informasi yang berlaku di Badan POM
    2) Persetujuan untuk turut melindungi keamanan aset informasi Badan POM terkait dengan akses yang diberikan.
    3) Jenis akses yang diberikan dan tata cara penggunaan akses tersebut dan mekanisme pemantauannya.
    4) Identitas dari pegawai Penyedia Produk/ Jasa yang menggunakan akses ini.

5) Pembatasan lokasi darimana akses dapat dilakukan dan waktu penggunaan akses.

b. Pihak ketiga dalam menyediakan jasa layanannya kepada Badan POM dan atau dalam melaksanakan baik sebagian atau seluruh pekerjaannya di Badan POM, harus menjamin bahwa segala persyaratan keamanan informasi yang berlaku di Badan POM ditulis di dalam perjanjian kontrak.

c. Kontrak yang dimaksud di butir di atas harus mencantumkan :

1. Jaminan bahwa pihak ketiga bertanggung jawab terhadap keamanan aset informasi Badan POM .
2. Kendali, baik fisik dan atau logikal, yang diterapkan untuk membatasi akses ke aset informasi hanya kepada personil yang telah diberikan otorisasi.
3. Tanggung jawab hukum (aspek legal) terhadap segala gangguan keamanan informasi yang mereka timbulkan selama menjalankan pekerjaan tertuang dalam kontrak.
4. Sumber daya yang terlibat dalam kegiatan sesuai klausul kontrak.

12.2 Pengelolaan Pemberian Layanan oleh Penyedia Produk/ Jasa

12.2.1 Monitoring dan Review Layanan Penyedia Produk/ Jasa

a. Unit Kerja memastikan bahwa penyedia produk/ jasa memelihara kemampuan menyediakan layanan yang ditetapkan.

b. Layanan yang disediakan penyedia produk/ jasa dipantau dan ditinjau ulang untuk melihat tingkat kesesuaiannya terhadap persyaratan yang ditetapkan paling sedikit satu kali dalam tiga bulan;

c. Unit kerja dapat melakukan audit terhadap penyediaan layanan yang diberikan pemasok paling sedikit satu kali dalam satu tahun;

d. Ketentuan dalam pelaksanaan audit kepada pemasok sebagai berikut:

1) Tanggung jawab untuk mengaudit tingkat layanan dimiliki oleh pihak, baik internal maupun eksternal, yang memiliki independensi dari pengguna layanan yang diberikan oleh supplier dan ditunjuk secara formal

2) Setiap ketidaksesuaian yang ditemukan dalam proses peninjauan dan audit harus dikelola dan ditindaklanjuti

12.2.2 Pengelolaan Perubahan terhadap Layanan Penyedia Produk/ Jasa

a. Perubahan layanan yang disediakan penyedia produk/ jasa dikelola dengan memperhatikan tingkat kerawanan sistem dan proses yang terkait dan hasil kaji ulang risikonya.

b. Perubahan terhadap layanan yang diberikan oleh supplier harus disetujui oleh Pimpinan unit kerja yang relevan dan diformalisasikan dalam kontrak kerja.

BAB XIII

PENGENDALIAN PENGELOLAAN GANGGUAN KEAMANAN INFORMASI

Pengendalian pengelolaan gangguan keamanan informasi ini bertujuan untuk memastikan adanya pendekatan yang konsisten dan efektif atas penanganan insiden keamanan informasi.

13.1 Pengelolaan Manajemen Insiden

13.1.1 Tanggung Jawab dan Prosedur

a. Kejadian (insiden) keamanan informasi adalah sebuah kejadian pada sistem, layanan ataupun jaringan yang dapat mengindikasikan adanya pelanggaran keamanan informasi atau kegagalan keamanan atau kejadian yang mungkin memiliki keterkaitan dengan keamanan informasi
b. Guna memastikan proses penanganan insiden yang responsif dan efektif, perlu dikembangkan berbagai prosedur yang mencakup:
    1) perencanaan dan persiapan penanganan insiden
    2) pemantauan, analisis, dan pelaporan atas insiden
    3) pencatatan atas aktivitas penanganan insiden
    4) penanganan bukti forensik
    5) penilaian dan pengambilan keputusan atas insiden dan kelemahan keamanan informasi
    6) pemulihan insiden.

13.1.2 Pelaporan Kejadian Gangguan Keamanan Informasi

a. Seluruh pegawai, mitra kerja dan pihak ketiga harus melaporkan sesegera mungkin ke Petugas Keamanan Informasi bila menemui kelemahan atau menjumpai terjadinya gangguan/insiden keamanan informasi.
b. Setiap kejadian insiden keamanan informasi harus dianalisis, diklasifikasikan,dan ditentukan skala prioritas penanganannya. Penanganan insiden beserta pemulihannya dilakukan berdasarkan klasifikasi dan prioritas yang telah ditetapkan.
c. Setiap insiden keamanan informasi harus ditangani dengan baik untuk mencegah meluasnya insiden, untuk memulihkan layanan atau informasi yang mungkin hilang dan untuk meminimalisasi dampak dari insiden

d. Setiap tindakan penanganan kejadian, kelemahan dan insiden keamanan informasi harus didokumentasikan dengan baik.

13.1.3 Penilaian dan Pengambilan Keputusan Terkait Gangguan Keamanan Informasi

a. Pejabat Keamanan Informasi harus mengevaluasi laporan dan penyelesaian insiden keamanan informasi untuk mengidentifikasi jenis, volume dan biaya yang terkait untuk keperluan pengawasan dan evaluasi kinerja.
b. Semua data dan rekaman yang dibutuhkan untuk menganalisa dan menyelesaikan insiden keamanan informasi harus diamankan. Untuk insiden yang terkait dengan tindakan perdata atau pidana, pengamanan rekaman harus sesuai dengan peraturan dan hukum yang berlaku

13.1.4 Respon terhadap Gangguan Keamanan Informasi

a. Petugas Keamanan Informasi harus merespon gangguan keamanan informasi berdasarkan hasil penilaian dan pengambilan keputusan penanganan terhadap gangguan keamanan informasi
b. Tindakan untuk memulihkan keamanan dari pelanggaran dan perbaikan kegagalan sistem harus dikendalikan secara hati-hati dan formal, prosedur harus memastikan bahwa:
    1) Hanya pegawai yang sudah diidentifikasi dan berwenang yang diizinkan untuk mengakses langsung ke sistem dan data
    2) Semua tindakan darurat yang diambil, didokumentasikan secara rinci
    3) Tindakan darurat dilaporkan kepada pihak berwenang
    4) Keutuhan sistem dan pengendaliannya dikonfirmasikan dengan pihak-pihak terkait sesegera mungkin

13.1.5 Belajar dari Gangguan Keamanan Informasi

a. Seluruh gangguan keamanan informasi yang terjadi dan tindakan mengatasinya harus dicatat dalam buku catatan pelaporan gangguan keamanan informasi, dan akan menjadi masukan pada proses peningkatan penanganan gangguan keamanan informasi
b. Seluruh catatan gangguan keamanan informasi akan dievaluasi dan dianalisa untuk perbaikan dan pencegahan agar gangguan keamanan informasi tidak berulang

13.1.6 Pengumpulan Bukti

a. Badan POM harus mengumpulkan, menyimpan dan menyajikan bukti pelanggaran terhadap kebijakan dan standar pengelolaan keamanan informasi Badan POM.

b. Jejak audit dan bukti serupa harus dikumpulkan dan diamankan untuk:

   1) Analisis masalah internal

   2) Digunakan sebagai bukti forensik yang berkaitan dengan potensi pelanggaran kontrak atau peraturan atau persyaratan dalam hal proses pidana atau perdata

   3) Digunakan sebagai bahan tuntutan ganti rugi pada pihak ketiga yang menyediakan perangkat lunak dan layanan

BAB XIV

PENGENDALIAN PENGELOLAAN KELANGSUNGAN KEGIATAN DARI SISI KEAMANANNYA

Keamanan informasi dalam pengelolaan kelangsungan kegiatan bertujuan untuk melindungi sistem informasi, memastikan berlangsungnya kegiatan dan layanan pada saat keadaan darurat serta memastikan pemulihan yang tepat.

14.1 Aspek Keamanan Informasi di dalam Pengelolaan Kelangsungan Layanan

14.1.1 Perencanaan Kelangsungan Keamanan Informasi

a. Badan POM mengembangkan suatu Kebijakan Pengelolaan Kelangsungan Kegiatan sistem informasi Badan POM untuk mengurangi dampak kegagalan sistem informasi atau bencana yang menyebabkan terganggunya kegiatan Badan POM .
b. Kebijakan Pengelolaan Kelangsungan Layanan TIK dilakukan dengan mempertimbangkan:
    1) Identifikasi aset-aset informasi vital dan sensitif, khususnya yang berklasifikasi RAHASIA.
    2) Identifikasi kejadian-kejadian yang menyebabkan gangguan tehadap proses kegiatan penting.
c. Unit Kerja harus menetapkan Prasyarat untuk keberlanjutan keamanan informasi dan diintegrasikan dengan prasyarat keberlanjutan bisnis organisasi untuk menjamin keberlanjutan dari keamanan informasi di Badan POM, pada saat dan setelah terjadinya gangguan besar atau bencana.
d. Prasyarat keamanan informasi dapat diintegrasikan pada siklus proces business continuity management yang mencakup:
    1) Memahami kebutuhan organisasi
    2) Menentukan strategi BCM
    3) Mengembangkan dan mengimplementasikan rencana penanggulangan / keberlanjutan bisnis
    4) Pengujian, pemeliharaan dan peninjauan rencana penanggulangan / keberlanjutan bisnis
e. Tim Pengelola Keamanan Informasi Badan POM mengelola DRP dan salinannya serta informasi lain yang diperlukan dalam penanganan disaster di lokasi yang aman dan mudah dijangkau.

f. Badan POM menerapkan strategi recovery layanan Badan POM sebagai berikut:
   1) *Hot Recovery*. Untuk Layanan dengan tingkat kritikalitas sangat tinggi. Tersedia layanan cadangan di DRC yang bersifat full redundancy (realtime atau periodic data replication).
   2) *Warm Standby*. Untuk Layanan dengan tingkat kritikalitas tinggi. Tersedia perangkat cadangan di DRC yang meliputi perangkat keras, sistem operasi, aplikasi dan data.
   3) *Cold Standby*. Untuk layanan dengan tingkat kritikalitas rendah. Tidak tersedia perangkat cadangan. Layanan tersedia setelah dilakukan pengadaan perangkat, melakukan instalasi atau restorasi sistem operasi, aplikasi, data dan sasaran unjuk kerja Layanan disesuaikan dengan kebutuhan.

14.1.2 Pelaksanaan Rencana Keberlangsungan Keamanan Informasi

a. Untuk menjamin agar Pengelolaan Kelangsungan Sistem Badan POM tetap relevan dan efektif, Pengelolaan Kelangsungan Sistem Badan POM harus diuji secara periodik. Hasil-hasil pengujian Pengelolaan Kelangsungan Sistem Badan POM dan tindakan-tindakan lanjutan yang perlu diambil dilaporkan ke Kepala Badan POM.
b. Pengelolaan Kelangsungan sistem Badan POM harus dilaksanakan untuk menjamin tetap beroperasinya Badan POM pada keadaan darurat sesuai dengan kebutuhan dan jangka waktu yang ditetapkan.
c. Penanggulangan keadaan darurat secara langsung ditangani oleh Tim Pengelola Keamanan Informasi yang keanggotaannya disesuaikan setiap satu tahun sekali.
d. Unit Kerja yang dalam pelaksanaan tugas dan fungsinya mengandalkan layanan *Data Center* Badan POM harus mempersiapkan prosedur kerja alternatif sesuai dengan ketentuan yang berlaku untuk mengurangi gangguan operasional pada saat terjadi keadaan darurat.
e. Tim Pengelolaan BCP Keamanan Informasi Badan POM memastikan kesiapan dan keahlian pegawai serta pihak terkait lainnya dalam menghadapi keadaan darurat dengan melaksanakan pelatihan secara berkala.

14.1.3 Verifikasi, Reviu dan Evaluasi Keberlangsungan Keamanan Informasi

a. Tim Pengelola BCP harus merencanakan dan mengkoordinasikan kegiatan uji coba secara berkala terhadap proses, prosedur, petunjuk pelaksanaan, sarana dan perangkat, untuk memastikan apakah berfungsi sebagaimana mestinya pada saat diperlukan.

b. Badan POM menerapkan dua metode uji coba yaitu:
   1) Uji fungsi (functional testing) untuk memastikan bagian-bagian dari Disaster Recovery Plan berfungsi sebagaimana mestinya. Uji fungsi dilaksanakan secara periodik.
   2) Uji coba keseluruhan (full scale testing) untuk memastikan seluruh bagian dari *Disaster Recovery Plan* berfungsi sebagaimana mestinya. Uji coba keseluruhan dilaksanakan secara periodik.

c. Uji coba keseluruhan harus dapat mensimulasikan kondisi darurat yang paling mendekati keadaan nyata dengan menggunakan skenario terburuk.

d. Pelaksanaan uji coba harus memperhatikan hal-hal berikut:
   1) Kesesuaian dengan kebutuhan
   2) Kemungkinan timbulnya dampak negatif
   3) Waktu dan lama pelaksanaan
   4) Kebutuhan sumberdaya dan biaya
   5) Kesiapan pelaksanaan
   6) Ketergantungan dengan pihak ketiga
   7) Secara formal mendapat persetujuan Kepala Badan POM

e. Hasil uji coba (uji fungsi dan uji coba keseluruhan) harus dievaluasi dan dijadikan sebagai masukan untuk perbaikan Disaster Recovery Plan, termasuk didalamnya perbaikan profil risiko, rencana mitigasi, materi pelatihan dan awareness.

f. Seluruh proses, prosedur dan petunjuk pelaksanaan Pengelolaan Kelangsungan sistem Badan POM dan Disaster Recovery Plan harus terdokumentasi dengan baik dan senantiasa diperbaharui sesuai dengan kebutuhan.

g. Tim Pengelola BCP harus melakukan review terhadap akurasi proses, prosedur dan petunjuk pelaksanaan secara berkala minimal 1 kali dalam 1 tahun.

14.2 Redundansi

14.2.1 Ketersediaan fasilitas pemrosesan informasi

a. Aspek redundansi harus ditetapkan untuk fasilitas pengolahan informasi dan sarana pendukungnya untuk memastikan ketersediaan dari proses bisnis dan operasional Badan POM serta pemberian layanan Badan POM

b. Fasilitas pengolahan informasi beserta sarana pendukungnya yang telah memenuhi aspek redundansi harus diuji secara berkala untuk menjamin kesesuaian dari fungsinya.

c. Guna menjamin ketersediaan layanan serta keamanan informasi dalam kondisi darurat (misalnya: bencana alam) pada lokasi utama, perlu adanya redundansi terhadap fasilitas pengolahan informasi yang disebut sebagai fasilitas *Backup Site*. *Backup Site* yang dimaksud dapat berupa lokasi kerja pengganti atau *Disaster Recovery Center* (DRC) bagi alternatif area Data Center.

d. Tim Pengelola Keamanan Informasi Data Center Badan POM mengupayakan tersedianya sarana *Disaster Recovery* yang paling tepat untuk memastikan ketersediaan layanan Data Center Badan POM utama dalam keadaan darurat sesuai tingkat kritikalitas proses bisnis terkait.

e. Ketentuan dalam pengelolaan terkait *Backup Site* meliputi:

   1) lokasi *Backup Site* secara geografis memiliki probabilitas kejadian bencana alam yang minimal

   2) *Backup Site* ditujukan sebagai media penyimpanan backup alternatif, serta sebagai fasilitas pengolahan informasi alternatif

   3) terpenuhinya pemulihan layanan operasional sepenuhnya pada fasilitas *Backup Site* sesuai kerangka parameter RTO (*Recovery Time Objective)*

   4) Pengelola Backup Site beserta Pemilik Aset Informasi melakukan uji keberlangsungan secara berkala dibawah koordinasi Penanggung Jawab Kelangsungan Bisnis, minimal 1 kali dalam setahun, untuk menguji kesiapan seluruh pihak dalam hal:

      (i) memindahkan operasional ke fasilitas *Backup Site*

      (ii) memulihkan operasional aplikasi beserta data sesuai parameter RPO (*Recovery Point Objective*) yang telah ditetapkan

f. DRC harus berada di lokasi yang memiliki profil risiko berbeda dengan Data Center dan harus berada di wilayah geografis Republik Indonesia.

BAB XV

PENGENDALIAN KEPATUHAN

Pengendalian kepatuhan bertujuan untuk menghindari pelanggaran terhadap peraturan perundangan yang terkait keamanan informasi.

15.1 Kajian Keamanan Informasi

15.1.1 Kajian Independen terhadap Keamanan Informasi

Secara berkala dilakukan review terhadap keamanan informasi Badan POM oleh pihak independen untuk menjamin dipatuhinya kebijakan, prosedur dan standar keamanan informasi di Badan POM

15.1.2 Kepatuhan terhadap kebijakan dan standar keamanan informasi

a. Kepala Badan POM menjamin dipatuhinya kebijakan, prosedur dan standar keamanan informasi di unit organisasi yang menjadi tanggungjawabnya dengan cara:
   1) Mengkomunikasikan kebijakan, pedoman dan prosedur keamanan informasi ke seluruh pegawai di unit organisasinya.
   2) Meningkatkan pengetahuan dan keterampilan pegawai.
   3) Memeriksa dan mengevaluasi tingkat kepatuhan pegawai secara berkala.

b. Ketidakpatuhan terhadap kebijakan, prosedur dan standar keamanan informasi Badan POM harus dicari penyebab utamanya, dan ditindaklanjuti untuk mencegah terjadinya hal serupa di kemudian hari. Pemeriksaan kepatuhan secara teknis seperti tes penetrasi (penetration test), pemindaian jaringan (scanning) atau teknik pencarian kelemahan keamanan informasi lainnya akan dilakukan secara berkala oleh pegawai yang betul-betul ahli dibidangnya, baik dari internal Badan POM atau menggunakan jasa ahli independen dari luar Badan POM .

15.1.3 Inspeksi Kepatuhan Teknis

a. Rencana pemeriksaan kepatuhan teknis harus didokumentasikan, dikomunikasikan dan disetujui Pimpinan unit kerja yang mengelola infrastruktur dan TIK.
b. Hasil-hasil pemeriksaan teknis dicatat dan dilaporkan sebagai masukan bagi evaluasi manajemen keamanan informasi.

15.2 Kepatuhan terhadap Persyaratan Hukum dan Kontraktual

15.2.1 Identifikasi persyaratan hukum dan kontraktual yang dapat diaplikasikan

a. Seluruh pengguna Badan POM, termasuk mitra kerja, dan pihak ketiga lainnya, harus mematuhi kebijakan keamanan informasi Badan POM, mentaati ketentuan hukum dan undang-undang yang relevan serta perjanjian tentang lisensi, termasuk persyaratan-persyaratan kontrak yang telah disetujui.

b. Badan POM menjamin bahwa setiap ketentuan hukum dan perundang-undangan yang relevan dengan sistem informasi yang dimiliki Badan POM akan diidentifikasi, didokumentasikan dan dipelihara kemutakhirannya.

15.2.2 Hak Atas Kekayaan Intelektual

a. Badan POM menjamin bahwa perangkat lunak yang dipasang di sistem komputer milik Badan POM mematuhi ketentuan penggunaan lisensi secara tepat. Penggandaan perangkat lunak secara tidak sah tidak diijinkan dan merupakan bentuk pelanggaran terhadap kebijakan Badan POM dan ketentuan hak cipta.

b. Setiap penemuan, kegiatan, atau gagasan-gagasan praktis yang diperoleh pegawai Badan POM selama bekerja untuk Badan POM, dan dihasilkan oleh sumber daya milik Badan POM, adalah menjadi hak milik eksklusif Badan POM.

c. Daftar lisensi perangkat lunak dipelihara dan diperbarui minimum setahun sekali. Lisensi perangkat lunak yang disediakan Badan POM tidak boleh digunakan atau dipasang di peralatan komputer selain milik Badan POM.

d. Pemeriksaan berkala terhadap lisensi perangkat lunak yang terpasang akan dilakukan untuk memastikan kebijakan ini diterapkan secara efektif.

15.2.3 Pengamanan Informasi yang terdokumentasi

a. Rekaman-rekaman penting milik Badan POM dan atau yang digunakan, dihasilkan oleh sistem informasi/aset informasi yang dikelola Badan POM (database, audit log, transaction log) harus dilindungi dari kehilangan, kerusakan atau penyalahgunaan, sesuai peraturan atau Undang-Undang yang berlaku.

b. Dokumen-dokumen penting Badan POM harus dilindungi dari kehilangan, pemalsuan, kerusakan, atau penyalahgunaan sesuai

dengan peraturan perundangan, regulasi, dan persyaratan kontrak dan bisnis.

15.2.4. Privasi dan pengamanan informasi personal

a. Badan POM melindungi kepemilikan dan kerahasiaan data pribadi pegawai selama yang bersangkutan bekerja di Badan POM. Data pribadi pegawai hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundang-undangan.

b. Seluruh pengguna sistem computer, baik pegawai Badan POM, mitra kerja dan pihak ketiga lainnya harus dicegah dari penyalahgunaan hal akses yang diberikan kepadanya.

c. Untuk mencegah kesalahan dan penyalahgunaan pemanfaatan asset informasi, Badan POM akan melakukan sosialisasi kebijakan keamanan informasi secara berkala dan memberikan pelatihan sesuai dengan hak akses yang dimiliki pengguna (*user*).

15.2.5. Regulasi untuk alat kriptografi

Data yang sensitif dan berisiko tinggi harus diamankan secara ketat baik dari aspek penyimpanannya maupun perlindungan secara eknsripsi bila ditransfer via email, atau jaringan.

KEPALA BADAN PENGAWAS OBAT DAN MAKANAN
REPUBLIK INDDONESIA,

ttd.

PENNY K. LUKITO