KEPALA BADAN PENGAWAS OBAT DAN MAKANAN
REPUBLIK INDONESIA

KEPUTUSAN KEPALA BADAN PENGAWAS OBAT DAN MAKANAN
NOMOR 444 TAHUN 2023
TENTANG
PEDOMAN MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN BADAN PENGAWAS OBAT DAN MAKANAN

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN PENGAWAS OBAT DAN MAKANAN,

Menimbang :

a. bahwa untuk melindungi kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availibility*) serta pembuktian keaslian (*authentication*) dan kenirsangkalan (*non repudiation*) aset informasi Badan Pengawas Obat dan Makanan dari berbagai bentuk ancaman keamanan informasi baik dari dalam maupun luar lingkungan Badan Pengawas Obat dan Makanan, perlu disusun Pedoman Manajemen Keamanan Informasi di lingkungan Badan Pengawas Obat dan Makanan;
b. bahwa ketentuan mengenai Keamanan Informasi di lingkungan Badan Pengawas Obat dan Makanan sebagaimana ditetapkan dalam Keputusan Kepala Badan Pengawas Obat dan Makanan Nomor 115 Tahun 2022 tentang Pedoman Manajemen Keamanan Informasi di Lingkungan Badan Pengawas Obat dan Makanan, perlu disesuaikan dengan perkembangan hukum sehingga perlu diganti;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Kepala Badan Pengawas Obat dan Makanan tentang Pedoman Manajemen Keamanan Informasi di Lingkungan Badan Pengawas Obat dan Makanan;

Mengingat :

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah 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 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196);

3. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Tahun 2019 Nomor 185);
4. Peraturan Presiden Nomor 80 Tahun 2017 tentang Badan Pengawas Obat dan Makanan (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 180);
5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
6. Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 233);
7. Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 99);
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 Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2016 Nomor 1829);
10. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);
11. Peraturan Badan Pengawas Obat dan Makanan Nomor 21 Tahun 2020 tentang Organisasi dan Tata Kerja Badan Pengawas Obat dan Makanan (Berita Negara Republik Indonesia Tahun 2020 Nomor 1002) sebagaimana telah diubah dengan Peraturan Badan Pengawas Obat dan Makanan Nomor 13 Tahun 2022 tentang Perubahan atas Peraturan Badan Pengawas Obat dan Makanan Nomor 21 Tahun 2020 tentang Organisasi dan Tata Kerja Badan Pengawas Obat dan Makanan (Berita Negara Republik Indonesia Tahun 2022 Nomor 629);
12. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 1375) sebagaimana diubah Peraturan Badan Siber dan Sandi Negara Nomor 9 Tahun 2021 tentang Perubahan Atas Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2021 tentang Penyelenggaraan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001 Menggunakan Indeks Keamanan Informasi (Berita Negara Republik Indonesia Tahun 2021 Nomor 975);

13. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
14. Peraturan Badan Pengawas Obat dan Makanan Nomor 19 Tahun 2023 tentang Organisasi dan Tata Kerja Unit Pelaksana Teknis pada Badan Pengawas Obat dan Makanan (Berita Negara Republik Indonesia Tahun 2023 Nomor 611);
15. Peraturan Badan Pengawas Obat dan Makanan Nomor 21 Tahun 2023 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Pengawas Obat dan Makanan (Berita Negara Republik Indonesia Tahun 2023 Nomor 622);
16. Keputusan Kepala Badan Pengawas Obat dan Makanan Nomor HK.00.06.74.3496 Tahun 2009 tentang Teknologi Informasi dan Komunikasi Terintegrasi di lingkungan Badan Pengawas Obat dan Makanan;

Memperhatikan : Pedoman Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 6 Tahun 2023 Tentang Tata Cara Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;

MEMUTUSKAN:

Menetapkan : KEPUTUSAN KEPALA BADAN PENGAWAS OBAT DAN MAKANAN TENTANG PEDOMAN MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN BADAN PENGAWAS OBAT DAN MAKANAN.

Kesatu : Menetapkan dan memberlakukan Pedoman Manajemen Keamanan Informasi di lingkungan Badan Pengawas Obat dan Makanan yang selanjutnya disebut Pedoman sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan ini.

Kedua : Pedoman sebagaimana dimaksud dalam diktum Kesatu digunakan sebagai acuan bagi seluruh unit kerja dan unit pelaksana teknis di lingkungan Badan Pengawas Obat dan Makanan dalam melaksanakan penerapan dan pengelolaan keamanan informasi yang mencakup perlindungan terhadap aset informasi, perangkat keras, perangkat lunak, jaringan, sarana pendukung dan keamanan fisik area kerja.

Ketiga : Proses penerapan dan pengelolaan keamanan informasi sebagaimana dimaksud dalam diktum Kedua dikoordinasikan pimpinan unit kerja dan pimpinan unit pelaksana teknis berkoordinasi dengan serta dimonitor oleh pimpinan unit kerja yang membidangi Teknologi Informasi dan Komunikasi.

Keempat : Dalam hal penerapan dan pengelolaan keamanan informasi tidak memenuhi ketentuan dalam Keputusan ini, pimpinan unit kerja yang membidangi Teknologi Informasi dan Komunikasi dapat memberikan arahan dan audit untuk memastikan kepatuhan Keamanan Informasi BPOM.

Kelima : Tim Koordinasi SPBE mengoordinasikan penyediaan dukungan penerapan keamanan informasi yang dilakukan dengan meningkatkan kapasitas terhadap:
a. sumber daya manusia keamanan Informasi; dan
b. anggaran Keamanan sesuai dengan perencanaan kebutuhan dan ketersediaan anggaran.

Keenam : Pada saat Keputusan ini mulai berlaku, Keputusan Kepala Badan Pengawas Obat dan Makanan Nomor 115 Tahun 2022 Tentang Kebijakan Keamanan Informasi di Lingkungan Badan Pengawas Obat dan Makanan dicabut dan dinyatakan tidak berlaku.

Ketujuh : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 21 November 2023

PLT. KEPALA BADAN PENGAWAS OBAT DAN MAKANAN,

LUCIA RIZKA ANDALUSIA

Salinan Keputusan ini disampaikan kepada:
1. Pejabat Pimpinan Tinggi Madya Badan Pengawas Obat dan Makanan;
2. Pejabat Pimpinan Tinggi Pratama Badan Pengawas Obat dan Makanan;
3. Kepala Unit Pelaksana Teknis di lingkungan Badan Pengawas Obat dan Makanan.

LAMPIRAN
KEPUTUSAN KEPALA BADAN PENGAWAS OBAT DAN MAKANAN
NOMOR 444 TAHUN 2023
TENTANG
PEDOMAN MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN BADAN PENGAWAS OBAT DAN MAKANAN

PEDOMAN MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN BADAN PENGAWAS OBAT DAN MAKANAN

BAB I
PENDAHULUAN

A. LATAR BELAKANG

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 5 (lima) 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.
4. *Authentication* yaitu aspek pembuktian keaslian atas informasi dan/atau terhadap pihak-pihak terkait dalam pemanfataan dan pengolahan informasi.
5. *Non-Repudiation* yaitu aspek kenirsangkalan untuk memastikan agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi melalui suatu mekanisme tertentu.

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

B. TUJUAN

Kebijakan Keamanan Informasi di lingkungan BPOM digunakan sebagai pedoman pengelolaan keamanan informasi BPOM dalam rangka melindungi Aset Informasi BPOM serta menjamin kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), keaslian (*authenticity*) dan kenirsangkalan (*non-repudiation*) Aset Informasi. Adapun sasaran Penyelenggaraan Keamanan Informasi adalah:

a. Terselenggaraanya layanan sistem elektronik yang memperhatikan tingkat keamanan sistem dan informasi.
b. Terlaksanaanya peningkatan proses keamanan informasi di lingkungan Organisasi BPOM 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.
e. Terlaksananya perlindungan aset informasi dari penyalahgunaan oleh pihak yang tidak berkepentingan atau tidak berhak mengelola informasi.

C. RUANG LINGKUP

Kebijakan ini berlaku untuk pengelolaan pengamanan seluruh aset informasi BPOM dan dilaksanakan oleh seluruh unit kerja, pegawai BPOM baik sebagai pengguna maupun pengelola Teknologi Informasi dan Komunikasi (TIK) dan pihak ketiga di lingkungan BPOM.

Penetapan ruang lingkup ini dilandasi oleh isu-isu internal keamanan SPBE di BPOM sebagai berikut:

1. penyelenggaraan layanan elektronik BPOM semakin luas dan intensif serta memerlukan pengamanan yang memadai dan menyeluruh;
2. tingkat kesadaran keamanan informasi pengguna yang relatif belum memadai dan masih beragam;
3. pelaksanaan aktivitas pengamanan data, aplikasi, dan infrastruktur TIK semakin krusial dalam penyelenggaraan layanan elektronik yang berkualitas;
4. perlunya peningkatan berkelanjutan dalam penyelenggaraan keamanan informasi BPOM; dan
5. penerapan kebijakan Manajemen Keamanan Informasi yang dilakukan secara menyeluruh.

Adapun pertimbangan isu-isu eksternal BPOM antara lain:

1. Potensi ancaman keamanan informasi yang semakin tinggi dan beragam, serta memiliki dampak yang serius dalam penyelenggaraan layanan elektronik.
2. Peraturan perundang-undangan, standar, dan *best practices* keamanan informasi yang semakin berkembang.
3. Isu-isu eksternal lainnya yang sesuai dengan ketentuan peraturan perundang-undangan.

D. PENGERTIAN UMUM

1. Aset BPOM adalah sumber daya yang memiliki nilai bagi BPOM.
2. Aset informasi, meliputi data/dokumen mencakup: data keuangan, data kepegawaian dokumen penawaran tender dan kontrak dengan pihak ketiga yang terkait dengan pengamanan data BPOM, dokumen perjanjian kerahasiaan, kebijakan BPOM, hasil penelitian serta pedoman/prosedur operasional berikut dokumentasi keluaran (*catatan; apakah rincian data perlu disebutkan secara menyeluruh dan jika iya maka perlu di petakan data-data yang termasuk dalam klasifikasi terbatas/rahasia dan sangat rahasia untuk perlindungan keamanan data ini).
3. Aset berwujud *(tangible)* meliputi: sumber daya manusia, gedung dan bangunan, perangkat computer, perangkat jaringan dan komunikasi, removable media, dan perangkat pendukung lainnya.
4. Aset tak berwujud *(intangible)* meliputi: pengetahuan, pengalaman, keahlian, citra dan reputasi.
5. Dokumen adalah data atau informasi yang tertulis atau tercetak yang dapat dipergunakan sebagai bukti atau keterangan. Dokumen dapat berbentuk *file* elektronik (*softcopy*) atau cetakan (*hardcopy*).

6. 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.
7. 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.
8. Informasi adalah sekumpulan data atau fakta yang dikelola menjadi sesuatu yang bermanfaat atau memiliki nilai bagi pemilik atau penerimanya.
9. Insiden keamanan informasi adalah peristiwa yang mengakibatkan tidak tercapainya aspek kerahasiaan, integritas, ketersediaan, keaslian atau kenirsangkalan aset milik BPOM dan mengakibatkan dampak gangguan terhadap proses kerja BPOM.
10. Kajian Risiko adalah keseluruhan proses analisis dan evaluasi risiko.
11. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian (*authenticity*) dan kenirsangkalan (*non-repudiation*) informasi.
12. Kebijakan Manajemen Keamanan Informasi adalah serangkaian aturan terkait keamanan informasi di lingkungan BPOM dalam rangka melindungi aset informasi milik BPOM, meliputi kebijakan keamanan informasi, standar teknis, dan kebijakan dasar (*baseline*) konfigurasi keamanan sistem dan perangkat TIK di lingkungan BPOM.
13. Kelemahan keamanan informasi adalah kondisi yang berpotensi mengakibatkan tidak tercapainya aspek kerahasiaan, integritas, ketersediaan, keaslian atau kenirsangkalan aset milik BPOM.
14. Koordinator keamanan Informasi adalah personil setingkat Koordinator atau Subkoordinator yang ditunjuk oleh Kepala Unit kerja atau setingkat eselon II di BPOM untuk melaksanakan kegiatan penerapan kebijakan dan prosedur keamanan informasi di lingkungan BPOM tempat dia ditugaskan. Petugas Keamanan Informasi bekerja dibawah pengawasan dan pengarahan Koordinator Keamanan Informasi.
15. Manajemen Puncak keamanan Informasi adalah pejabat setingkat Eselon II yang ditunjuk oleh Kepala BPOM untuk mengkoordinasikan dan mengarahkan kegiatan penerapan kebijakan dan prosedur keamanan informasi di lingkungan BPOM.
16. *Mobile Computing* adalah penggunaan perangkat komputasi jinjing (*portable*), seperti *notebook*/laptop dan *smartphone*, untuk melakukan akses/konektivitas, pengolahan data dan penyimpanan data
17. Panduan adalah rekomendasi tindakan yang dianjurkan dapat dilakukan untuk mencapai suatu sasaran.
18. Pedoman adalah kumpulan ketentuan yang menjadi dasar, pegangan, acuan atau petunjuk dan memberi arah bagaimana sesuatu harus dilakukan.
19. Pemilik Aset Informasi adalah pihak yang secara hukum ditunjuk sebagai penanggung jawab aset informasi atau proses kerja di BPOM/pimpinan unit organisasi dimana data/informasi itu dibuat.
20. Penasehat adalah pejabat yang memberikan arahan terhadap masukan proyek TI dan penanganan masalah atau risiko-risiko yang signifikan dan berdampak pada kegiatan operasional BPOM.
21. Pengguna adalah pihak atau personil yang menggunakan sistem informasi dan diberikan hak akses berdasarkan level tertentu.
22. Pemasok adalah penyedia yang menyalurkan layanan (barang dan/atau jasa) kepada entitas bisnis di lingkungan BPOM.

23. Perangkat jaringan adalah peralatan jaringan komunikasi data, yang mencakup antara lain namun tidak terbatas pada: *modem, hub, router, switch, firewall, repeater, bridge, server*.
24. Perangkat lunak meliputi: perangkat lunak aplikasi, perangkat lunak sistem operasi, perangkat lunak pemrograman dan perangkat lunak tambahan/program bantu.
25. Perangkat pengolah informasi adalah perangkat yang digunakan untuk memproses informasi, termasuk namun tidak terbatas pada komputer, laptop, telepon dan fax, printer, mesin fotokopi.
26. Perangkat pendukung adalah peralatan yang berfungsi untuk menjamin beroperasinya perangkat pengolah informasi serta melindunginya dari kerusakan, termasuk namun tidak terbatas pada *Uninterruptible Power Supply* (UPS), genset, pemadam api ringan (*fire extinguisher*), *access door electronic*, HVAC, A/C, CCTV, sensor suhu, sensor temperatur, sensor air.
27. Pihak ketiga adalah seluruh pihak yang terkait dan berkepentingan atau memiliki hubungan dengan proses bisnis di BPOM yang berada di luar struktur organisasi BPOM.
28. Prosedur adalah serangkaian kegiatan, tindakan yang harus dijalankan dengan cara yang baku agar selalu memperoleh hasil yang sama dari keadaan yang sama.
29. Rekaman adalah dokumen yang menyatakan hasil yang dicapai atau memberi bukti suatu aktivitas dilakukan.
30. Sistem informasi adalah serangkaian perangkat keras, perangkat lunak, sumber daya manusia, serta prosedur dan/atau aturan yang diorganisasikan secara terpadu untuk mengolah data menjadi informasi yang memiliki manfaat untuk mencapai suatu tujuan.
31. Sistem Manajemen Keamanan Informasi (SMKI) adalah kerangka kerja manajemen pengamanan informasi yang menggunakan pendekatan berbasis risiko dalam menyusun, menerapkan, melaksanakan, mengawasi, mengkaji, memelihara dan meningkatkan kinerja keamanan informasi.
32. *Teleworking* adalah aktivitas dengan perjanjian kerja untuk melaksanakan pekerjaan secara jarak jauh (*remote*) untuk mengakses informasi atau sistem informasi di sistem atau jaringan internal BPOM melalui jaringan eksternal atau publik.
33. Unit kerja adalah organisasi di lingkungan BPOM setingkat eselon II, termasuk Unit Pelaksana Teknis.
34. Unit kerja pengelola TIK BPOM adalah organisasi yang menyelenggarakan tata kelola, pengelolaan dan pemanfaatan TIK di lingkungan BPOM.

BAB II
KEBIJAKAN MANAJEMEN KEAMANAN INFORMASI

A. KETENTUAN UMUM

Penanggungjawab penerapan sistem manajemen keamanan informasi adalah Tim Koordinasi SPBE BPOM, yang dalam penyelenggaraannya dikoordinasikan oleh unit kerja pengelola TIK BPOM. Pimpinan unit kerja harus memastikan tanggung jawab dalam penerapan sistem manajemen keamanan melalui:

1. Unit kerja harus menerapkan kebijakan keamanan informasi sebagaimana diatur dalam Keputusan Kepala BPOM ini di lingkungan Unit Kerja masing-masing.
2. Unit kerja menetapkan perencanaan penerapan manajemen keamanan informasi di lingkungan unit kerja masing-masing, berkoordinasi dengan Unit Kerja Pengelola TIK BPOM yang mencakup:
   a. edukasi kesadaran Keamanan SPBE;
   b. penilaian kerentanan Keamanan SPBE;
   c. peningkatan Keamanan SPBE;
   d. penanganan insiden Keamanan SPBE; dan
   e. audit Keamanan SPBE
3. Unit kerja memberikan pernyataan komitmen penerapan Kebijakan Manajemen Keamanan Informasi serta penerapan pengendalian Keamanan Informasi oleh masing-masing unit kerja dengan berbasis risiko.
4. Unit kerja menerapkan dan mengembangkan manajemen risiko dengan mengikuti ketentuan mengenai manajemen risiko yang berlaku di lingkungan BPOM. Pertimbangan lain dalam pengelolaan risiko di unit kerja harus memperhatikan:
   a. Kajian risiko yang dilakukan secara periodik minimal 1 (satu) tahun sekali terhadap aset-aset informasi 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.
   b. Setiap risiko yang perlu dimitigasi berdasarkan hasil kajian risiko perlu dilakukan proses pengendalian risiko dengan memilih opsi penanganan risiko dengan dapat memperhatikan kontrol keamanan informasi berdasarkan standar keamanan atau kontrol lainnya pada peraturan perundang-undangan yang berlaku.
5. Unit kerja harus secara kontinu melakukan sosialisasi dan pelatihan mengenai Keamanan Informasi kepada seluruh pegawai. Sosialisasi dan pelatihan harus mempertimbangkan penerapan kontrol keamanan yang dijalankan pada setiap fungsi yang terdapat di unit kerja di BPOM.
6. Unit kerja mengendalikan dan mengkoordinasikan komunikasi, baik internal ataupun eksternal, yang relevan dengan Keamanan Informasi yang bertujuan untuk memastikan adanya informasi terkait Keamanan Informasi kepada pihak-pihak yang berkepentingan.
7. Unit kerja mengelola dokumentasi terkait pengelolaan keamanan informasi dalam suatu prosedur yang bertujuan untuk menjaga kemutakhiran dokumen dan ketersediaannya, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan dan mencegah akses oleh pihak yang tidak berwenang. Pengendalian dokumen juga mengatur mekanisme:
   a. Pengendalian catatan penerapan dan pelaksanaan keamanan informasi dilakukan untuk menjamin agar catatan tersebut dapat tersedia, terpelihara, dan terkendali.

b. Identifikasi dan pendokumentasian informasi terkait dengan keamanan informasi yang berasal dari sumber eksternal untuk memastikan kesesuaian dan kepatuhannya dan dikomunikasikan kepada pihak yang relevan dalam Kebijakan Keamanan Informasi organisasi.
c. Semua dokumentasi Kebijakan Keamanan Informasi harus ditinjau paling sedikit satu kali dalam satu tahun atau apabila terdapat perubahan dalam Kebijakan Keamanan Informasi dan/atau organisasi untuk menjamin kesesuaian dan kecukupannya.

8. Unit kerja melaksanakan pengendalian Keamanan Informasi untuk memastikan implementasi dan operasional sistem manajemen keamanan informasi melalui:
   a. Pengelolaan ketersediaan dari sumber daya yang dibutuhkan dalam rangka implementasi keamanan informasi.
   b. Memastikan koordinasi implementasi kontrol keamanan informasi terhadap data dan informasi yang dikelola telah dilakukan secara berkala.
   c. Peningkatan yang berkesinambungan yang dijabarkan dalam program aktivitas Sistem Manajemen Keamanan Informasi.
   d. Tanggung jawab atas terlaksananya kontrol keamanan informasi untuk memastikan perlindungan terhadap data dan informasi yang dikelola.
9. Unit kerja pengelola TIK berkoordinasi dengan Unit kerja melakukan evaluasi secara berkala untuk menjamin efektivitas dan meningkatkan keamanan informasi, mencakup proses pengukuran efektivitas penerapan keamanan Informasi atau pencapaian sasaran, audit internal dan tinjauan manajemen. Hasil evaluasi harus didokumentasikan secara jelas dan ditindaklanjuti.
10. Audit internal Keamanan Informasi dilaksanakan oleh fungsi kepatuhan internal atau unit yang mengkoordinasikan fungsi pengawasan internal di BPOM. Pelaksana-audit internal Keamanan Informasi harus dipastikan telah memiliki kompetensi yang memadai serta memiliki objektifitas dan independen terhadap proses audit.
11. Unit Kerja harus memastikan bahwa setiap ketidaksesuaian telah ditindaklanjuti secara memadai dan memastikan upaya berkelanjutan untuk meningkatkan kinerja dan efektivitas penerapan Kebijakan Keamanan Informasi.
12. Inisiatif peningkatan keamanan informasi harus secara formal diidentifikasi, direncanakan, diimplementasikan, dan ditinjau.
13. BPOM berperan serta secara aktif dalam pelaksanaan strategi dan rencana aksi nasional keamanan siber berkoordinasi dengan lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan sandi sesuai dengan ketentuan peraturan perundang-undangan.

B. KETENTUAN PENGENDALIAN PENGAMANAN INFORMASI

Pengendalian pengamanan informasi pada unit kerja diterapkan sesuai dengan ruang lingkup pelaksanaan keamanan Informasi di masing-masing unit kerja, mencakup 14 (empat belas) domain pengendalian sebagai berikut:

1. Kebijakan Keamanan Informasi

a. Unit kerja menerapkan kebijakan keamanan informasi sebagaimana diatur dalam Keputusan Kepala BPOM ini.
b. Unit kerja mengkomunikasikan dan mensosialisasikan kebijakan keamanan informasi kepada seluruh pegawai dan pihak terkait di lingkungan masing-masing unit kerja.
c. Unit kerja melakukan evaluasi dan peninjauan (*review*) secara berkala atas penerapan kebijakan keamanan informasi di masing-masing unit kerja.

d. Peninjauan (*review*) berkala atas kebijakan keamanan informasi dikoordinasikan oleh unit pengelola TIK.

2. Organisasi Keamanan Informasi

a. Organisasi Internal

i. BPOM menetapkan Komite Pengarah Keamanan Informasi yang bertujuan membantu Kepala BPOM dalam mengawasi tindakan perbaikan dan peningkatan terkait keamanan informasi, yang terdiri:
   1) Pimpinan unit kerja yang membawahi fungsi pengelolaan TIK;
   2) Pimpinan unit kerja yang membawahi fungsi Manajemen Risiko; dan
   3) Pimpinan unit kerja yang membawahi fungsi audit.

ii. Unit kerja membentuk tim pengelolaan keamanan informasi untuk memastikan penerapan kontrol keamanan informasi di unit kerja yang mencakup namun tidak terbatas pada peran sebagai berikut:
   1) Manajemen Puncak keamanan Informasi;
   2) Koordinator keamanan Informasi; dan
   3) Tim Keamanan Informasi, yang mencakup fungsi peran setidaknya sebagai berikut:
      a) Pengelolaan standar dan kepatuhan.
      b) Pengelolaan risiko.
      c) Pengendalian dokumen.
      d) Pengelolaan insiden keamanan informasi.

iii. Peran dan tanggung jawab dari Penasehat dan Tim Pengelola Keamanan Informasi di unit kerja dijabarkan pada lampiran terpisah.

iv. Pimpinan unit kerja menjamin dilakukannya pemisahan tugas pada proses-proses kerja yang melibatkan informasi kritikal agar tidak ada personil atau pihak yang memiliki kontrol menyeluruh terhadap semua aset informasi serta tidak terdapat konflik kepentingan. Pemisahan tugas tanggung jawab meliputi pembagian terhadap kewenangan antara lain namun tidak terbatas pada proses penginputan, validasi, persetujuan dan lainnya terhadap pengelolaan informasi yang dilakukan.

v. Unit kerja harus mengidentifikasi dan menjalin komunikasi dengan pihak-pihak berwenang di luar BPOM yang terkait dengan keamanan informasi.

vi. Unit kerja harus menjalin komunikasi dengan komunitas keamanan informasi di luar BPOM yang terkait dengan keamanan informasi. Tujuan dari keikutsertaan komunitas keamanan informasi adalah untuk mendapatkan informasi mengenai pembaharuan teknologi dan referensi keamanan informasi, ancaman yang sedang terjadi dan informasi solusi terhadap penanganan kejadian keamanan informasi.

vii. Unit kerja harus senantiasa mempertimbangkan aspek keamanan informasi dalam manajemen proyek yang dilaksanakan di BPOM.

b. Perangkat Bergerak (*Mobile Device*) dan *Teleworking*

i. Unit kerja pengelola TIK membangun kepedulian terhadap penggunaan *mobile device* dan *teleworking* terkait risiko keamanan perangkat dan risiko keamanan informasi dari masing-masing penggunaannya.

ii. Pengguna *mobile device* dan *teleworking* harus mengikuti ketentuan yang berlaku terkait penggunaan *mobile divice* dan *teleworking* untuk menjaga keamanan perangkat dan informasi di dalamnya.

3. Keamanan Sumber Daya Manusia

a. Sebelum Bekerja

i. Unit kerja, berkoordinasi dengan unit pengelola kepegawaian di BPOM, harus melaksanakan pemeriksaan latar belakang calon pegawai dan pihak ketiga yang akan bekerja di unit kerja dengan memperhatikan privasi, perlindungan data pribadi dan/atau pekerjaan, berdasarkan ketentuan peraturan dan perundangan yang berlaku.

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

iii. Peran dan tanggung jawab pegawai, mitra kerja dan pihak ketiga lainnya 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).

b. Selama Bekerja

i. Seluruh pegawai unit kerja serta mitra dan pihak ketiga lainnya harus mematuhi ketentuan terkait keamanan informasi yang berlaku di BPOM serta bersedia dikenakan sanksi sesuai ketentuan yang berlaku jika terjadi pelanggaran.

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

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

iv. Terdapat pemberian sanksi yang formal dan dikomunikasikan untuk mengambil tindakan terhadap pegawai yang melakukan pelanggaran keamanan informasi, sesuai dengan kebijakan dan prosedur yang berlaku di institusi.

c. Ketika Terdapat Perubahan Atas Status Kepegawaian

i. Unit kerja harus melakukan peninjauan dan penyesuaian terhadap aset dan hak akses setiap kali terdapat perubahan atas status kepegawaian, baik untuk pegawai maupun mitra atau pihak ketiga.

ii. Setiap pengguna harus mengembalikan sumber daya informasi milik BPOM yang digunakannya segera setelah penugasannya berakhir atau sumber daya informasi tersebut tidak lagi digunakan untuk bekerja di unit kerja.

iii. Hak akses pengguna dihapus atau dinonaktifkan segera setelah pengguna berubah tugas dan/atau fungsinya, setelah penugasan berakhir atau mutasi.

iv. 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 BPOM terutama yang terkait dengan kewajiban menjaga kerahasiaan.

4. Pengelolaan Aset

a. Tanggung Jawab Terkait Aset

i. Unit kerja melaksanakan identifikasi aset dan mendokumentasikannya dalam daftar inventarisasi aset masing-masing unit kerja.

ii. Aset 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*, perangkat jaringan komunikasi yang terdapat di area kerja.

2) Perangkat lunak, meliputi perangkat lunak yang digunakan untuk mengolah informasi dalam bentuk elektronik, yang mencakup namun tidak terbatas pada sistem operasi, aplikasi, pemrograman dan program bantu *(utility)*.

3) 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*.

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

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

6) 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*.

iii. Pemilik aset bertanggung jawab terhadap perlindungan keamanan seluruh aset informasi yang berada dibawah pengawasannya.

iv. Ketentuan penggunaan aset mengacu pada Pedoman Penggunaan Aset TI yang berlaku di BPOM. Seluruh pengguna aset, tanpa kecuali, wajib mematuhi kebijakan dan aturan yang telah ditetapkan.

b. Klasifikasi Informasi

i. Seluruh informasi yang dikelola unit kerja harus diklasifikasikan sesuai tingkat kerahasiaan, nilai, ketentuan/kebutuhan kegiatan yang menggunakannya, tingkat kerahasiaan, tingkat kritikalitas serta aspek hukumnya dan dinyatakan secara jelas pada daftar aset informasi.

ii. BPOM menetapkan 3 (tiga) golongan aset informasi sebagai berikut:

1) Rahasia

Merupakan informasi yang sangat peka dan berisiko tinggi. Hilangnya informasi ini akan menyebabkan kerugian finansial dan/atau gangguan operasional yang sangat besar. Pihak ketiga dapat mengakses informasi ini secara terbatas karena kewajiban dan kebutuhan BPOM melalui serah terima resmi dengan syarat pihak ketiga dan pegawai pihak ketiga menandatangani Kesepakatan Kewajiban Menjaga Rahasia/*Non-Disclosure Agreement*.

Contoh: Topologi Jaringan, *IP address*, *password* komputer, bahan/materi pelatihan, rencana anggaran atau pengadaan, data gaji dan penilaian kinerja pegawai, hasil *penetration test*, *log system administrator* dan data kesehatan pribadi yang secara legal harus dilindungi.

2) Terbatas
Merupakan aset informasi yang telah terdistribusi secara luas di lingkungan internal BPOM yang penyebarannya secara internal tidak lagi memerlukan izin dari Pemilik Aset Informasi dan risiko penyebarannya oleh pihak yang tidak berwenang tidak menimbulkan kerugian yang berarti. Informasi ini dapat diberikan kepada pihak ketiga oleh pemiliknya untuk kepentingan dinas melalui prosedur serah terima resmi.
Contoh: kebijakan BPOM, panduan kerja, prosedur kerja, instruksi kerja, memo/publikasi internal, informasi yang disediakan dalam intranet, dokumen kontrak dan data operasional TI lainnya.

3) Publik
Merupakan aset informasi yang secara sengaja disediakan BPOM untuk dapat diketahui publik/masyarakat umum.
Contoh: brosur, situs publik BPOM, dan siaran pers (*press release*).

iii. Pemberian label klarifikasi informasi harus dilakukan secara konsisten terhadap seluruh aset informasi. Ketentuan tata cara pemberian label klarifikasi informasi dan penanganannya ditetapkan oleh masing-masing unit kerja.

iv. Penanganan terhadap aset informasi harus mempertimbangkan tingkat klasifikasi yang telah ditetapkan oleh unit kerja. Penanganan informasi rahasia perlu mempertimbangkan proses siklus informasi mulai dari pembuatan, penggunaan, penyimpanan, distribusi, peminjaman, hingga pemusnahan. Tingkat perlindungan dan pembatasan akses harus diterapkan.

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

c. Penanganan Media

i. Penggunaan media penyimpan yang bergerak harus diperhatikan terkait penanganan dari data/informasi sesuai dengan tingkat kritikalitas dari informasi.

ii. Informasi yang terkandung dalam media penyimpan informasi yang bisa dipakai ulang dan digunakan sebagai media transit (media yang bergerak) harus dihapus jika tidak lagi diperlukan dan harus dipastikan bahwa salinan asli informasi tersebut masih tersedia.

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

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

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

vi. Pertukaran informasi antara BPOM dengan pihak lain melalui media fisik hanya akan dilakukan atas persetujuan tertulis kedua belah pihak. Pengamanan media fisik harus diperhatikan sesuai dengan informasi yang tersimpan berdasarkan tingkat kritikalitas informasi agar keamanan data terjamin saat proses pertukaran tersebut.

vii. Pengiriman media penyimpanan yang memuat informasi harus dilindungi terhadap akses yang tidak sah serta penyalahgunaan selama proses pengiriman.

5. Pengendalian Akses

a. Unit kerja menyusun, mendokumentasikan, dan mengkaji ketentuan akses terhadap aset berdasarkan kebutuhan organisasi persyaratan keamanan informasi. Ketentuan hak akses harus didokumentasikan dalam bentuk matriks hak akses.
b. 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.
c. Persyaratan untuk pengendalian hak akses mencakup:
   i. Pengembangan aturan pemberian akses perlu mempertimbangkan:
      1) Klasifikasi dari informasi;
      2) Kritikalitas dari aset yang digunakan untuk mendukung operasional bisnis;
      3) Prasyarat hukum perundang-undangan, kontraktual serta keamanan yang relevan; dan
      4) Didasarkan atas prinsip *need to know* dan *need to use*, yaitu disesuaikan dengan kebutuhan pekerjaan dan operasional dalam lingkungan BPOM.
   ii. Pemisahan peran pengendalian akses, seperti administrasi akses, dan otorisasi akses.
      1) Unit kerja pengelola TIK mengatur dan membatasi akses pengguna dalam mengakses jaringan internal BPOM sesuai peruntukannya.
      2) Unit kerja pemilik sistem informasi harus mengembangkan mekanisme pemberian hak akses pengguna dan hak akses khusus yang dikelola secara formal pada seluruh siklusnya, mulai dari proses pendaftaran, penyediaan, peninjauan (*review*), penghapusan/penonaktifan, dan penyesuaian, serta dilaksanakan oleh para pihak terkait sesuai jenjang kewenangannya.
      3) Setiap permintaan registrasi dari pengguna harus disertai surat permohonan dan harus disetujui oleh pimpinan dari pemilik sistem informasi.
      4) Hak akses khusus (*privileged access rights*) harus sangat dibatasi kepada personil yang terotorisasi dan terlatih. Hak akses khusus harus disetujui dan didokumentasikan secara formal. Pertimbangan dalam pembuatan hak akses khusus mencakup:
         a) Hak akses khusus untuk pihak ketiga hanya diberikan sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu.
         b) Hak akses khusus tidak boleh diberikan sebelum proses otorisasi dilakukan oleh pimpinan pemilik sistem informasi.
         c) Apabila memungkinkan, hak akses khusus harus dialokasikan secara individual dan tidak dibagikan. Hal ini dilakukan untuk menjamin akuntabilitas dari pengguna khusus.
         d) 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.
      5) Unit kerja memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya.

6) Setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan menyesuaikan atau menghapus hak akses khusus yang menyimpang.
7) 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.
8) Pemilik Aset Informasi harus memastikan bahwa sistem dan aplikasi dibawah pengelolaannya memiliki fasilitas manajemen hak akses pengguna, manajemen *password* yang baik, mekanisme otentikasi pengguna yang aman, serta penerapan *captcha (challenge-response test)* pada akses login.
9) Ketentuan *password* yang ditetapkan di BPOM adalah:
   a) Minimum terdiri dari 8 (delapan) karakter, dengan kombinasi:
      - angka
      - huruf besar dan huruf kecil
      - karakter khusus
   b) Tidak boleh menggunakan *password* yang mudah ditebak dan tidak terdiri dari informasi pribadi seperti ulang tahun pengguna, nama perusahaan, atau nama pengguna.
   c) *Password* diganti secara berkala atau segera diganti bila diduga telah diketahui orang lain. Periode penggantuan *password* untuk administrator dan pengguna setiap 90 hari.
10) Pengguna bertanggung jawab atas pengelolaan *password* sesuai dengan Pedoman Pengendalian Keamanan Akses di BPOM.
11) Unit kerja pengelola TIK bertanggung jawab untuk membatasi dan mengendalikan penggunaan *system utilities* pada sistem informasi. 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.
12) 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.
13) Untuk sistem aplikasi yang dikembangkan oleh penyedia jasa/pihak ketiga, *source code* dan akses terkaitnya harus diserahkan kepada BPOM. Penyedia jasa/pihak ketiga harus menjaga kerahasiaan informasi dan tidak menyebarluaskan kepada pihak yang tidak berwenang.

6. Kriptografi

a. Unit kerja pengelola TIK menerapkan kriptografi yang tepat dan efektif untuk melindungi kerahasiaan, keabsahan, integritas dan keaslian dari informasi.
b. Sistem kriptografi harus digunakan untuk melindungi aset informasi yang memiliki klasifikasi RAHASIA.
c. Pelaksanaan penerapan kriptografi disesuaikan dengan Pedoman Kriptografi/Enkripsi di BPOM.

7. Pengelolaan Keamanan Fisik dan Lingkungan

a. Pengamanan Area

i. Unit kerja harus menerapkan perimeter keamanan fisik untuk melindungi daerah-daerah yang berisi informasi dan fasilitas pengolahan informasi.

ii. BPOM menetapkan pengelompokan area wilayah/fisik di lingkungan BPOM ke dalam 3 (tiga) kategori sebagai berikut:

1) Area Publik
Area Publik merupakan wilayah area yang dapat dimasuki oleh seluruh pihak. Area publik meliputi: area *lobby*, area penerimaan tamu/resepsionis.

2) Area Terbatas
Area Terbatas merupakan wilayah area yang hanya dapat dimasuki oleh seluruh pegawai dari unit kerja serta tamu yang telah diberikan izin akses. Area Terbatas meliputi: area kerja dari unit kerja.

3) Area Tertutup
Area Tertutup merupakan wilayah area dimana terdapat proses dan/atau perangkat yang bersifat kritikal/sensitif dan hanya diperbolehkan diakses oleh kalangan pegawai tertentu dari unit kerja serta tamu yang telah memperoleh izin atau otorisasi khusus. Area Tertutup meliputi antara lain: ruang Data *Center* dan DRC, ruang perangkat jaringan, ruang arsip, ruang keuangan.

iii. Unit kerja harus menetapkan ketentuan aturan pembatasan atau prosedur untuk bekerja di area terbatas dan tertutup. Mekanisme pembatasan ini dapat dilakukan dengan aturan penerimaan tamu yang diterapkan berdasarkan kategori area tersebut.

iv. 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.

v. Pengendalian akses masuk fisik

1) Seluruh pegawai, mitra kerja, tamu, dan pihak ketiga lainnya yang memasuki lingkungan BPOM harus mengenakan kartu identitas (ID *Card*) resmi yang dikeluarkan BPOM.
2) 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 kategori area tersebut.
3) Kunjungan ke dalam area tersebut harus disetujui secara formal oleh pengelolaan area tersebut.
4) Selama kunjungan di dalam area tersebut, pengunjung harus senantiasa didampingi oleh personil unit kerja atau petugas keamanan.

6) Kartu identitas pengunjung perlu diverifikasi, disimpan oleh petugas selama kunjungan, dan dikembalikan sesudah selesai kunjungan;
7) Setiap pengunjung ke dalam area harus tercatat, mencakup jam masuk dan keluar.
8) Pengamanan kantor, ruangan, dan fasilitas menjadi beberapa level.
   a) Level pertama
      Untuk masuk ke gedung dijaga oleh petugas keamanan.
   b) Level Kedua
      masuk kedalam area tertutup diperlukan penggunaan Untuk *tools* akses fisik dan kartu akses.

vi. Seluruh area yang terdapat perangkat pemrosesan informasi harus terlindungi dari terjadinya pencurian dan akses oleh pihak yang tidak berwenang.
vii. Setiap area harus dipastikan terdapat alat pemadam kebakaran kebakaran ringan (APAR) dan diusahakan terdapat sistem pendeteksi asap (*smoke detector*) dan/atau sistem pemercik air otomatis (*sprinkler system*). Sistem pemadam kebakaran harus dipelihara secara berkala melalui pengujian rutin.
viii. Aktivitas pada area-area kritikal harus disertai dengan fasilitas CCTV dan dimonitor secara berkala.
ix. Unit kerja menjaga, mengawasi, dan mengendalikan area keluar masuk barang untuk menghindari risiko akses yang tidak terotorisasi ke informasi dan ke perangkat pengolah informasi.

b. Pengamanan Perangkat
i. Seluruh perangkat harus ditempatkan di lokasi yang aman dan diposisikan sedemikian rupa untuk mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang serta ancaman lingkungan/eksternal seperti: kebakaran, air, debu.
ii. Perangkat pendukung harus dipasang/tersedia untuk menjamin beroperasinya perangkat pengolah informasi dan secara berkala harus diperiksa dan diuji ulang kinerjanya.
iii. 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.
iv. Penempatan kabel data dan sumber daya listrik harus dilindungi dari kerusakan.
v. Pasokan listrik yang digunakan untuk mengoperasikan perangkat pengolah informasi BPOM harus mempunyai sumber alternatif dengan daya dan jangka waktu ketersediaan (jangka waktu pengoperasian) yang cukup.
vi. Unit kerja harus melaksanakan pemeliharaan (*maintenance*) perangkat secara berkala serta melindungi perangkat dan fasilitas pengelolaan informasi dari gangguan, ancaman, dan bencana dalam rangka memastikan ketersediaan, keutuhan, dan fungsinya berjalan dengan baik. Proses pemeliharaan tersebut mencakup aktivitas sebagai berikut:
   1) Seluruh perangkat pengolah informasi penting dan peralatan pendukung harus diperiksa dan diujicoba efektifitasnya secara teratur/berkala, dirawat, dan dibersihkan sesuai dengan spesifikasi pabrikannya.
   2) Perawatan dan perbaikan perangkat pengolah informasi hanya dilakukan oleh personil yang berwenang dan mempunyai kompetensi teknis yang sesuai.

3) Bagi pemeliharaan yang tidak dapat dilakukan di lokasi kantor BPOM, maka informasi rahasia dan kritikal yang tersimpan dalam peralatan tersebut harus dipindahkan terlebih dahulu dan harus mendapatkan persetujuan dari pejabat yang berwenang.

vii. Perangkat pengolah informasi penyimpan data yang tidak lagi digunakan harus disanitasi sebelum digunakan kembali atau dihapuskan/dimusnahkan. 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.

viii. Penggunaan perangkat keras yang dibawa ke luar area kerja diperbolehkan tetapi harus disetujui oleh pejabat yang berwenang.

ix. Pengguna harus memastikan aset yang tidak berada dalam pengawasan secara langsung atau yang digunakan diluar area kerja, telah diberikan perlindungan keamanan yang memadai.

x. Pengguna harus memastikan bahwa tidak terdapat atau tertampilkan informasi rahasia pada perangkat atau media yang digunakan ketika meninggalkan area kerja.

8. Keamanan Operasional

a. Prosedur Operasional dan Tanggung Jawab

i. Unit kerja harus mendokumentasikan, memelihara, dan menyediakan prosedur operasional terkait dengan penggunaan perangkat pengolah informasi bagi pengguna sesuai peruntukannya.

ii. Unit kerja harus mengendalikan setiap perubahan terkait organisasi, proses bisnis, dan fasilitas pengolah informasi, yang berdampak pada keamanan informasi. Proses pengendalian terhadap perubahan setidaknya mencakup proses permohonan, analisis, dan evaluasi serta persetujuan. Seluruh proses terkait pengelolaan perubahan harus didokumentasikan.

iii. Unit kerja harus memantau penggunaan atau utilisasi kapasitas sumber daya yang dimiliki serta membuat proyeksi kebutuhan ke depan untuk menjamin ketersediaan aset yang diperlukan. Pemantauan kapasitas tersebut dengan mempertimbangkan batas ambang kapasitas yang ditetapkan.

iv. Unit kerja pengelola TIK harus melakukan pemilahan lingkungan pengembangan, pengujian, dan operasional sistem informasi untuk mengurangi risiko perubahan dan/atau akses oleh pihak yang tidak berwenang terhadap sistem informasi.

b. Perlindungan Terhadap Ancaman Program Yang Membahayakan (*Malware*)

i. Unit kerja harus menerapkan sistem yang mampu melakukan pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan (*malware*).

ii. Sistem sebagaimana disebutkan pada butir i harus senantiasa dipantau dan dimutakhirkan untuk memastikan kesesuaiannya dengan kondisi terkini.

iii. Unit kerja pengelola TIK harus memantau dan mengevaluasi jaringan dari ancaman virus dan dapat menutup akses ke *website* yang dapat menimbulkan ancaman kepada sistem informasi.

iv. Setiap insiden terkait dengan *malware* harus dilaporkan kepada Petugas Keamanan Informasi dan dikategorikan sebagai insiden keamanan informasi.

c. Pengelolaan Pencadangan (*Backup*) Informasi
   i. Unit kerja mengidentifikasi informasi penting dan/atau kritikal yang dimiliki atau dikelola untuk kemudian menetapkan perencanaan pencadangan (*backup*) informasi yang mencakup setidaknya: jenis/nama informasi, metode dan/atau media *backup* serta periode/frekuensi pelaksanaan *backup*.
   ii. Unit kerja melaksanakan proses *backup* secara berkala sesuai dengan perencanaan yang telah ditetapkan untuk menjamin keutuhan dan ketersediaannya saat diperlukan.
   iii. Data hasil *backup* harus dilakukan uji pemulihan *(restore test)* secara berkala, sesuai dengan kategori kritikalitas sistem informasi untuk memastikan keutuhannya.
   iv. Unit kerja pengelola TIK bertanggung jawab atas proses *backup* terhadap aplikasi dan *database* dari infrastruktur utama (Data *Center*/DC) ke infrastruktur pengganti (*Disaster Recovery Center*/DRC) berdasarkan kritikalitas sistem yang disetujui oleh Komite Pengarah keamanan informasi.
d. Pengelolaan dan Pemantauan Data Aktivitas (*Log*)
   i. Unit kerja pemilik sistem informasi harus memastikan bahwa pencatatan aktivitas (*log*) pada sistem, yang mencakup: aktivitas pengguna, *exceptions*, *fault*, kejadian (*event*) keamanan informasi serta aktivitas administrator dan operator sistem telah dapat tercatat/terekam, tersimpan secara aman, dan ditinjau (*review*) secara berkala untuk membantu pengendalian akses dan investigasi dimasa mendatang.
   ii. Fasilitas pencatatan *log* dan informasi *log* yang dicatat harus dilindungi dari penghapusan dan akses oleh pihak yang tidak berwenang.
   iii. Masa penyimpanan *log* didalam sistem sekurang-kurangnya 1 (satu) bulan serta dilakukan *backup* dan pengarsipan log sekurang-kurangnya selama 12 (dua belas) bulan.
   iv. Data aktifitas (*log*) yang sudah tidak terpakai dapat dihapuskan sesuai prosedur yang berlaku.
   v. Unit kerja pemilik sistem informasi harus memastikan bahwa seluruh perangkat pengolah informasi yang dikelolanya telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.
e. Pengendalian Perangkat Lunak
   i. Proses untuk mengendalikan instalasi perangkat lunak pada sistem operasional harus ditetapkan dan diimplementasikan untuk memastikan terjaganya kerahasiaan, integritas, dan ketersediaan informasi.
   ii. Ketentuan terkait instalasi perangkat lunak pada sistem operasional dan pada perangkat pengolah informasi di pengguna ditetapkan oleh unit kerja pengelola TIK di BPOM.
   iii. Instalasi perangkat lunak hanya diperbolehkan untuk dilakukan oleh personil yang telah ditunjuk atau fungsi yang berwenang sesuai tugas dan tanggung jawabnya.
   iv. Perangkat lunak yang diinstal harus perangkat yang berlisensi atau *opensource* serta dapat diketahui asalnya usulnya.
f. Pengelolaan Kerentanan Teknis
   i. Unit kerja pengelola TIK harus melaksanakan evaluasi dan penilaian terkait kerentanan teknis pada sistem dan teknologi informasi di BPOM serta menerapkan pengendalian dan penanganan yang memadai terhadap kerentanan yang ditemukan.

ii. Pelaksanaan aktivitas terkait evaluasi kerentanan teknis dan audit sistem informasi harus direncanakan secara seksama agar tidak menimbulkan gangguan terhadap operasional sistem informasi di BPOM.

9. Keamanan Komunikasi

a. Pengelolaa Keamanan Jaringan
   i. Unit kerja pengelola TIK bertanggung jawab atas pengelolaan dan pengendalian keamanan jaringan termasuk memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi.
   ii. Pengelolaan keamanan jaringan meliputi:
      1) Pemantauan dan evaluasi kegiatan pengelolaan jaringan;
      2) Pengendalian dan pengaturan tentang penyambungan atau perluasan jaringan internal atau eksternal BPOM;
      3) Pengendalian dan pengaturan akses ke sistem jaringan internal atau eksternal BPOM;
      4) Pencatatan informasi pihak ketiga yang diizinkan mengakses ke jaringan BPOM dan menerapkan pemantauan serta pencatatan kegiatan selama menggunakan jaringan;
      5) Pemutuskan layanan jaringan jika terjadi gangguan keamanan informasi; dan
      6) Perlindungan jaringan dari akses yang tidak berwenang.
   iii. Unit kerja pengelola TIK harus menerapkan fitur keamanan layanan dan memberikan jaminan layanan jaringan yang tertuang dalam kesepakatan penyediaan layanan, termasuk layanan yang disediakan oleh Pihak Ketiga.

b. Keamanan dalam Perpindahan (*Transfer*) Informasi
   i. Penyediaan informasi internal BPOM bagi masyarakat umum harus disetujui oleh pemilik informasi dan dilindungi keutuhannya dari modifikasi oleh pihak yang tidak berwenang.
   ii. Pertukaran informasi penting dan/atau rahasia, hanya dilakukan jika telah terdapat pengendalian pengamanan yang memadai serta penetapan ketentuan-ketentuan keamanan informasi dalam perjanjian pertukaran informasi antara pihak yang terkait.
   iii. Pertukaran informasi melalui sarana surat elektronik harus memperhatikan prinsip perlindungan data dan informasi baik dari aspek penggunaan oleh pegawai maupun dari teknologi yang diterapkan.
   iv. Akses ke informasi dan sistem informasi baik oleh pegawai maupun pihak ketiga hanya diberikan untuk pelaksanaan kegiatan di BPOM dan setelah perjanjian kesepakatan Kewajiban Menjaga Rahasia (*Non-Disclosure Agreement/NDA*) disetujui oleh kedua belah pihak.

10. Akusisi, Pengembangan, dan Pemeliharaan Sistem

a. Persyaratan Keamanan Pada Sistem Informasi
   i. Pengembangan sistem informasi dalam hal ini mencakup proses atau aktivitas pembangunan sistem informasi baru, peningkatan (*enhancement*) dan/atau penambahan fungsi/fitur baru serta perbaikan kode program (*bugs fixing*).
   ii. Pemilik sistem informasi harus mengidentifikasi, menetapkan, dan mendokumentasikan secara jelas persyaratan-persyaratan keamanan informasi yang relevan sebelum pelaksanaan pengembangan sistem informasi, pada dokumen persyaratan dan spesifikasi perangkat lunak.

iii. Persyaratan dan spesifikasi sebagaimana tercantum pada butir i harus disetujui dan disepakati bersama antara pemilik aset informasi yang terlibat serta pihak pengembang sistem sebelum kegiatan pengembangan sistem informasi dimulai.
iv. Unit kerja pengelola TIK harus melindungi informasi dalam layanan aplikasi yang melewati jaringan publik dari kemungkinan aktivitas penipuan (*fraud*), perselisihan kontrak (*contract dispute*), dan pengungkapan informasi yang tidak sah.
v. Unit kerja pengelola TIK harus melindungi informasi dalam transaksi pada layanan aplikasi untuk mencegah transmisi yang tidak lengkap, kesalahan *routing*, dan perubahan serta pengungkapan dan duplikasi pesan yang tidak sah.

b. Keamanan Dalam Proses Pengembangan dan Pendukung
i. Unit kerja pengelola TIK harus menetapkan ketentuan pengembangan sistem informasi yang aman.
ii. Kebutuhan terkait keamanan informasi harus dimasukkan dalam persyaratan untuk perancangan sistem informasi yang baru atau ditambahkan pada sistem informasi yang sedang berjalan.
iii. Unit kerja yang melakukan pengembangan sistem informasi harus mengawasi dan memantau pengembangan sistem informasi yang dilakukan oleh pihak ketiga untuk memastikan bahwa proses pengembangannya memenuhi syarat-syarat keamanan informasi yang ditetapkan dalam kontrak.
iv. Aturan untuk pengembangan sistem harus ditetapkan dan diimplementasikan untuk proses pengembangan sistem di BPOM, mencakup setidaknya:
1) Panduan *secure coding*;
2) Pengendalian versi aplikasi;
3) Pengelolaan penyimpanan *source code*; dan
4) Metode pengujian untuk mengidentifikasi dan memperbaiki kerentanan.
v. Pengendalian perubahan pada proses pengembangan sistem informasi harus dikendalikan untuk memastikan keakuratan sistem informasi yang sedang dikembangkan.
vi. Informasi yang terlibat dalam layanan aplikasi yang melewati jaringan publik harus dilindungi dari kegiatan kecurangan, pengungkapan yang tidak sah serta kegiatan modifikasi.
vii. Apabila *platform* operasional, misalnya sistem operasi, *database* dan/atau *middleware*, dari sistem informasi BPOM mengalami perubahan, harus dilakukan peninjauan dan pengujian terhadap sistem informasi/aplikasi kritikal BPOM untuk memastikan tidak ada dampak buruk terhadap operasional dan keamanan organisasi.
viii. Perubahan terhadap sistem dalam siklus pengembangan harus dikendalikan dengan menggunakan prosedur pengendalian perubahan yang formal.
ix. Unit kerja yang melakukan pengembangan sistem informasi harus melakukan perlindungan terhadap lingkungan pengembangan sepanjang siklus pelaksanaan pengembangan sistem/*System Development Life Cylce* (SDLC) dan melakukan pengawasan dalam hal pengembangan dilakukan oleh pihak eksternal/pihak ketiga.
x. Prinsip untuk rekayasa sistem yang aman harus ditetapkan, didokumentasikan, dipelihara, dan diterapkan untuk setiap upaya implementasi sistem informasi.
xi. Unit kerja pemilik sistem informasi harus mengawasi aktivitas pengembangan sistem yang dialihdayakan (*outsourced*). Hal ini mencakup setidaknya:

1) Perjanjian terkait lisensi dan kepemilikan sistem.
2) Pengujian penerimaan sistem untuk menguji kualitas dan akurasi dari sistem.
3) Prasyarat dokumentasi untuk sistem.

xii. Unit kerja yang melakukan pengembangan sistem informasi bertanggung jawab untuk membuat perencanaan, melaksanakan pengujian aplikasi yang mencakup pendekatan/metode, alur, dan parameter pengujian. Proses pengujian sistem informasi mencakup beberapa hal sebagai berikut:
1) Menetapkan kriteria dan jadwal untuk pengujian penerimaan sistem, baik untuk pengembangan sistem informasi baru serta peningkatan (*enhancement*) dan versi baru dari sistem informasi.
2) Pengujian terhadap suatu aplikasi, dapat dilakukan secara bertingkat mulai dari *unit testing*, *System Integration Testing* (SIT), sampai dengan *User Acceptance Testing* (UAT).
3) *Unit testing* dipersiapkan dan dilakukan oleh masing-masing pengembang (*developer*) pada lingkungan pengembangan dengan mengacu kepada standar pengujian yang telah ditentukan.
4) *System Integration Testing* (SIT) dilakukan di lingkungan pengembangan/pengujian, oleh pengembang bersama dengan unit kerja pengelola TIK dan unit pemilik sistem informasi.
5) *User Acceptance Testing* (UAT) dilakukan di lingkungan pengujian di infrastruktur milik BPOM, oleh unit pemilik sistem informasi bersama dengan pengguna (*user*) terkait dan unit kerja pengelola TIK.

c. Data Pengujian
i. Data yang digunakan dalam pengujian sistem (*system test data*) harus dilindungi dari kemungkinan rusak, hilang atau perubahan yang dilakukan tanpa ijin.
ii. Data Pengujian harus dipilih dengan hati-hati, dilindungi, dan dikendalikan.
iii. Pengamanan terhadap data hasil pengujian perlu memperhatikan hal-hal 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 (*production*) yang digunakan untuk keperluan pengujian harus dihapus dari lingkungan/server pengujian segera setelah proses pengujian telah selesai dilaksanakan.

11. Pengelolaan Hubungan Dengan Pemasok (Pengendalian Pihak Ketiga (Pemasok)

a. Unit kerja melalui unit/fungsi terkait dengan pengelolaan hubungan dengan pemasok (*supplier*) harus memastikan pemasok telah menyetujui seluruh persyaratan keamanan informasi yang ditetapkan dalam perjanjian untuk mengurangi risiko yang terkait dengan akses pemasok ke dalam aset BPOM.
b. Perjanjian dengan pemasok harus meliputi persyaratan untuk mengatasi risiko keamanan informasi yang terkait dengan teknologi informasi dan komunikasi layanan serta rantai suplai produk.
c. Akses terhadap aset informasi di lingkungan BPOM harus dikendalikan secara ketat. Sebelum memberikan akses kepada penyedia produk/jasa, harus dilakukan identifikasi dan evaluasi risiko-risiko yang mungkin

terjadi sehubungan dengan pemberian akses dan menerapkan kontrol yang memadai untuk mengurangi dampak atau mencegah terjadinya risiko-risiko tersebut.

d. Unit kerja melalui unit/fungsi terkait dengan pengelolaan hubungan dengan pemasok (*supplier*) harus melakukan pemantauan dan peninjauan secara berkala terhadap kinerja layanan dari pemasok serta memastikan setiap perubahan terhadap layanan dari pemasok telah dikelola dan dikendalikan.
e. Unit kerja harus secara teratur memonitor, mereviu, dan melakukan audit terhadap kinerja pelayanan yang diberikan pemasok setidaknya 1 (satu) kali dalam setahun.
f. Perubahan terhadap penyediaan layanan oleh pemasok harus dikelola, dengan mempertimbangkan kritikalitas dari informasi bisnis, sistem, dan proses yang terlibat serta kajian risiko.
g. Dalam perjanjian kontrak dengan pemasok harus dicantumkan antara lain:
    i. Kewajiban Penyedia Produk/Jasa untuk mematuhi kebijakan keamanan informasi yang berlaku di BPOM.
    ii. Persetujuan untuk turut melindungi keamanan aset informasi BPOM terkait dengan akses yang diberikan.
    iii. Jenis akses yang diberikan dan tata cara penggunaan akses tersebut dan mekanisme pemantauannya.
    iv. Identitas dari pegawai Penyedia Produk/Jasa yang menggunakan akses ini.
    v. Pembatasan lokasi darimana akses dapat dilakukan dan waktu penggunaan akses.

12. Pengelolaan Gangguan Keamanan Informasi (Pegelolaan Insiden Keamanan Informasi)

a. Unit kerja pengelola TIK menyusun dan menetapkan ketentuan terkait dengan pengelolaan gangguan keamanan informasi.
b. Unit kerja memastikan bahwa setiap kelemahan keamanan informasi dan kejadian keamanan informasi dalam sistem atau layanan TIK harus dilaporkan dan ditindaklanjuti secepat mungkin sesuai mekanisme yang berlaku dan terdokumentasi.
c. Unit kerja harus memastikan pengelolaan dan penanganan gangguan keamanan informasi dilakukan sesuai dengan prosedur.
d. Tindakan untuk memulihkan keamanan dari pelanggaran dan perbaikan kegagalan sistem harus dikendalikan secara hati-hati dan formal.
e. Unit kerja pengelola TIK atau unit/fungsi terkait dengan pengelolaan gangguan keamanan informasi mendokumentasikan seluruh gangguan keamanan informasi yang terjadi beserta tindakan perbaikannya untuk digunakan sebagai basis pengetahuan agar dapat mengurangi peluang atau dampak gangguan dimasa mendatang.
f. Seluruh gangguan keamanan informasi yang terjadi dan tindakan mengatasinya harus dicatat/didokumentasikan dalam pelaporan gangguan keamanan informasi, dan akan menjadi masukan pada proses peningkatan penanganan gangguan keamanan informasi.
g. Pengetahuan yang diperoleh dari proses analisis dan penyelesaian masalah insiden keamanan informasi digunakan untuk mengurangi kemungkinan atau dampak dari insiden di masa depan.
h. BPOM harus mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap kebijakan dan standar pengelolaan keamanan informasi BPOM.

13. 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.

a. Perencanaan Kelangsungan Keamanan Informasi

i. BPOM mengembangkan suatu Kebijakan Pengelolaan Kelangsungan Kegiatan sistem informasi BPOM untuk mengurangi dampak kegagalan sistem informasi atau bencana yang menyebabkan terganggunya kegiatan BPOM.

ii. 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.

iii. Unit kerja harus menetapkan prasyarat untuk keberlanjutan keamanan informasi dan diintegrasikan dengan prasyarat keberlanjutan bisnis organisasi untuk menjamin keberlanjutan dari keamanan informasi di BPOM, pada saat, dan setelah terjadinya gangguan besar atau bencana.

iv. 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.

v. Tim Pengelola Keamanan Informasi BPOM mengelola DRP dan salinannya serta informasi lain yang diperlukan dalam penanganan *disaster* di lokasi yang aman dan mudah dijangkau.

vi. BPOM menerapkan strategi *recovery* layanan BPOM 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.

vii. Pelaksanaan Rencana Keberlangsunan Keamanan Informasi
   1) Untuk menjamin agar Pengelolaan Kelangsungan Sistem BPOM tetap relevan dan efektif, Pengelolaan Kelangsungan Sistem BPOM harus diuji secara periodik. Hasil-hasil pengujian Pengelolaan Kelangsungan Sistem BPOM dan tindakan-tindakan lanjutan yang perlu diambil dilaporkan ke Kepala BPOM.
   2) Pengelolaan Kelangsungan sistem BPOM harus dilaksanakan untuk menjamin tetap beroperasinya BPOM pada keadaan darurat sesuai dengan kebutuhan dan jangka waktu yang ditetapkan.

3) Penanggulangan keadaan darurat secara langsung ditangani oleh Tim Pengelola Keamanan Informasi yang keanggotaannya disesuaikan setiap satu tahun sekali.
4) Unit kerja yang dalam pelaksanaan tugas dan fungsinya mengandalkan layanan Pusat Data Nasional Sementara (PDNs) Kominfo harus mempersiapkan prosedur kerja alternatif sesuai dengan ketentuan yang berlaku untuk mengurangi gangguan operasional pada saat terjadi keadaan darurat.
5) Tim Pengelolaan BCP Keamanan Informasi BPOM memastikan kesiapan dan keahlian pegawai serta pihak terkait lainnya dalam menghadapi keadaan darurat dengan melaksanakan pelatihan secara berkala.

viii. Verifikasi, Reviu, dan Evaluasi Keberlangsunan Keamanan Informasi
1) 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.
2) BPOM menerapkan dua metode uji coba yaitu:
   a) Uji fungsi (*functional testing*) untuk memastikan bagian-bagian dari *Disaster Recovery Plan* berfungsi sebagaimana mestinya. Uji fungsi dilaksanakan secara periodik.
   b) 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.
3) Pelaksanaan uji coba harus memperhatikan hal-hal berikut:
   a) Kesesuaian dengan kebutuhan.
   b) Kemungkinan timbulnya dampak negatif.
   c) Waktu dan lama pelaksanaan.
   d) Kebutuhan sumberdaya dan biaya.
   e) Kesiapan pelaksanaan.
   f) Ketergantungan dengan pihak ketiga.
   g) Secara formal mendapat persetujuan Kepala BPOM.
4) 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*.
5) Seluruh proses, prosedur, dan petunjuk pelaksanaan Pengelolaan Kelangsungan sistem BPOM dan *Disaster Recovery Plan* harus terdokumentasi dengan baik dan senantiasa diperbaharui sesuai dengan kebutuhan.
6) Tim Pengelola BCP harus melakukan *review* terhadap akurasi proses, prosedur, dan petunjuk pelaksanaan secara berkala minimal 1 kali dalam 1 tahun.

ix. Redundansi
1) Aspek redundansi harus ditetapkan untuk fasilitas pengolahan informasi dan sarana pendukungnya untuk memastikan ketersediaan dari proses bisnis dan operasional BPOM serta pemberian layanan BPOM.

2) Fasilitas pengolahan informasi beserta sarana pendukungnya yang telah memenuhi aspek redundansi harus diuji secara berkala untuk menjamin kesesuaian dari fungsinya.
3) 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*.
4) Tim Pengelola Keamanan Informasi Data *Center* BPOM mengupayakan tersedianya sarana *Disaster Recovery* yang paling tepat untuk memastikan ketersediaan layanan Data *Center* BPOM utama dalam keadaan darurat sesuai tingkat kritikalitas proses bisnis terkait.
5) Ketentuan dalam pengelolaan terkait *Backup Site* meliputi:
   a) Lokasi *Backup Site* secara geografis memiliki probabilitas kejadian bencana alam yang minimal.
   b) *Backup Site* ditujukan sebagai media penyimpanan backup alternatif serta sebagai fasilitas pengolahan informasi alternatif.
   c) Terpenuhinya pemulihan layanan operasional sepenuhnya pada fasilitas *Backup Site* sesuai kerangka parameter RTO (*Recovery Time Objective).*
   d) 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.
      iii. DRC harus berada di lokasi yang memiliki profil risiko berbeda dengan Data Center dan harus berada di wilayah geografis Republik Indonesia.

14. Kepatuhan

a. Kepatuhan Terhadap Persyaratan Hukum dan Kontrak
   i. Unit kerja pengelola TIK, berkoordinasi dengan unit/fungsi terkait hukum/legal, harus mengidentifikasi, mendokumentasikan dan memelihara kemutakhiran seluruh persyaratan peraturan perundang-undangan dan kontrak terkait dengan keamanan informasi.
   ii. Seluruh pengguna, baik internal BPOM maupun pihak ketiga, harus memastikan pemenuhan kepatuhan terhadap peraturan perundang-undangan dan/atau persyaratan kontrak, hak atas kekayaan intelektual, dan penggunaan materi berlisensi.
   iii. Unit kerja pengelola TIK bertanggung jawab atas penerapan pengendalian keamanan informasi sesuai standar teknis dan prosedur keamanan informasi rangka kepatuhan terhadap perjanjian dan peraturan perundang undangan yang mencakup:
      a) keamanan data dan informasi
         penerapan keamanan data dan informasi dilakukan dengan memastikan terpenuhinya aspek-aspek kerahasiaan, keaslian, keutuhan, kenirsangkalan, dan ketersediaan.data dan informasi BPOM, yaitu:

1) pemenuhan aspek kerahasian melalui penetapan dan penerapan klasifikasi informasi, penerapan enkripsi dengan sistem kriptografi, serta pembatasan akses data dan informasi sesuai kewenangan dan kebijakan yang ditetapkan.
2) pemenuhan aspek keaslian melalui penyediaan mekanisme verifikasi, mekanisme validasi, dan penerapan sistem *hash function*.
3) pemenuhan aspek keutuhan melalui penerapan deteksi modifikasi dan penerapan tanda tangan elektronik.
4) pemenuhan aspek kenirsangkalan melalui penerapan tanda tangan elektronik tersertifikasi dan penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik
5) pemenuhan aspek ketersediaan melalui penerapan sistem pencadangan secara berkala, penerapan perencanaan untuk memastikan data dan informasi selalu dapat diakses, serta penerapan sistem pemulihan.

b) keamanan Aplikasi SPBE
penerapan keamanan Aplikasi SPBE dilakukan dengan memastikan pengamanan aplikasi berbasis web dan aplikasi berbasis *mobile,* serta pelaksanaan pengujian keamanan aplikasi setiap periode waktu tertentu.
1) pengamanan aplikasi berbasis web dilaksanakan dengan memastikan terpenuhinya fungsi-fungsi autentikasi, manajemen sesi, persyaratan kontrol akses, validasi input, kriptografi pada verifikasi statis, penanganan eror dan pencatatan log, proteksi data, keamanan komunikasi, pengendalian kode berbahaya, logika bisnis, file, keamanan API dan web service, serta keamanan konfigurasi.
2) pengamanan aplikasi berbasis *mobile* dilaksanakan dengan memastikan terpenuhinya fungsi-fungsi penyimpanan data dan persyaratan privasi, kriptografi, autentikasi dan manajemen sesi, komunikasi jaringan, interaksi platform, kualitas kode dan pengaturan *build*; dan ketahanan.
3) pengujian keamanan aplikasi yang dilakukan dengan mengidentifikasi persyaratan minimum keamanan yang belum diterapkan, memastikan pengkodean pemrograman aplikasi yang dibuat tidak memiliki kerawanan, melakukan pemindaian otomatis dan/atau pengujian penetrasi sistem, mengidentifikasi kerentanan dan mengelola ancaman sejak awal siklus pengembangan Aplikasi SPBE, serta menganalisis kerentanan keamanan Aplikasi SPBE.

c) keamanan Sistem Penghubung Layanan
penerapan keamanan Sistem Penghubung Layanan dilakukan dengan memastikan terpenuhinya fungsi-fungsi keamanan interoperabilitas data dan informasi, kontrol sistem integrasi, kontrol perangkat integrator, keamanan API dan web service, serta keamanan migrasi data

d) keamanan Jaringan Intra
penerapan keamanan Jaringan Intra dilakukan dengan memastikan terpenuhinya aspek administrasi keamanan Jaringan Intra, kontrol akses dan autentikasi, persyaratan perangkat dan aplikasi keamanan Jaringan Intra, kontrol keamanan *gateway*, kontrol keamanan access point pada

jaringan nirkabel, serta kontrol konfigurasi *access point* pada jaringan nirkabel.

e) keamanan penggunaan Pusat Data Nasional
penerapan keamanan penggunaan Pusat Data Nasional dilakukan dengan memastikan seluruh Aplikasi SPBE BPOM yang diimplementasikan di Pusat Data Nasional telah dilakukan pengujian keamanan secara memadai, serta terpenuhinya persyaratan keamanan perangkat yang terkoneksi ke Pusat Data Nasional.

iv. Rekaman milik BPOM harus dilindungi dari kehilangan, kerusakan, pemalsuan, akses yang tidak sah, dan rilis yang tidak sah.

v. Privasi dan perlindungan terhadap informasi identitas pribadi harus dipastikan sebagaimana dipersyaratkan dalam peraturan perundang-undangan yang berlaku. Kepemilikan dan kerahasiaan data pribadi yang terdapat pada sistem informasi harus dijaga dan dilindungi secara memadai, data pribadi hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan dan ketentuan perundang-undangan.

b. Peninjauan Keamanan Informasi

i. Penerapan dan pengelolaan keamanan informasi di BPOM harus ditinjau (*review*) secara mandiri atau oleh pihak independen dalam selang waktu yang direncanakan dan/atau ketika terdapat perubahan yang signifikan.

ii. Unit kerja pengelola TIK bertanggung jawab terkait proses peninjauan terhadap sistem dan teknologi informasi terkait kepatuhan teknis secara berkala.

BAB III
PENUTUP

Dengan disusunnya Kebijakan Keamanan Informasi BPOM diharapkan dapat meningkatkan kesadaran seluruh pegawai di lingkungan BPOM bahwa aset data dan informasi sangat penting serta menjadi acuan dalam pengamanan data dan informasi.

Pengaturan yang lebih teknis dalam bentuk pedoman, panduan, standar teknis, dan/atau prosedur kerja dikoordinasikan oleh Unit kerja pengelola TIK BPOM dan menjadi bagian yang tidak terpisahkan dari Keputusan Kepala Badan ini.

PLT. KEPALA BADAN PENGAWAS OBAT DAN MAKANAN,

LUCIA RIZKA ANDALUSIA