LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH

SALINAN

KEPUTUSAN

KEPALA LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH

REPUBLIK INDONESIA

NOMOR 372 TAHUN 2023

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH

KEPALA LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH,

Menimbang : a. bahwa untuk menindaklanjuti ketentuan Pasal 48 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik dan Pasal 3 Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE, perlu Menyusun pedoman dalam melaksanakan serangkaian proses manjemen keamanan informasi;

b. bahwa untuk menjamin keamanan informasi di lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah, perlu melaksanakan manjemen keamanan informasi dalam rangka menjamin kerahasiaan, keutuhan, ketersediaan, keaslian dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan informasi, infrastruktur SPBE, dan Aplikasi SPBE;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Kepala Lembaga Kebijakan Pengadaan

Barang/Jasa Pemerintah tentang Sistem Manajemen Keamanan Informasi di lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah.

Mengingat : 1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
2. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 1375);
3. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan standar Teknis dan Prosedur Keamanan SPBE (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
4. Peraturan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah Nomor 2 Tahun 2023 tentang Organisasi dan Tata Kerja Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah (Berita Negara Republik Indonesia Tahun 2023 Nomor 112);

MEMUTUSKAN:

Menetapkan : KEPUTUSAN KEPALA LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH.

KESATU : Menetapkan Sistem Manajemen Keamanan Informasi di Lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan ini.

KEDUA : Pedoman Sistem Manajemen Keamanan Informasi di Lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah bertujuan untuk memberikan pedoman dalam implementasi keamanan dan informasi serta sebagai petunjuk tentang langkah-langkah yang akan diambil untuk membangun, mengelola serta mempertahankan keamanan informasi serta efektif di lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah.

KETIGA : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 20 November 2023
KEPALA LEMBAGA KEBIJAKAN
PENGADAAN BARANG/JASA
PEMERINTAH,

ttd

HENDRAR PRIHADI

Salinan sesuai dengan aslinya
Kepala Biro Hukum, Organisasi dan
Sumber Daya Manusia LKPP,

Suharti

LAMPIRAN : KEPUTUSAN KEPALA LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH.

NOMOR : 372 TAHUN 2023

TANGGAL : 20 NOVEMBER 2023

BAB I
PENDAHULUAN

A. Latar belakang

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE telah mendorong transformasi layanan pemerintahan dari semula dilakukan secara manual menjadi berbasis digital. Transformasi layanan berbasis digital menawarkan berbagai keuntungan antara lain efisiensi, efektifitas, dan akuntabilitas yang tinggi. Namun demikian, transformasi layanan berbasis digital juga menimbulkan risiko baru yaitu munculnya kerentanan dan potensi ancaman terhadap kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan informasi yang dikelola yang diakibatkan oleh berbagai gangguan terhadap sistem yang dimiliki termasuk serangan dan insiden siber.

Keamanan informasi merupakan hal penting yang harus diperhatikan dalam membangun dan menjalankan layanan berbasis digital. Dengan semakin meningkatnya risiko dan insiden siber dalam penyelenggaraan SPBE, maka upaya pengamanan terhadap SPBE harus dilakukan. Data pribadi, infrastruktur, dan aset lainnya yang dimiliki oleh Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah harus dapat dikelola dengan baik. Dalam rangka memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan dalam pengelolaan informasi di lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah, diperlukan Sistem Manajemen Keamanan Informasi.

Kebijakan Sistem Manajemen Keamanan Informasi disusun sebagai pedoman bagi setiap personel yang terlibat dalam pengelolaan informasi untuk memastikan terjaganya keamanan informasi. Pedoman ini mengatur proses pengelolaan pengamanan informasi maupun kendali yang diperlukan dalam melakukan pengamanan informasi. Pedoman ini menjadi acuan dalam penyusunan prosedur, petunjuk teknis maupun aturan yang lainnya dalam rangka pengamanan informasi di Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah.

B. Tujuan

Kebijakan Sistem Manajemen Keamanan Informasi ini digunakan sebagai pedoman dalam rangka melindungi aset informasi Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah (LKPP) dari berbagai bentuk ancaman baik internal maupun eksternal, yang dilakukan secara sengaja maupun tidak sengaja. Pengamanan dan perlindungan ini diberikan untuk menjamin kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian (*authentication*), dan kenirsangkalan (*non-repudiation*) aset informasi selalu terjaga dan terpelihara dengan baik.

C. Ruang Lingkup

Kebijakan dan standar ini berlaku untuk pengelolaan pengamanan seluruh aset informasi di lingkungan LKPP yang dilaksanakan oleh setiap unit kerja yang terlibat baik sebagai pengguna atau pengelola, instansi pemerintah terkait, mitra kerja, dan pihak ketiga di lingkungan LKPP. Cakupan aset informasi meliputi:

1. Data dan Informasi;
2. Aplikasi;
3. Infrastruktur; dan
4. Sumber Daya Manusia.

D. Ketentuan Umum

1. Akun adalah identifikasi pengguna yang diberikan oleh unit Pengelola TIK, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem TIK.

2. Akun yang Unik adalah akun yang diberikan oleh unit Pengelola TIK sesuai kebutuhan tetapi tidak terbatas pada pengelolaan TIK (baik berupa aplikasi atau sistem), dan kelompok kerja (baik berupa acara kedinasan, tim, atau unit kerja).
3. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan.
4. Audit Eksternal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi eksternal Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah yang memiliki sertifikasi sebagai Auditor Keamanan Informasi.
5. Audit Internal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi internal Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah.
6. Audit Keamanan Informasi adalah Audit TIK cakupan keamanan informasi.
7. Auditor Keamanan Informasi adalah orang yang memiliki kompetensi untuk melakukan Audit Keamanan Informasi.
8. Audit *logging* adalah catatan mengenai perubahan data dalam aplikasi, yang dicatat biasanya kolom mana yang berubah, siapa yang mengubah, diubah dari apa menjadi apa, dan kapan berubah.
9. Audit TIK adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.
10. *Backup* adalah sebuah proses pembuatan gandaan/duplikat/ cadangan dari aset informasi yang dilakukan sebagai upaya pengamanan dan pemulihan sebagai bagian dari manajemen risiko.
11. Data adalah tulisan, suara, gambar, peta, rancangan, foto, video, *electronic data interchange* (EDI), *source code*, log, surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, atau simbol.
12. Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau

dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.

13. Daftar inventaris aset informasi adalah kumpulan informasi yang memuat bentuk, pemilik, lokasi, retensi, dan hal-hal yang terkait dengan aset informasi.
14. Hak akses khusus adalah akses terhadap sistem informasi sensitif, termasuk di dalamnya dan tidak terbatas pada sistem operasi, perangkat penyimpanan, *file server*, dan aplikasi-aplikasi sensitif. Hanya diberikan kepada pengguna yang membutuhkan, pemakainnya terbatas dan dikontrol.
15. Informasi Elektronik adalah satu atau sekumpulan Data Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *eletronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
16. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
17. Insiden siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam keamanan informasi antara lain namun tidak terbatas pada *web defacement, malware* (*virus, worm, trojan backdoor dan ransomware*), *unauthorized access*, *data breach*, dan *Distributed Denial of Service* (DDoS).
18. Kata sandi adalah serangkaian kode yang dibuat Pengguna, bersifat rahasia dan pribadi yang digunakan bersamaan dengan Akun Pengguna.
19. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan informasi.
20. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
21. Kriptografi adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal

untuk meningkatkan keamanan informasi. Dalam kriptografi terdapat dua prinsip yaitu enkripsi dan dekripsi.

22. Manajemen Risiko adalah aktivitas terkoordinasi untuk identifikasi, penilaian, dan penentuan prioritas risiko yang kemudian akan dikelola, dipantau, dan dikontrol untuk mengurangi dampak dan/atau kemungkinan terjadinya risiko tersebut.
23. Organisasi Keamanan Informasi Di Lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah merupakan unit kerja yang dibentuk melalui keputusan Kepala Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah untuk melaksanakan tugas dan fungsi Sistem Manajemen Keamanan Informasi.
24. Pihak ketiga adalah semua unsur di luar pengguna unit TIK Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah yang bukan bagian dari Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah, misal mitra kerja Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah (seperti: konsultan, penyedia jasa komunikasi, pemasok dan pemelihara perangkat pengolah informasi), dan kementerian/lembaga lain.
25. Pemilik Aset Informasi adalah unit kerja yang memiliki kewenangan terhadap aset informasi.
26. Pengguna adalah pegawai Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah dan atau pihak ketiga serta tidak terbatas pada pengelola TIK dan kelompok kerja yang diberikan hak mengakses sistem TIK di lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah.
27. Perjanjian Kerahasiaan adalah perikatan antara para pihak yang mencantumkan bahan rahasia, pengetahuan, atau informasi yang mana pihak-pihak ingin berbagi satu sama lain untuk tujuan tertentu, tetapi ingin membatasi akses dengan pihak lain.
28. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
29. Risiko adalah kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negatif terhadap pencapaian sasaran kinerja dari layanan Sistem Elektronik.
30. *Risk Treatment Plan* (RTP) atau Rencana Tindak Lanjut (RTL) Risiko adalah respon yang direncanakan manajemen untuk menindaklanjuti

hasil evaluasi risiko, seperti *mitigate/reduce*, *avoid*, *share/ transfer* atau *accept*.

31. Sanitasi adalah proses penghilangan informasi yang disimpan secara permanen dengan menggunakan medan magnet besar atau perusakan fisik.
32. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.
33. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
34. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan keamanan informasi berdasarkan pendekatan risiko.
35. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
36. Teknologi Informasi dan Komunikasi selanjutnya disebut TIK adalah terminologi yang mencakup seluruh peralatan teknis untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
37. Tim Respon Insiden Keamanan Komputer adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.

E. Dasar Hukum

Dasar hukum yang digunakan dalam pembuatan SMKI ini adalah:

1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

2. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 1375);
3. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan standar Teknis dan Prosedur Keamanan SPBE (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
4. Peraturan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah Nomor 2 Tahun 2023 tentang Organisasi dan Tata Kerja Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah (Berita Negara Republik Indonesia Tahun 2023 Nomor 112);

BAB II
ORGANISASI KEAMANAN INFORMASI

A. Umum

LKPP menetapkan, menerapkan, memelihara, dan memperbaiki secara berkelanjutan. SMKI dijalankan melalui organisasi keamanan informasi yang peran dan tanggung jawabnya ditetapkan melalui pedoman ini.

B. Peran

1. Sekretaris Utama berperan sebagai Koordinator SPBE.
2. Sekretaris Utama dalam menjalankan tugasnya sebagai Koordinator SPBE dibantu oleh Tim SMKI selaku Pelaksana Teknis keamanan informasi.
3. Sekretaris Utama bersama dengan Tim SMKI menjalankan pengelolaan keamanan informasi di lingkungan LKPP.
4. Inspektur berperan melaksanakan audit internal keamanan informasi di lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah untuk memastikan pengendalian, proses dan prosedur SMKI dilaksanakan secara efektif dan dipelihara dengan baik.
5. Kapusdatin berperan sebagai Ketua Tim SMKI yang memiliki kewenangan dalam menentukan komposisi, kualifikasi dan jumlah anggota tim.
6. Tim SMKI ditetapkan oleh Kepala LKPP.

C. Tanggung Jawab

1. Sekretaris Utama bertanggung jawab untuk:
   a. memastikan pelaksanaan Kebijakan SMKI;
   b. menyediakan sumber daya yang memadai untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan SMKI Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah;
   c. menetapkan kriteria penerimaan risiko dan tingkat risiko yang dapat diterima;
   d. memastikan pelaksanaan audit internal SMKI;

e. menetapkan arsitektur keamanan informasi;
f. menetapkan peta rencana 5 (lima) tahunan dan sasaran keamanan informasi setiap tahunnya;
g. melakukan tinjauan secara berkala atas pelaksanaan kebijakan SMKI; dan
h. menyampaikan kinerja pelaksanaan kebijakan SMKI kepada Kepala Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah.

2. Inspektur bertanggung jawab untuk:
a. menyusun pedoman dan perencanaan audit internal keamanan informasi;
b. melaksanakan kegiatan audit internal keamanan informasi;
c. memberikan rekomendasi perbaikan atas hasil temuan audit internal keamanan informasi;
d. menyusun laporan audit internal keamanan informasi; dan
e. menyampaikan laporan audit internal keamanan informasi kepada Sekretaris Utama.

3. Tim SMKI bertanggung jawab untuk:
a. menyusun, mengkomunikasikan, dan memantau pelaksanaan kebijakan SMKI di lingkungan LKPP;
b. melakukan analisis kebutuhan keamanan informasi, yang mencakup:
1) mengidentifikasi aplikasi dan infrastruktur untuk keamanan informasi;
2) mengidentifikasi standar kompetensi personel keamanan informasi; dan
3) mengidentifikasi program peningkatan kompetensi keamanan informasi dan penanggulangan insiden siber;
c. merumuskan, mengkoordinasikan, dan melaksanakan program kerja dan anggaran keamanan informasi;
d. memastikan seluruh pembangunan/pengembangan aplikasi dan infrastruktur informasi termasuk yang dilakukan oleh Pihak Ketiga, minimal memenuhi Standar Teknis dan Prosedur Keamanan Informasi

yang ditetapkan oleh Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber;

e. memastikan peningkatan kesadaran, kepedulian, dan kepatuhan oleh seluruh pegawai terhadap kebijakan, prosedur, dan standar keamanan informasi dapat berjalan dengan efektif;
f. memastikan diterapkannya perjanjian menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen perjanjian kerahasiaan (*Non Disclosure Agreement*);
g. mengendalikan dan menjaga kemutakhiran kebijakan, prosedur, dan standar keamanan informasi;
h. memfasilitasi pelaksanaan audit internal dan audit eksternal keamanan informasi. Dalam memfasilitasi pelaksanaan audit internal keamanan informasi, Tim SMKI dapat menunjuk pihak yang berkompeten di bidang audit keamanan informasi sebagai konsultan;
i. memastikan diterapkannya manajemen risiko, manajemen insiden siber, dan manajemen aset dalam pelaksanaan pengamanan aset Informasi;
j. mendorong perbaikan penerapan keamanan informasi berdasarkan hasil temuan audit internal dan audit eksternal; dan
k. membuat laporan evaluasi penerapan Kebijakan SMKI dan menyampaikannya kepada Sekretaris Utama.

BAB III
PERENCANAAN KEAMANAN INFORMASI

A. Kategorisasi Sistem Elektronik

LKPP sebagai penyelenggara SPBE yang merupakan Sistem Elektronik Lingkup Publik melakukan kategorisasi pada sistem elektronik yang dimiliki. Sebagai salah satu dasar dalam pelaksanaan keamanan informasi, penentuan kategorisasi sistem elektronik dilakukan sesuai dengan peraturan perundangan yang ditetapkan oleh Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

B. Manajemen Risiko

Pelaksanaan keamanan informasi dilakukan dengan memperhatikan berbagai risiko yang dapat mengakibatkan terjadinya kegagalan keamanan informasi di lingkungan LKPP. Oleh karenanya, dalam perencanaan keamanan informasi, Tim SMKI melakukan manajemen risiko keamanan informasi, yang terdiri dari:

1. penilaian risiko keamanan informasi dengan mengindentifikasi ancaman, kerentanan, peluang, dan dampak apabila risiko terjadi.
2. bersama dengan unit terkait, menyusun Rencana Tindak Lanjut (RTL).
3. melakukan sosialisasi dan komunikasi RTL pada para pemilik risiko.
4. proses manajemen risiko dilakukan secara berkala paling sedikit setiap 1 (satu) tahun sekali atau jika ada perubahan aset atau proses bisnis yang berdampak tinggi terhadap profil risiko yang ada saat ini.

C. Perencanaan Keamanan Informasi

Tim SMKI menyusun program kerja keamanan informasi berdasarkan Rencana Tindak Lanjut (RTL) sebagai wujud realisasi atas risiko keamanan informasi. Program kerja keamanan informasi dituangkan ke dalam peta rencana 5 (lima) tahunan dan sasaran keamanan informasi setiap tahun.

Dalam menyusun perencanaan Keamanan Informasi, TIM SMKI setidaknya melaksanakan setiap program kerja keamanan informasi paling sedikit meliputi:

1. edukasi kesadaran keamanan informasi.
2. penilaian kerentanan keamanan informasi.
3. peningkatan keamanan informasi.
4. penanganan insiden siber.
5. audit keamanan informasi.

BAB IV
DUKUNGAN PENGOPERASIAN

Dukungan Pengoperasian meliputi:

1. Sekretaris Utama memberikan dukungan pengoperasian keamanan informasi dengan menyediakan personel keamanan informasi yang berkompeten dan anggaran keamanan informasi;
2. Sekretaris Utama menyediakan anggaran keamanan informasi berdasarkan arsitektur dan peta rencana keamanan informasi yang telah disusun;
3. Personel keamanan informasi yang disediakan harus memiliki kompetensi:
   a. Keamanan Infrastruktur TIK; dan
   b. Keamanan Aplikasi.
4. Dalam hal personel keamanan informasi yang disediakan belum memiliki kompetensi memadai, maka Sekretaris Utama memfasilitasi peningkatan kompetensi melalui kegiatan pelatihan dan/atau bimbingan teknis; dan
5. Anggaran keamanan informasi dibebankan pada Anggaran Pendapatan dan Belanja Negara atau sumber lainnya yang sah dan tidak mengikat.

BAB V
KEAMANAN PERSONEL

Keamanan personel dilakukan untuk mengendalikan personel dalam melaksanakan Kebijakan SMKI. Keamanan personel di lingkungan LKPP dilaksanakan oleh Tim SMKI bekerja sama dengan Unit Organisasi terkait namun tidak terbatas, dengan metode sebagai berikut:

1. Saling komunikasi dan berkoordinasi terhadap peran dan tanggung jawab pelaksanaan Kebijakan SMKI kepada seluruh pegawai dan pihak ketiga yang terlibat dalam pengelolaan dan pengamanan aset informasi;
2. melakukan pembagian tugas dan wewenang (*segregation of duty*) untuk menghindari kesalahan atau pelanggaran;
3. melakukan pemeriksaan data pribadi pegawai dan pihak ketiga yang terlibat dalam pengelolaan dan pengamanan aset informasi secara berkala;
4. membuat perjanjian tertulis dengan pegawai dan pihak ketiga yang terlibat dalam penggunaan dan/atau pengelolaan informasi yang menyatakan tanggung jawab terhadap keamanan informasi dan sanksi atas pelanggaran keamanan informasi;
5. menghentikan hak penggunaan aset informasi bagi pegawai yang sedang dalam pemeriksaan terkait dengan dugaan pelanggaran keamanan informasi;
6. mencabut hak akses ke aset informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi memiliki kepentingan terhadap aset informasi, dimutasi atau tidak lagi bekerja di lingkungan LKPP;
7. membuat berita acara serah terima terkait penerimaan seluruh aset informasi yang digunakan selama bekerja dan pengembalian seluruh aset informasi bagi pegawai yang berhenti bekerja atau mutasi;
8. memberikan edukasi kesadaran keamanan informasi melalui kegiatan sosialisasi, bimbingan teknis, dan/atau pelatihan mengenai keamanan informasi yang dilaksanakan secara berkala; dan
9. memelihara catatan pelatihan, kompetensi, pengalaman, dan kualifikasi pegawai yang mengelola keamanan informasi.

BAB VI
KEAMANAN ASET

Keamanan aset dilakukan untuk mengamankan aset informasi di lingkungan LKPP berdasarkan tingkat kritikalitasnya. Keamanan aset informasi di lingkungan LKPP dilakukan oleh Tim SMKI bekerja sama dengan unit organisasi terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. mengidentifikasi aset informasi dan melakukan dokumentasi ke dalam daftar inventaris aset informasi minimal memuat tingkat kritikalitas dan penanggung jawab setiap aset informasi.
2. memberikan label sesuai tingkat insiden siber.
3. menetapkan pihak-pihak yang dapat mengakses aset informasi.
4. menetapkan aturan penggunaan aset informasi.
5. menempatkan aset informasi di lokasi yang aman guna mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang.
6. penggunaan aset informasi yang dibawa ke luar dari lingkungan Pusat Data atau tempat layanan informasi harus disetujui oleh Kepala Pusat Data dan Informasi LKPP.
7. perangkat penyimpanan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dimusnahkan.
8. pemusnahan perangkat penyimpanan data harus dilakukan secara aman sesuai prosedur pemusnahan perangkat penyimpanan.
9. melaksanakan manajemen aset TIK sesuai dengan ketentuan manajemen aset TIK yang ditetapkan oleh Kementerian yang melaksanakan tugas di bidang Komunikasi dan Informatika.

BAB VII
KEAMANAN AKSES

Keamanan akses dilakukan untuk mengendalikan akses ke aset informasi yaitu memastikan perangkat pengguna yang terhubung ke aset informasi mendapatkan perlindungan keamanan dan tidak diakses oleh pihak yang tidak berhak. Keamanan akses terhadap aset informasi di lingkungan LKPP dilakukan oleh Tim SMKI bekerja sama dengan unit organisasi terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. menyusun prosedur pengelolaan hak akses pengguna yang berisi ketentuan akses ke aset informasi sesuai dengan kebutuhan organisasi, persyaratan keamanan, dan peraturan yang berlaku.
2. mengelola akses pengguna dengan cara:
   a. menggunakan akun yang unik untuk setiap pengguna;
   b. memeriksa tingkat akses yang diberikan sesuai dengan tujuan penggunaan;
   c. membatasi dan mengendalikan penggunaan hak akses khusus (jika ada);
   d. mengatur pengelolaan kata sandi pengguna sesuai dengan ketentuan pengelolaan kata sandi di lingkungan LKPP;
   e. memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya;
   f. memelihara catatan pengguna layanan (*user log*);
   g. menonaktifkan akses pengguna yang telah berakhir penugasannya; dan
   h. memantau dan mengevaluasi akun dan hak akses secara berkala minimal setiap 6 (enam) bulan.
3. mengendalikan akses ke jaringan dan layanan jaringan informasi dengan cara:
   a. menerapkan prosedur otorisasi pemberian akses ke jaringan dan layanan jaringan untuk setiap akses ke dalam jaringan internal;
   b. akses ke infrastruktur dan aplikasi yang digunakan untuk melakukan analisis harus dikontrol dan hanya digunakan untuk pegawai yang bertugas untuk melakukan pengujian, pemecahan masalah, serta pengembangan sistem;

c. memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi;
d. memberikan akses jaringan kepada tamu hanya untuk akses terbatas dan waktu tertentu; dan
e. melakukan penghentian layanan jaringan pada area jaringan yang mengalami gangguan keamanan informasi.

4. mengendalikan akses ke aplikasi dan sistem informasi dengan cara:
   a. akses terhadap aplikasi dan sistem informasi hanya diberikan kepada pengguna sesuai dengan peruntukannya dan dikontrol dengan menggunakan sistem manajemen akses pengguna;
   b. setiap pengguna wajib memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya dan proses otorisasi pengguna wajib menggunakan teknik otentikasi yang sesuai untuk memvalidasi identitas pengguna;
   c. menggunakan sistem pengelolaan kata sandi sesuai dengan Ketentuan Pengelolaan Kata sandi di lingkungan LKPP untuk memastikan kualitas kata sandi yang dibuat pengguna;
   d. fasilitas *session time-out* wajib diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu;
   e. membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia; dan
   f. akses ke kode sumber aplikasi dibatasi secara ketat diperuntukkan hanya bagi pihak-pihak yang sah dan berkepentingan melalui hak akses khusus.
5. mengendalikan perangkat kerja jarak jauh dengan cara menentukan parameter-parameter keamanan yang harus dipenuhi oleh perangkat kerja jarak jauh yang digunakan dalam mengakses aset informasi namun tidak terbatas terdiri atas:
   a. *Virtual Private Network* (VPN);
   b. *Secure Socket Layer* (SSL); dan/atau
   c. *Two Step Authentication*;

6. hak akses khusus dapat dibuat untuk mengakses sistem informasi berklasifikasi rahasia pada sistem operasi, perangkat penyimpanan (*storage devices*), *file server*, dan aplikasi sensitif, dengan cara:
   a. mengidentifikasi hak akses khusus untuk dialokasikan kepada pengguna terkait;
   b. memberikan hak akses khusus hanya kepada pengguna sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu;
   c. mengelola proses otorisasi dan catatan dari seluruh hak akses khusus; dan
   d. memberikan hak akses khusus secara terpisah dari akun yang digunakan untuk kegiatan umum.
7. melakukan pemantauan terhadap akses ke aset informasi meliputi:
   a. kegagalan akses;
   b. penggunaan hak akses tidak wajar;
   c. alokasi dan penggunaan hak akses khusus;
   d. penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan
   e. penggunaan sumber daya sensitif.
8. menghapus akun setiap pegawai dan pihak ketiga yang tidak lagi memiliki kepentingan terhadap akses aset informasi, dimutasi, berhenti, atau telah berakhir kontraknya.

BAB VIII
KEAMANAN KRIPTOGRAFI

Keamanan kriptografi untuk memastikan penggunaan kriptografi yang tepat untuk melindungi kerahasiaan, keutuhan, dan keotentikan data dan informasi rahasia dan/atau sangat rahasia yang dikelola dalam perangkat informasi. Keamanan kriptografi untuk informasi rahasia dan/atau sangat rahasia dilaksanakan oleh Tim SMKI bekerja sama dengan Unit Organisasi terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. melakukan klasifikasi informasi yang disimpan dan dikelola dalam perangkat informasi sesuai dengan peraturan yang berlaku; dan
2. menerapkan keamanan kriptografi untuk informasi berklasifikasi rahasia dan/atau sangat rahasia dengan cara sebagai berikut namun tidak terbatas pada:
   a. menerapkan jalur komunikasi aman dengan menerapkan *Secure Socket Layer* (SSL) untuk proses otentikasi antara pengguna dengan aplikasi berbasis website;
   b. menjaga kerahasiaan kata sandi dan menyimpannya dalam basis data dengan mekanisme *hash function*;
   c. melindungi kerahasiaan data dan informasi rahasia dan/atau sangat rahasia yang dipertukarkirimkan dan disimpan dalam basis data dengan melakukan enkripsi;
   d. menerapkan otentikasi berbasis tanda tangan digital dengan menggunakan sertifikat elektronik yang dikeluarkan oleh Pihak Ketiga Terpercaya; dan
   e. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan peraturan perundangan dan/atau rekomendasi dari Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

BAB IX
KEAMANAN FISIK DAN LINGKUNGAN

Keamanan fisik dan lingkungan dilakukan untuk memberikan pelindungan, pemeliharaan, keamanan, dan ketersediaan aset informasi. Keamanan fisik dan lingkungan dilaksanakan oleh Tim SMKI bekerja sama dengan Unit Organisasi terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. menyimpan infrastruktur di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai antara lain namun tidak terbatas pada:
   a. Pintu dengan kontrol akses;
   b. Kamera pengawas (CCTV);
   c. Pendeteksi asap;
   d. Pendeteksi kelembapan udara;
   e. Pendeteksi suhu ruangan;
   f. Sistem pemadam kebakaran; dan
   g. Perangkat pemutus aliran listrik.
2. akses ke Pusat Data dan/atau area kerja layanan informasi yang berisi data dan/atau informasi rahasia dan/atau sangat rahasia harus dibatasi dan hanya diberikan kepada pegawai yang memiliki akses;
3. Pihak Ketiga yang memasuki Pusat Data dan/atau area kerja layanan informasi yang berisikan data dan/atau informasi rahasia dan/ atau sangat rahasia harus didampingi oleh pegawai yang ditugaskan sepanjang waktu kunjungan;
4. makanan dan minuman dilarang untuk dibawa masuk ke atau dikonsumsi di dalam ruang *server* Pusat Data;
5. semua area yang digunakan untuk menyimpan aset informasi merupakan area bebas rokok;
6. batas minimum dan maksimum suhu dan kelembaban di dalam ruang server Pusat Data harus memenuhi standar yang disyaratkan pabrikan perangkat dan senantiasa dilakukan pengawasan terhadap kondisi suhu dan kelembaban;
7. pengamanan area Pusat Data dan area kerja layanan informasi dilakukan sesuai Prosedur Keamanan Area;

8. pengamanan kantor, ruangan, dan fasilitas kerja sesuai dengan peraturan dan standar keamanan dan keselamatan kerja, termasuk *clear screen policy* dan *clean desk policy*;
9. infrastruktur yang digunakan untuk menjalankan aplikasi dipelihara sesuai dengan buku petunjuk/manualnya;
10. Dalam hal pemeliharaan infrastruktur tidak dapat dilakukan di tempat, maka pemindahan infrastruktur dilakukan berdasarkan persetujuan kepala Pusat Data dan Informasi Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah;
11. Dalam hal pemindahan infrastruktur terdapat data dan/atau informasi berklasifikasi rahasia dan/atau sangat rahasia yang tersimpan pada perangkat tersebut, maka data dan/atau informasi berklasifikasi rahasia dan/atau sangat rahasia tersebut harus dipindahkan terlebih dahulu ke dalam media penyimpanan lain;
12. Dalam hal pemeliharaan dilakukan oleh Pihak Ketiga, maka pelaksanaannya dilakukan dengan membuat perjanjian kerja sama yang paling sedikit memuat perjanjian menjaga kerahasiaan, pemeliharaan yang disediakan, dan tingkat kinerja yang harus dipenuhi Pihak Ketiga;
13. infrastruktur beserta perangkat pemulihan dan media penyimpanan data cadangan wajib diletakkan di tempat yang aman dengan struktur yang memadai untuk menghindari kerusakan dari hama (misal: tikus, semut dan rayap) dan bencana (misal: banjir dan gempa);
14. semua infrastruktur harus mendapatkan pasokan daya yang sesuai dengan spesifikasi yang disyaratkan oleh pabrikan infrastruktur;
15. pasokan listrik yang digunakan untuk mengoperasikan infrastruktur harus mempunyai sumber alternatif dengan daya dan jangka waktu ketersediaan atau jangka waktu pengoperasian yang cukup, yang paling sedikit mencakup generator listrik dan *Uniterruptable Power Supply* (UPS) dengan daya yang cukup dan dengan konfigurasi yang dapat memindahkan pasokan listrik tanpa gangguan terhadap infrastruktur;
16. bahan berbahaya atau mudah terbakar di lingkungan LKPP wajib disimpan pada jarak yang aman dari Pusat Data dan area kerja layanan informasi;
17. perangkat pemadam kebakaran wajib disediakan, dipelihara, dan diletakkan di tempat yang mudah dijangkau;

18. infrastruktur diletakkan pada lokasi yang meminimalisasi akses pihak yang tidak berwenang;
19. infrastruktur yang menangani informasi sensitif diposisikan dan dibatasi sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak tidak berwenang;
20. perlindungan petir wajib diterapkan untuk semua bangunan dan filter perlindungan petir dipasang untuk semua jalur komunikasi dan listrik; dan
21. pengamanan kabel di Pusat Data dan/atau area kerja layanan informasi dilakukan dengan mengikuti standar mekanikal/elektrikal Pusat Data yang berlaku.

BAB X
KEAMANAN OPERASIONAL

Keamanan operasional dilakukan untuk memastikan operasional yang aman dan benar pada aset informasi, mengimplementasikan dan memelihara keamanan aset informasi, mengelola layanan yang diberikan oleh Pihak Ketiga, meminimalkan risiko kegagalan, dan melindungi keutuhan dan ketersediaan aset informasi. Keamanan operasional di lingkungan LKPP dilakukan oleh Tim SMKI bekerja sama dengan Unit Organisasi terkait, cara sebagai berikut namun tidak terbatas pada:

1. mendokumentasikan, memelihara, dan menyediakan prosedur penggunaan perangkat informasi sesuai dengan peruntukannya;
2. perubahan pada aset informasi yang dapat mempengaruhi keamanan informasi harus didokumentasikan dan dikendalikan dengan memperhatikan manajemen risiko dan persetujuan dari pemilik aset informasi;
3. menetapkan kriteria penerimaan untuk sistem informasi baru, pemutakhiran dan versi baru serta melakukan pengujian sebelum penerimaan;
4. memantau penggunaan aset informasi yang dimiliki dan membuat proyeksi kebutuhan ke depan untuk menjamin aset informasi yang dibutuhkan. Untuk aset informasi yang kritikal harus senantiasa dimonitor dan dievaluasi kapasitas dan ketersediaannya;
5. melakukan pemisahan akses terhadap informasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia (seorang pegawai dihindari memiliki akses terhadap seluruh aset informasi dan perangkat pengolahnya);
6. memisahkan lingkungan pengembangan, pengujian, dan operasional untuk mengurangi risiko perubahan atau akses oleh pihak yang tidak berhak terhadap sistem operasional;
7. menerapkan sistem pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman *malware*;
8. Perlindungan dilakukan dengan cara pemasangan paling sedikit meliputi:
   a. perangkat *firewall*;
   b. perangkat *Intrusion Prevention System* (IPS);

c. perangkat antivirus;
d. perangkat manajemen akses pengguna; dan
e. perangkat monitoring / pendukung lainnya sesuai perkembangan teknologi keamanan informasi.

9. melakukan pembuatan backup informasi dan aplikasi yang berada di Pusat Data dan/atau area kerja layanan informasi secara berkala sesuai dengan Prosedur *backup* di lingkungan LKPP;
10. salinan cadangan data/informasi, aplikasi, dan image sistem harus diambil dan diuji secara berkala; dan
11. mencatat *(logging)* setiap aktivitas administrator, aktivitas pengguna, peristiwa kegagalan, dan kejadian keamanan serta disimpan dalam periode tertentu;
12. melindungi sistem pencatatan (*log*) dari pemalsuan dan akses yang tidak berwenang; dan
13. melakukan penilaian kerentanan terhadap perangkat informasi (*vulnerability assessment*) secara berkala dan melakukan tindakan perlindungan terhadap kerentanan dan/atau ancaman yang teridentifikasi.

BAB XI
KEAMANAN KOMUNIKASI

Keamanan komunikasi dilakukan untuk memastikan keamanan pertukaran informasi melalui jaringan komunikasi. Keamanan komunikasi di lingkungan LKPP dilakukan oleh Tim SMKI bekerja sama dengan Unit Organisasi terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. Tim SMKI mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh pihak ketiga;
2. dalam hal pihak ketiga diizinkan mengakses ke jaringan, maka dilakukan pemantauan serta pencatatan kegiatan selama menggunakan jaringan;
3. melindungi jaringan dari pihak yang tidak berhak mengakses, minimal dengan cara:
    a. melakukan dokumentasi arsitektur jaringan yang meliputi seluruh komponen infrastruktur dan aplikasi jaringan;
    b. menerapkan teknologi keamanan jaringan berbasis enkripsi dan otentikasi (termasuk sertifikat elektronik);
    c. menerapkan pemisahan jaringan untuk kelompok pengguna, layanan informasi, dan sistem informasi;
    d. menerapkan parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan; dan
    e. menerapkan Prosedur Penggunaan Layanan Jaringan yang membatasi akses ke layanan jaringan atau aplikasi.
4. informasi yang terdapat dalam aplikasi yang melewati jaringan publik harus dilindungi dari upaya pengungkapan, modifikasi, dan perusakan dengan menerapkan mekanisme kriptografi;
5. melakukan pendeteksian dan perlindungan terhadap kode berbahaya (*malicious code*) yang disisipkan pada file yang dikirim melalui sistem elektronik;
6. memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan untuk informasi elektronik berklasifikasi rahasia dan/atau sangat rahasia;

7. menetapkan prosedur pertukaran informasi yang mengatur sistem dan keamanan yang digunakan untuk pertukaran informasi;
8. menerapkan audit logging yang mencatat aktivitas pengguna dan kejadian keamanan informasi dalam kurun waktu tertentu untuk membantu investigasi di masa mendatang, antara lain:
   a. kegagalan akses;
   b. penggunaan hak akses tidak wajar;
   c. alokasi dan penggunaan hak akses khusus;
   d. penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan
   e. penggunaan sumber daya sensitif.
9. menerapkan sistem pencatatan aktivitas administrator dan operator sistem;
10. menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindak pengamanan yang tepat; dan
11. memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.

BAB XII
KEAMANAN PENGEMBANGAN DAN PEMELIHARAAN

Keamanan pengembangan dan pemeliharaan sistem dilakukan untuk memastikan bahwa keamanan informasi merupakan bagian yang terintegrasi dalam daur hidup aset informasi untuk mencegah terjadinya kesalahan, eksploitasi, modifikasi, dan perusakan aset informasi oleh pihak yang tidak berwenang. Keamanan pengembangan dan pemeliharaan di lingkungan LKPP dilakukan oleh Tim bekerja sama dengan Unit Organisasi terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. lingkungan pengembangan, pengujian, dan operasional aplikasi harus dipisahkan baik secara fisik, *logic*, maupun aksesnya;
2. menjaga agar lingkungan pengembangan tidak boleh diakses dari sistem operasional layanan;
3. mengupayakan lingkungan pengujian sama dengan lingkungan operasional layanan;
4. memilih data uji dengan hati-hati, melindungi dan mengendalikannya;
5. mengawasi dan memantau aktivitas pembangunan/pengembangan aplikasi dan infrastruktur yang dialihdayakan pada pihak ketiga;
6. memastikan bahwa dalam proses perencanaan dan pembangunan/pengembangan aplikasi dan infrastruktur termasuk yang dilakukan oleh pihak ketiga, telah memasukkan fitur-fitur keamanan dalam spesifikasi aplikasi dan infrastruktur yang dibangun/dikembangkan;
7. fitur-fitur keamanan yang dimasukkan sesuai dengan standar keamanan relevan, yang mencakup:
   a. Standar keamanan data dan informasi;
   b. Standar keamanan aplikasi;
   c. Standar keamanan pusat data;
   d. Standar keamanan sistem penghubung layanan; dan
   e. Standar keamanan jaringan intra.
8. standar keamanan sebagaimana dimaksud pada angka 7 minimal memenuhi standar keamanan ditetapkan oleh Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.

9. melaksanakan uji kelaikan aplikasi sebelum aplikasi digunakan dan sewaktu-waktu sesuai kebutuhan dengan memenuhi aspek berikut:
   a. uji fungsi, yaitu pengujian yang memastikan aplikasi yang dibangun dan/atau dikembangkan telah memenuhi fungsi-fungsi sesuai dengan dokumentasi terkait;
   b. uji integrasi, yaitu pengujian yang memastikan aplikasi yang dibangun dan/atau dikembangkan telah memenuhi kebutuhan dan persyaratan integrasi dengan aplikasi, data, serta komponen-komponen lain yang terkait;
   c. uji beban, yaitu pengujian yang memastikan aplikasi yang dibangun dan/atau dikembangkan dapat berfungsi sebagaimana mestinya menghadapi beban kerja yang dikenakan terhadapnya; dan
   d. uji keamanan, yaitu pengujian yang memastikan aplikasi yang dibangun dan/atau dikembangkan dapat menjaga keamanan data dan informasi yang terkait dengannya.
10. uji kelaikan pada aspek uji fungsi, uji integrasi, dan uji beban dapat menggunakan pedoman/instrumen pengukuran yang ditetapkan oleh Kementerian yang menyelenggarakan tugas pemerintahan di bidang komunikasi dan informatika;
11. uji kelaikan pada aspek uji keamanan dapat menggunakan pedoman/instrumen pengukuran yang ditetapkan oleh Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber; dan
12. pelaksanaan pembangunan dan pengembangan aplikasi dilakukan sesuai dengan Standar Teknis dan Prosedur Pembangunan dan Pengembangan Aplikasi yang ditetapkan oleh Kementerian yang melaksanakan tugas di bidang komunikasi dan informatika.

BAB XIII
KEAMANAN PIHAK KETIGA

Keamanan Pihak Ketiga dilakukan untuk memastikan perlindungan dari aset informasi yang dapat diakses oleh Pihak Ketiga. Keamanan Pihak Ketiga di lingkungan LKPP dilakukan oleh Tim SMKI bekerja sama dengan Unit Organisasi terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. melakukan pemeriksaan latar belakang Pihak Ketiga dengan tetap memperhatikan privasi dan perlindungan data pribadi;
2. membuat dan meninjau ulang secara berkala perjanjian tertulis dengan pihak ketiga yang terlibat dalam penggunaan dan/atau pengelolaan aset informasi yang menyatakan tanggung jawab terhadap keamanan aset informasi. Perjanjian tertulis sebagaimana dimaksud paling sedikit memuat:
   a. perlindungan atas informasi rahasia dan/atau sangat rahasia dan hak kekayaan intelektual setiap pihak;
   b. dalam hal aset informasi disediakan oleh Pihak Ketiga, maka adanya jaminan bahwa tidak terdapat *malicious code* dan *backdoor*;
   c. hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia dan/atau sangat rahasia;
   d. pengawasan atas akses terhadap aset informasi yang diberikan pada pihak ketiga;
   e. pelaporan terhadap penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan;
   f. syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian;
   g. penggunaan jalur komunikasi yang aman untuk perpindahan informasi antara LKPP dengan pihak ketiga; dan
   h. dalam hal Pihak Ketiga tidak lagi menjadi bagian dalam pengelolaan aset informasi, maka aset informasi yang dikuasainya harus diserahkan kembali kepada Tim SMKI.
3. memastikan secara berkala bahwa pengendalian keamanan informasi, definisi layanan, dan tingkat layanan yang termuat dalam kesepakatan

penyediaan layanan, telah diterapkan, dioperasikan, dan dipelihara oleh pihak ketiga;

4. memastikan *Level Service Agreement* (SLA) pihak ketiga telah mengatur ketersediaan layanan dan penyelesaian insiden keamanan;
5. melakukan pemantauan terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh pihak ketiga secara berkala;
6. memperhatikan kritikalitas, proses yang terkait dan hasil penilaian ulang risiko layanan apabila terjadi perubahan pada layanan yang disediakan oleh pihak ketiga;
7. mencatat peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan oleh pihak ketiga;
8. memberikan informasi tentang gangguan keamanan dan mengkaji informasi bersama pihak ketiga;
9. mencabut hak akses terhadap akses informasi yang dimiliki pihak ketiga apabila yang bersangkutan tidak lagi bekerja di lingkungan LKPP;
10. membuat berita acara serah terima terkait mengembalikan seluruh aset informasi yang dipergunakan selama bekerja bagi pihak ketiga yang berakhir masa kontraknya; dan
11. memastikan pihak ketiga dan tamu yang memasuki lingkungan area pusat data, dan tempat layanan informasi harus mematuhi standar keamanan fisik dan lingkungan.

BAB XIV
MANAJEMEN INSIDEN SIBER

Manajemen insiden siber dilaksanakan untuk mengendalikan insiden siber. Manajemen insiden siber di lingkungan LKPP dilakukan oleh Tim SMKI bekerja sama dengan Unit Organisasi terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. membentuk Tim Respon Insiden Keamanan Komputer yang bertugas melakukan pencegahan dan penanganan insiden siber yang terjadi di lingkungan LKPP;
2. Tim Respon Insiden Keamanan Komputer melakukan tindakan pencegahan insiden siber paling sedikit meliputi:
   a. melakukan penilaian kerentanan dan/atau *penetration testing* untuk menemukan celah keamanan pada aset informasi;
   b. mengimplementasikan alat monitoring keamanan antara lain berupa namun tidak terbatas pada *Security Information and Event Management* (SIEM); dan
   c. melakukan monitoring dan pendeteksian serangan terhadap aset informasi.
3. Dalam hal terjadi insiden siber, Tim Respon Insiden Keamanan Komputer melaksanakan prosedur penanganan insiden siber paling sedikit meliputi:
   a. mengidentifikasi sumber serangan;
   b. menganalisis informasi yang berkaitan dengan insiden selanjutnya;
   c. memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
   d. mendokumentasikan bukti insiden yang terjadi; dan
   e. memitigasi atau mengurangi dampak risiko Keamanan SPBE.
4. menyusun berbagai macam skenario penanganan insiden siber;
5. melakukan simulasi secara berkala skenario penanganan insiden siber yang telah disusun;
6. memberikan pelatihan terhadap SDM internal yang terlibat pada penanganan insiden siber sesuai skenario yang disusun;
7. menjalankan program kesadaran ancaman dan penanganan insiden siber, serta ajakan peran aktif pada seluruh pegawai;

8. memastikan tersedianya kontak pelaporan insiden siber yang dapat diakses oleh seluruh pegawai di lingkungan LKPP termasuk oleh pihak ketiga; dan
9. melakukan pengukuran tingkat kematangan penanganan insiden siber secara berkala.

BAB XV
MANAJEMEN KEBERLANGSUNGAN LAYANAN INFORMASI

Manajemen keberlangsungan layanan informasi dilakukan untuk menjamin ketersediaan layanan informasi pada saat terjadi keadaan darurat. Manajemen keberlangsungan layanan informasi dilakukan oleh Tim SMKI bekerja sama dengan Unit Organisasi terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. melakukan identifikasi risiko terhadap keberlangsungan layanan informasi;
2. menyusun dan menerapkan rencana keberlangsungan layanan informasi (*Business Continuity Planning)* untuk menjaga dan mengembalikan operasional aset informasi dalam jangka waktu yang disepakati dan tingkat keberlangsungan yang dibutuhkan;
3. rencana keberlangsungan layanan informasi paling sedikit meliputi:
   a. prosedur keberlangsungan layanan informasi pada saat keadaan darurat, manajemen risiko, analisis dampak kegiatan, pengembalian kondisi sebelum terjadi gangguan peralihan kondisi normal, dan uji coba keberlangsungan kegiatan;
   b. penetapan peran dan penanggung jawab pegawai yang terlibat dalam pelaksanaan keberlangsungan layanan informasi; dan
   c. pelaksanaan sosialisasi dan pelatihan keberlangsungan layanan informasi;
4. aplikasi umum/sistem elektronik berkategori strategis, harus memiliki redudansi yang cukup untuk memenuhi ketersediaan layanan informasi;
5. melakukan uji coba rencana keberlangsungan layanan informasi secara berkala;
6. melaksanakan proses keberlangsungan layanan informasi pada saat keadaan darurat sesuai prosedur keberlangsungan layanan informasi; dan
7. pelaksanaan pengelolaan layanan dilakukan sesuai dengan pedoman manajemen layanan SPBE yang ditetapkan oleh Kementerian yang melaksanakan tugas di bidang komunikasi dan informatika.

BAB XVI
PENGENDALIAN KEPATUHAN

Pengendalian kepatuhan dilaksanakan untuk memastikan kepatuhan pegawai dan Pihak Ketiga dalam melaksanakan keamanan informasi sesuai dengan ketentuan peraturan perundang-undangan, kontrak dan keselarasan dengan kebijakan keamanan informasi yang berlaku di lingkungan LKPP. Pengendalian kepatuhan keamanan informasi di lingkungan LKPP, dilakukan oleh Tim SMKI bekerja sama dengan Unit Organisasi terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. mengidentifikasi, mendokumentasikan, mereviu, dan memelihara regulasi, standar, dan prosedur keamanan informasi;
2. memeriksa kepatuhan seluruh pegawai dan pihak ketiga terhadap regulasi, standar, dan prosedur keamanan informasi;
3. mendapatkan aplikasi hanya melalui sumber yang dikenal dan memiliki reputasi baik, untuk memastikan tidak ada pelanggaran hak cipta;
4. memeriksa kepatuhan penggunaan lisensi aplikasi dan menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;
5. memelihara bukti kepemilikan lisensi, *master disk*, dan buku manual;
6. melakukan pemeriksaan bahwa tidak ada produk bajakan yang terinstal (pelanggaran hak kekayaan intelektual) di lingkungan LKPP;
7. memastikan rekaman terlindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah, dan rilis tidak sah sesuai dengan persyaratan peraturan perundang-undangan, kontraktual dan bisnis;
8. memastikan pengamanan privasi dan data pribadi yang dapat diidentifikasi sesuai dengan persyaratan peraturan perundang-undangan yang berlaku;

9. memastikan penyesuaian penerapan kriptografi dengan peraturan perundang-undangan yang berlaku;
10. kebijakan, standar dan keamanan informasi dan implementasinya harus direviu berkala secara independen atau ketika terjadi perubahan; dan
11. mereviu sistem informasi secara berkala agar sesuai dengan kebijakan dan standar keamanan informasi di lingkungan LKPP.

BAB XVII
AUDIT KEAMANAN INFORMASI

Audit keamanan informasi dilaksanakan secara berkala untuk memastikan diterapkannya kebijakan, standar, dan Prosedur keamanan informasi. Audit keamanan informasi dilaksanakan melalui kegiatan Audit Internal dan Audit Eksternal yang dilaksanakan dengan cara sebagai berikut namun tidak terbatas pada:

1. Audit Internal keamanan informasi

a. Audit Internal keamanan informasi di lingkungan LKPP dilaksanakan oleh APIP;
b. APIP merencanakan, menetapkan, dan menjalankan program audit sesuai dengan pedoman audit internal keamanan informasi. Program audit minimal mencakup frekuensi, metode, kriteria, lingkup, tanggung jawab, dan pelaporan audit, serta mempertimbangkan pentingnya proses yang sedang berjalan dan hasil audit sebelumnya;
c. Audit Internal keamanan informasi dilaksanakan dalam Peta Rencana SPBE LKPP;
d. Audit Internal keamanan informasi dilaksanakan oleh Auditor yang memiliki kompetensi memadai dan memiliki objektivitas serta imparsialitas (ketidakberpihakan) dalam melaksanakan Audit Internal keamanan informasi;
e. Setiap temuan audit harus dicatat secara formal oleh Auditor dan diberikan kepada Auditan;
f. Auditan harus melakukan perbaikan terhadap setiap temuan yang diberikan oleh Auditor dalam jangka waktu yang disepakati;

g. Laporan Audit Internal dilaporkan kepada Tim SMKI dan Sekretaris Utama sebagai bahan evaluasi penerapan Kebijakan SMKI;
h. Menyimpan dan mendokumentasikan proses dan hasil audit internal sebagai alat bukti dari program audit; dan
i. Pelaksanaan audit internal keamanan informasi dapat menggunakan instrumen penilaian Audit Keamanan SPBE yang ditetapkan oleh Kepala Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.

2. Audit Eksternal Keamanan Informasi

Audit Eksternal Keamanan Informasi di lingkungan LKPP dilaksanakan oleh pihak ketiga sesuai dengan peraturan perundang-undangan yang berlaku.

BAB XVIII
EVALUASI KINERJA DAN PERBAIKAN BERKELANJUTAN KEAMANAN INFORMASI

A. Evaluasi Kinerja keamanan informasi

Evaluasi kinerja keamanan informasi dilaksanakan paling sedikit satu kali dalam satu tahun untuk memastikan pencapaian target keamanan informasi yang telah direncanakan. Tim SMKI melakukan evaluasi kinerja pelaksanaan keamanan informasi berdasarkan peta rencana dan sasaran keamanan informasi yang telah ditetapkan, dengan cara sebagai berikut namun tidak terbatas pada:

1. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan keamanan informasi;
2. menetapkan indikator kinerja pada setiap area proses;
3. memformulasi pelaksanaan keamanan informasi dengan mengukur secara kuantitatif kinerja yang diharapkan;
4. melakukan evaluasi terhadap penyelenggaraan atau pelaksanaan SMKI;
5. menganalisis efektifitas pelaksanaan keamanan informasi; dan
6. mendukung dan merealisasikan program audit keamanan informasi.

Hasil evaluasi kinerja keamanan informasi didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja keamanan informasi berikutnya yang patut disampaikan sebagai laporan kinerja tahunan kepada Kepala Pusat Data dan Informasi Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah dan Sekretaris Utama Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah.

B. Perbaikan Berkelanjutan Keamanan Informasi

Perbaikan berkelanjutan merupakan tindak lanjut dari hasil evaluasi kinerja keamanan informasi. Tim SMKI melakukan perbaikan berkelanjutan dengan cara sekurang-kurangnya sebagai berikut:

1. mengatasi permasalahan dalam pelaksanaan keamanan informasi; dan
2. memperbaiki pelaksanaan keamanan informasi secara berkala. Tindakan perbaikan yang telah dilakukan didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja keamanan informasi.

KEPALA LEMBAGA KEBIJAKAN
PENGADAAN BARANG/JASA
PEMERINTAH,

ttd

HENDRAR PRIHADI