Yth.

1. Direksi Perusahaan Perasuransian;
2. Pengurus dan Pelaksana Tugas Pengurus Dana Pensiun;
3. Direksi Lembaga Pembiayaan;
4. Direksi Perusahaan Pergadaian;
5. Direksi Lembaga Penjamin;
6. Direksi Penyelenggara Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi;
7. Direktur Eksekutif Lembaga Pembiayaan Ekspor Indonesia;
8. Direksi Perusahaan Pembiayaan Sekunder Perumahan;
9. Direksi Badan Penyelenggara Jaminan Sosial; dan
10. Direksi PT Permodalan Nasional Madani (Persero),

di tempat.

SALINAN

SURAT EDARAN OTORITAS JASA KEUANGAN

NOMOR 22 /SEOJK.05/2021

REPUBLIK INDONESIA

TENTANG

PENERAPAN MANAJEMEN RISIKO DALAM PENGGUNAAN TEKNOLOGI INFORMASI OLEH LEMBAGA JASA KEUANGAN NONBANK

Sehubungan dengan amanat Pasal 33 Peraturan Otoritas Jasa Keuangan Nomor 4/POJK.05/2021 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Lembaga Jasa Keuangan Nonbank (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 78, Tambahan Lembaran Negara Republik Indonesia Nomor 6668), perlu untuk mengatur ketentuan lebih lanjut mengenai penerapan manajemen risiko dalam penggunaan teknologi informasi oleh lembaga jasa keuangan nonbank dalam Surat Edaran Otoritas Jasa Keuangan sebagai berikut:

I. KETENTUAN UMUM

Dalam Surat Edaran Otoritas Jasa Keuangan ini, yang dimaksud dengan:

1. Lembaga Jasa Keuangan Nonbank yang selanjutnya disebut LJKNB adalah lembaga yang melaksanakan kegiatan di sektor perasuransian, dana pensiun, lembaga pembiayaan, dan lembaga jasa keuangan lainnya.

2. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
3. Layanan Keuangan Elektronik adalah layanan bagi konsumen untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi keuangan melalui media elektronik.
4. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
5. Pusat Data adalah suatu fasilitas yang digunakan untuk menempatkan Sistem Elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.
6. Pusat Pemulihan Bencana adalah suatu fasilitas yang digunakan untuk memulihkan kembali data atau informasi serta fungsi penting Sistem Elektronik yang terganggu atau rusak akibat terjadinya bencana yang disebabkan oleh alam atau manusia.
7. Pangkalan Data adalah sekumpulan data komprehensif dan disusun secara sistematis, dapat diakses oleh pengguna sesuai wewenang masing-masing dan dikelola oleh administrator Pangkalan Data.
8. Rencana Pemulihan Bencana adalah dokumen yang berisikan rencana dan langkah untuk menggantikan dan/atau memulihkan kembali akses data, perangkat keras dan perangkat lunak yang diperlukan, agar LJKNB dapat menjalankan kegiatan operasional bisnis yang kritikal setelah adanya gangguan dan/atau bencana.
9. Direksi adalah organ perseroan yang berwenang dan bertanggung jawab penuh atas pengurusan perseroan untuk kepentingan perseroan, sesuai dengan maksud dan tujuan perseroan serta mewakili perseroan, baik di dalam maupun di luar pengadilan sesuai dengan ketentuan anggaran dasar bagi LJKNB yang berbentuk badan hukum perseroan terbatas atau yang setara dengan Direksi bagi LJKNB yang berbentuk badan hukum koperasi, usaha bersama, dana pensiun, lembaga pembiayaan ekspor Indonesia, badan penyelenggara jaminan sosial, atau badan usaha perseroan komanditer.

10. Dewan Komisaris adalah organ perseroan yang bertugas melakukan pengawasan secara umum dan/atau khusus sesuai dengan anggaran dasar serta memberi nasihat kepada Direksi bagi LJKNB yang berbentuk badan hukum perseroan terbatas atau yang setara dengan Dewan Komisaris bagi LJKNB yang berbentuk badan hukum koperasi, usaha bersama, dana pensiun, lembaga pembiayaan ekspor Indonesia, badan penyelenggara jaminan sosial, atau badan usaha perseroan komanditer.

II. CAKUPAN LEMBAGA JASA KEUANGAN NONBANK

LJKNB sebagaimana dimaksud dalam Romawi I angka 1 meliputi:

1. perusahaan perasuransian, yang terdiri atas:
   a. perusahaan asuransi;
   b. perusahaan reasuransi;
   c. perusahaan asuransi syariah;
   d. perusahaan reasuransi syariah;
   e. perusahaan pialang asuransi;
   f. perusahaan pialang reasuransi; dan
   g. perusahaan penilai kerugian asuransi,

   sebagaimana dimaksud dalam peraturan perundang-undangan mengenai perasuransian;
2. dana pensiun sebagaimana dimaksud dalam peraturan perundang-undangan mengenai dana pensiun;
3. lembaga pembiayaan, terdiri atas:
   a. perusahaan pembiayaan;
   b. perusahaan pembiayaan syariah;
   c. perusahaan modal ventura;
   d. perusahaan modal ventura syariah; dan
   e. perusahaan pembiayaan infrastruktur,

   sebagaimana dimaksud dalam peraturan perundang-undangan mengenai lembaga pembiayaan;
4. lembaga jasa keuangan lainnya, terdiri atas:
   a. perusahaan pergadaian sebagaimana dimaksud dalam peraturan perundang-undangan mengenai pergadaian;
   b. lembaga penjamin, yang terdiri atas
      1) perusahaan penjaminan;

2) perusahaan penjaminan syariah;
3) perusahaan penjaminan ulang; dan
4) perusahaan penjaminan ulang syariah,

sebagaimana dimaksud dalam peraturan perundang-undangan mengenai penjaminan;

c. penyelenggara layanan pinjam meminjam uang berbasis teknologi informasi sebagaimana dimaksud dalam peraturan perundang-undangan mengenai layanan pinjam meminjam uang berbasis teknologi informasi;
d. lembaga pembiayaan ekspor Indonesia sebagaimana dimaksud dalam peraturan perundang-undangan mengenai lembaga pembiayaan ekspor Indonesia;
e. perusahaan pembiayaan sekunder perumahan sebagaimana dimaksud dalam peraturan perundang-undangan mengenai perusahaan pembiayaan sekunder perumahan;
f. badan penyelenggara jaminan sosial sebagaimana dimaksud dalam peraturan perundang-undangan mengenai badan penyelenggara jaminan sosial; dan
g. PT Permodalan Nasional Madani (Persero) sebagaimana dimaksud dalam peraturan perundang-undangan mengenai PT Permodalan Nasional Madani (Persero),

yang menggunakan Teknologi Informasi dalam penyelenggaraan usaha.

III. RUANG LINGKUP MANAJEMEN RISIKO TEKNOLOGI INFORMASI

1. Penerapan manajemen risiko dalam penggunaan Teknologi Informasi mencakup paling sedikit:
   a. pengawasan aktif Direksi dan Dewan Komisaris;
   b. kecukupan kebijakan dan prosedur penggunaan Teknologi Informasi;
   c. kecukupan proses identifikasi, pengukuran, pengendalian, dan pemantauan risiko penggunaan Teknologi Informasi; dan
   d. sistem pengendalian internal atas penggunaan Teknologi Informasi.
2. Penerapan manajemen risiko sebagaimana dimaksud pada angka 1 dilakukan secara terintegrasi dalam setiap tahapan penggunaan Teknologi Informasi sejak proses perencanaan, pengadaan,

pengembangan, operasional, pemeliharaan hingga penghentian dan penghapusan sumber daya Teknologi Informasi.

3. Penerapan manajemen risiko dalam penggunaan Teknologi Informasi sebagaimana dimaksud pada angka 1 wajib disesuaikan dengan tujuan, kebijakan usaha, ukuran, dan kompleksitas usaha LJKNB.
4. Penerapan manajemen risiko dalam penggunaan Teknologi Informasi sebagaimana dimaksud pada angka 1 diwujudkan dalam bentuk dokumentasi yang baik atas aspek paling sedikit:
   a. organisasi dan manajemen pendukung pelaksanaan manajemen risiko Teknologi Informasi;
   b. penerapan komponen manajemen risiko dalam penggunaan Teknologi Informasi;
   c. kebijakan dan prosedur penggunaan Teknologi Informasi;
   d. arsitektur aplikasi;
   e. daftar aplikasi;
   f. jaringan komunikasi;
   g. Pusat Data dan Pusat Pemulihan Bencana;
   h. pengamanan Teknologi Informasi;
   i. Rencana Pemulihan Bencana;
   j. pihak penyedia jasa Teknologi Informasi; dan
   k. biaya Teknologi Informasi.
5. Dokumentasi sebagaimana dimaksud pada angka 4 disusun sesuai dengan format 1 sampai dengan format 11 tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

IV. PENGAWASAN AKTIF DIREKSI DAN DEWAN KOMISARIS

1. LJKNB wajib menetapkan wewenang dan tanggung jawab yang jelas dari Direksi, Dewan Komisaris, dan pejabat pada setiap jenjang jabatan yang terkait dengan penggunaan Teknologi Informasi secara tertulis.
2. Bagi LJKNB yang memiliki komite pengawas Teknologi Informasi, pelaksanaan tugas dan tanggung jawab komite pengawas Teknologi Informasi diwujudkan dengan pertemuan secara berkala yang didokumentasikan dalam bentuk risalah rapat.

3. Pertemuan secara berkala sebagaimana dimaksud pada angka 2 dapat melibatkan satuan kerja terkait di LJKNB dan dilakukan secara fisik atau virtual.
4. Komite pengarah Teknologi Informasi menetapkan jangka waktu pertemuan secara berkala sebagaimana dimaksud pada angka 3 dalam kebijakan secara tertulis.

V. KECUKUPAN KEBIJAKAN DAN PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI

1. Kebijakan dan prosedur penggunaan Teknologi Informasi paling sedikit memuat aspek:
   a. manajemen;
   b. pengembangan dan pengadaan;
   c. operasional Teknologi Informasi;
   d. jaringan komunikasi;
   e. pengamanan informasi;
   f. Rencana Pemulihan Bencana;
   g. penggunaan pihak penyedia jasa Teknologi Informasi; dan
   h. Layanan Keuangan Elektronik, bagi LJKNB yang menyelenggarakan Layanan Keuangan Elektronik.
2. Kebijakan dan prosedur aspek manajemen sebagaimana dimaksud pada angka 1 huruf a paling sedikit terdiri atas:
   a. kesadaran risiko (*risk awareness*) mengenai penyelenggaraan Teknologi Informasi dari manajemen;
   b. pemahaman yang jelas mengenai tingkat risiko yang akan diambil (*risk appetite*), toleransi risiko (*risk tolerance*), dan limit risiko (*risk limit*) dari LJKNB;
   c. pemahaman terhadap ketentuan peraturan perundang-undangan mengenai Teknologi Informasi; dan
   d. transparansi dan tanggung jawab mengenai risiko yang signifikan dari setiap aspek terkait penyelenggaraan Teknologi Informasi.
3. Kebijakan dan prosedur aspek pengembangan dan pengadaan sebagaimana dimaksud pada angka 1 huruf b meliputi:
   a. tahap pengembangan:
      1) inisiasi dan perencanaan;

2) pendefinisian kebutuhan pengguna;
3) perancangan sistem;
4) pemrograman;
5) pengujian;
6) implementasi;
7) pengkajian ulang pasca implementasi;
8) pemeliharaan; dan
9) pemusnahan; dan

b. tahap pengadaan:
1) pedoman pengadaan;
2) kontrak pembelian dan lisensi;
3) pemeliharaan;
4) garansi;
5) penyelesaian perselisihan;
6) perubahan perjanjian;
7) keamanan; dan
8) pengalihan sebagian kegiatan (subkontrak) kepada pihak lain.

4. Tahap inisiasi dan perencanaan sebagaimana dimaksud pada angka 3 huruf a angka 1) paling sedikit terdiri atas:
a. Penyusunan proposal yang berisi:
1) rencana untuk menambah, menyempurnakan, atau memperbaiki suatu sistem;
2) tujuan dan manfaat yang diharapkan;
3) analisis dan penanganan risiko;
4) penjelasan bagaimana sistem yang akan dikembangkan dapat mendukung perkembangan usaha LJKNB;
5) pencapaian tujuan bisnis LJKNB; dan
6) perlindungan konsumen LJKNB;
b. evaluasi oleh manajemen, satuan kerja penyelenggara Teknologi Informasi;
c. persetujuan prinsip oleh manajemen, pejabat tertinggi pada satuan kerja penyelenggara Teknologi Informasi, dan/atau pejabat tertinggi pada satuan kerja pengguna Teknologi Informasi atas rencana pengembangan sistem baru dan/atau perubahan sistem;

d. studi kelayakan, yang antara lain berupa pertimbangan bisnis LJKNB, kebutuhan fungsional, rencana waktu pelaksanaan, faktor yang memengaruhi pengembangan, serta analisis biaya dan manfaat; dan
e. persetujuan dan penandatanganan dokumen studi kelayakan oleh manajemen, pejabat tertinggi pada satuan kerja penyelenggara Teknologi Informasi, dan/atau pejabat tertinggi pada satuan kerja pengguna Teknologi Informasi.

5. Tahap pendefinisian kebutuhan pengguna sebagaimana dimaksud pada angka 3 huruf a angka 2) paling sedikit terdiri atas:
   a. pengumpulan kebutuhan yang merupakan proses pengumpulan informasi, baik dengan melalui metode wawancara maupun melalui riset atau melalui pengisian formulir tertentu, mengenai tujuan pengembangan sistem, *output* yang diinginkan, kemampuan sistem dalam mengakomodasi kebutuhan proses bisnis dan mekanisme kerja sistem, serta prosedur penggunaan sistem;
   b. analisis kebutuhan yang merupakan proses pemahaman permasalahan dan kebutuhan untuk menentukan solusi yang dapat dikembangkan;
   c. spesifikasi kebutuhan yang merupakan proses untuk mendeskripsikan fungsional sistem yang akan dikembangkan, spesifikasi proses atau prosedur dan sistem yang ada saat ini, baik dari segi perangkat lunak maupun perangkat keras pendukung serta desain Pangkalan Data; dan
   d. pengelolaan kebutuhan yang merupakan proses untuk mengidentifikasi, mengendalikan, dan menyimpan setiap perubahan terhadap kebutuhan pada saat pengembangan sistem berjalan.

6. Tahap perancangan sistem sebagaimana dimaksud pada angka 3 huruf a angka 3) merupakan proses konversi kebutuhan informasi, fungsi, dan infrastruktur yang teridentifikasi selama tahap inisiasi dan perencanaan menjadi spesifikasi rancangan atau desain yang menjadi dasar pengembangan sistem. Pada tahap perancangan sistem perlu dilakukan pengendalian terhadap aspek yang meliputi

informasi *input*, proses, dan *output* yang terotorisasi, akurat, lengkap, dan aman.

7. Tahap pemrograman sebagaimana dimaksud pada angka 3 huruf a angka 4) paling sedikit terdiri atas:
   a. standar pemrograman yang meliputi penjabaran tanggung jawab *programmer* dan pihak-hak yang terlibat langsung dalam proses pemrograman yaitu dengan cara:
      1) membatasi akses terhadap data, program, utilitasi, dan sistem yang di luar tanggung jawabnya salah satunya dengan pengendalian pengelolaan *library*[1]; dan
      2) pengendalian versi yaitu metode yang secara sistematis menyimpan kronologis dari salinan program yang disempurnakan dan menjadi salah satu dokumentasi dalam penyelenggaraan pengembangan; dan
   b. dokumentasi yang dilakukan terhadap sistem yang dikembangkan sendiri dan sistem yang dibeli atau dikembangkan oleh pihak penyedia jasa Teknologi Informasi yang mencakup deskripsi detail aplikasi, dokumentasi pemrograman, format yang digunakan, standar penamaan, dan petunjuk pelaksanaan bagi pengguna akhir.
8. Tahap pengujian sebagaimana dimaksud pada angka 3 huruf a angka 5) mencakup antara lain:
   a. *unit test*, yaitu uji coba yang dilakukan oleh pengembang atas fungsional setiap unit atau sub modul dari sistem yang telah selesai dikembangkan;
   b. *system integration test*, yaitu pengujian yang dilakukan oleh pengembang terhadap keseluruhan fungsional sistem setelah diintegrasikan menjadi satu kesatuan yang utuh;
   c. *stress test*, yaitu uji ketahanan yang dilakukan oleh pengembang terhadap kemampuan sistem dalam menangani proses atau transaksi dalam skala atau jumlah yang besar, yang kriteria lebih lanjut mengenai proses atau transaksi dalam skala atau jumlah yang besar dapat ditetapkan lebih lanjut oleh LJKNB; dan

---

[1] Kumpulan perangkat lunak atau data yang memiliki fungsi tertentu dan disimpan serta siap untuk digunakan.

d. *user acceptance test*, yaitu uji coba akhir yang dilakukan oleh pengguna akhir terhadap sistem yang telah selesai dikembangkan dalam rangka menguji fungsionalitas keseluruhan sistem, apakah telah sesuai dengan kebutuhan pengguna pada tahapan pendefinisian kebutuhan pengguna sebelum memutuskan implementasi dapat dilakukan.

9. Dalam hal hasil pengujian pada tahap *user acceptance test* sebagaimana dimaksud pada angka 8 huruf d telah sesuai dengan kebutuhan pengguna dan standar pengamanan LJKNB maka harus dibuat suatu berita acara yang disetujui pengguna akhir.

10. Tahap implementasi sebagaimana dimaksud pada angka 3 huruf a angka 6) harus memperhatikan antara lain:
    a. pengecekan integritas program berupa pengendalian yang memadai terhadap konversi dari kode sumber ke dalam sistem yang akan diimplementasikan;
    b. migrasi data dari sistem lama ke sistem baru;
    c. pengecekan akurasi dan keamanan data hasil migrasi pada sistem baru;
    d. kemungkinan diberlakukannya *parallel run*[2] antara sistem yang lama dengan yang baru, sampai dipastikan bahwa data pada sistem yang baru telah akurat dan andal;
    e. kepastian integritas data berupa keakuratan dan keandalan dari Pangkalan Data termasuk data yang tersimpan di dalamnya;
    f. perbaikan data dan referensi secara langsung (*patching data*) pada saat implementasi harus dihindari karena dapat memengaruhi integritas data pada Pangkalan Data di *server* produksi;
    g. pengaturan penyimpanan kode sumber dan Pangkalan Data dari sistem lama; dan
    h. antisipasi adanya kelemahan sistem operasi, sistem yang dikembangkan, Pangkalan Data dan jaringan, termasuk ancaman dari pihak yang tidak berwenang seperti *virus*[3]*, trojan*

---

[2] Salah satu strategi implementasi sistem di mana kedua sistem lama dan baru berjalan berdampingan sampai pengguna yakin bahwa sistem baru tidak memiliki masalah. Setelah periode waktu ketika sistem baru terbukti bekerja dengan benar, sistem lama akan dihapus sepenuhnya dan pengguna akan tergantung hanya pada sistem baru.

[3] Program yang bersifat merusak dan akan aktif dengan bantuan orang (dieksekusi) dan tidak dapat mereplikasi sendiri penyebarannya, karena dilakukan oleh orang, biasanya melalui attachement surat elektronik, game, atau program bajakan.

horse[4]*, worms*[5]*, spyware*[6]*, Denial-of-Service* (DoS)[7], *wardriving*, *spoofing*[8], dan *logic bomb*[9], dengan menguji dan menerapkan pengendalian pengamanan atas sistem yang akan diimplementasikan.

11. Tahap pengkajian ulang pasca implementasi sebagaimana dimaksud pada angka 3 huruf a angka 7) meliputi analisis atas:
    a. efektivitas aktivitas manajemen proyek dengan membandingkan antara lain rencana dan realisasi biaya, manfaat yang diperoleh, dan ketepatan jadwal proyek; dan
    b. kinerja sistem, permasalahan yang terjadi, dan langkah yang telah dilakukan untuk mengatasi permasalahan tersebut.
12. Hasil analisis sebagaimana dimaksud pada angka 11 didokumentasikan dan dilaporkan kepada manajemen.
13. Tahap pemeliharaan sebagaimana dimaksud pada angka 3 huruf a angka 8) dilakukan guna menetapkan metodologi pemeliharaan yang sesuai dengan karakteristik dan risiko tiap proyek dari sistem yang dimiliki LJKNB.
14. Tahap pemusnahan sebagaimana dimaksud pada angka 3 huruf a angka 9) merupakan proses terakhir dari pengembangan sistem dengan cara menghapus atau menghancurkan sistem termasuk data yang tidak dipergunakan lagi untuk menghindari penyalahgunaan oleh pihak yang tidak berwenang.
15. Pedoman pengadaan sebagaimana dimaksud pada angka 3 huruf b angka 1) harus memperhatikan antara lain:
    a. pengajuan atau usulan rencana pengadaan untuk mendapatkan persetujuan manajemen yang paling sedikit memuat analisis kebutuhan pengguna terhadap tujuan dan manfaat yang diharapkan, analisis biaya dan manfaat, serta manfaat dari

---

[4] Program yang bersifat merusak yang disusupkan oleh *hacker* di dalam program yang sudah dikenal oleh pengguna replikasi atau distribusinya harus diaktivasi oleh program yang sudah dikenal oleh penggunanya melalui metode *social engineering*.
[5] Program komputer yang dirancang untuk memperbanyak diri secara otomatis dan melekat pada surat elektronik atau sebagai bagian dari pesan jaringan.
[6] Perangkat lunak yang mengumpulkan informasi-informasi sensitif tentang pengguna tanpa sepengetahuan atau izin dari pengguna.
[7] Serangan terhadap sistem teknologi informasi sehingga menjadi lambat atau tidak dapat berfungsi sama sekali misalnya dengan membuat kapasitas (*bandwidth*) jaringan atau kapasitas (*disk space*) komputer seolah-olah telah terpakai penuh, gangguan pada *server* serta gangguan penyediaan jasa kepada sistem lain atau pengguna.
[8] Suatu keadaan dimana seseorang atau suatu program dapat menyerupai orang lain atau program lain dengan cara memalsukan data dengan tujuan untuk mendapatkan keuntungan-keuntungan tertentu.
[9] Suatu kode yang sengaja dimasukkan ke dalam suatu sistem perangkat lunak yang pada suatu kondisi tertentu akan melakukan serangkaian fungsi yang bersifat merusak.

sistem yang akan diadakan untuk mendukung kebutuhan bisnis LJKNB;

b. kesesuaian pihak penyedia jasa Teknologi Informasi, kontrak, lisensi, dan produk yang diperoleh terhadap kebutuhan penyelenggaraan Teknologi Informasi LJKNB;

c. kesesuaian spesifikasi penawaran yang diajukan oleh pihak penyedia jasa Teknologi Informasi dengan spesifikasi kebutuhan penyelenggaraan Teknologi Informasi di LJKNB;

d. perbandingan penawaran yang diajukan antar pihak penyedia jasa Teknologi Informasi; dan

e. kondisi keuangan pihak penyedia jasa Teknologi Informasi dan komitmen pihak penyedia jasa Teknologi Informasi terhadap pelayanan yang diberikan kepada LJKNB.

16. Kontrak pembelian dan lisensi sebagaimana dimaksud pada angka 3 huruf b angka 2) harus memperhatikan antara lain:

a. penjelasan tertulis bahwa penggunaan perangkat lunak bersifat eksklusif atau tidak;

b. informasi dan jumlah pengguna yang dapat menggunakan perangkat lunak;

c. daftar entitas terkait lainnya yang dapat menggunakan perangkat lunak tersebut, seperti perusahaan anak atau grup perusahaan;

d. informasi mengenai pengembangan perangkat lunak secara *inhouse* atau alih daya (*outsourcing*) oleh pihak penyedia jasa Teknologi Informasi, serta pembelian perangkat lunak disertai dengan kode sumbernya atau tidak, atau hanya berupa hak pakai atau sewa dengan pembatasan waktu atau fitur tertentu; dan

e. lokasi penggunaan, apakah lisensi lokasi penggunaan terbatas pada suatu lokasi atau tidak.

17. Pemeliharaan sebagaimana dimaksud pada angka 3 huruf b angka 3) mencakup paling sedikit:

a. pelatihan oleh pihak penyedia jasa Teknologi Informasi kepada LJKNB;

b. pihak penyedia jasa Teknologi Informasi memberikan dokumentasi perangkat lunak, termasuk petunjuk teknis penggunaan perangkat lunak;
c. pelaksanaan dan biaya pengkinian dan/atau modifikasi perangkat lunak;
d. kemungkinan LJKNB untuk mengakses kode sumber dalam hal pihak penyedia jasa Teknologi Informasi tidak dapat memberikan layanan lagi atau terdapat kebutuhan modifikasi yang tidak dapat dilakukan oleh pihak penyedia jasa Teknologi Informasi; dan
e. kemungkinan pihak penyedia jasa Teknologi Informasi untuk membantu proses konversi data pada saat penggantian sistem pada masa mendatang.

18. Garansi sebagaimana dimaksud pada angka 3 huruf b angka 4) memiliki aspek yang mencakup paling sedikit:
    a. tidak melanggar hak kekayaan intelektual dari pihak lainnya baik di dalam maupun luar negeri;
    b. tidak mengandung kode rahasia, pembatasan yang tidak diungkapkan, atau pembatasan secara otomatis pada perjanjian;
    c. berfungsi sesuai spesifikasi dan harus dinyatakan batasan tanggung jawab pihak penyedia jasa Teknologi Informasi dalam hal terjadi permasalahan;
    d. pemeliharaannya dilakukan oleh pihak penyedia jasa Teknologi Informasi selama jangka waktu yang diperjanjikan; dan
    e. tetap berlaku dalam hal terjadi penggabungan, peleburan, pengambilalihan, atau perubahan kepemilikan baik pada LJKNB atau pihak penyedia jasa Teknologi Informasi.
19. Penyelesaian perselisihan sebagaimana dimaksud pada angka 3 huruf b angka 5) mencakup paling sedikit klausula penyelesaian perselisihan pada perjanjian lisensi antara LJKNB dengan pihak penyedia jasa Teknologi Informasi.
20. Perubahan perjanjian sebagaimana dimaksud pada angka 3 huruf b angka 6) perlu didasari perjanjian yang memuat klausula yang secara jelas menyatakan bahwa pihak penyedia jasa Teknologi Informasi

tidak dapat memodifikasi perjanjian tanpa adanya persetujuan dari kedua belah pihak.

21. Keamanan sebagaimana dimaksud pada angka 3 huruf b angka 7) mencakup paling sedikit:
    a. tanggung jawab secara terus menerus dari pihak penyedia jasa Teknologi Informasi untuk melindungi keamanan dan kerahasiaan sumber daya Teknologi Informasi dan data LJKNB;
    b. larangan bagi pihak penyedia jasa Teknologi Informasi untuk menggunakan atau mengungkapkan informasi yang dimiliki LJKNB tanpa persetujuan LJKNB;
    c. jaminan dari pihak penyedia jasa Teknologi Informasi bahwa perangkat lunak tidak mengandung fitur yang dapat mengakses sistem dan/atau data tanpa proses autentifikasi (*back door*[10]) yang memungkinkan akses oleh pihak yang tidak berwenang ke dalam sistem dan data LJKNB; dan
    d. pernyataan secara eksplisit bahwa pihak penyedia jasa Teknologi Informasi tidak akan menggunakan fitur yang dapat mengakibatkan perangkat lunak tidak berfungsi dengan baik.
22. Pengalihan sebagian kegiatan (subkontrak) kepada pihak lain sebagaimana dimaksud pada angka 3 huruf b angka 8) mencakup paling sedikit klausula yang menyatakan bahwa pihak penyedia jasa Teknologi Informasi:
    a. hanya dapat melakukan pengalihan sebagian kegiatan (subkontrak) kepada pihak ketiga berdasarkan persetujuan LJKNB yang dibuktikan dengan dokumen tertulis; dan
    b. bertanggung jawab terhadap perangkat lunak meskipun perangkat lunak dirancang dan/atau dikembangkan oleh pihak lain.
23. Kebijakan dan prosedur aspek operasional Teknologi Informasi sebagaimana dimaksud pada angka 1 huruf c mencakup paling sedikit:
    a. Kebijakan dan prosedur pengelolaan data, yang paling sedikit terdiri atas:

---

[10] Metode untuk melewati otentikasi normal atau remote access yang aman dari suatu komputer terhadap pengaksesan suatu sistem namun tidak teridentifikasi melalui pemeriksaan biasa.

1) pengelolaan Pusat Data, bagi LJKNB yang dikenai kewajiban kepemilikan Pusat Data;
2) pengelolaan Pusat Pemulihan Bencana, bagi LJKNB yang dikenai kewajiban kepemilikan Pusat Pemulihan Bencana; dan
3) pengelolaan Pangkalan Data;

b. Kebijakan dan prosedur terkait pengelolaan perubahan, yang paling sedikit terdiri atas:
1) pengendalian perubahan, yaitu setiap perubahan pada sumber daya Teknologi Informasi yang terjadi dan/atau dimungkinkan terjadi perlu dikendalikan dengan baik melalui fungsi pengawasan yang terkoordinasi dengan melibatkan satuan kerja terkait;
2) manajemen pengkinian perangkat lunak, yaitu LJKNB harus memiliki dokumentasi yang lengkap tentang instalasi perangkat lunak terbaru yang dilakukan sehingga dapat mengetahui informasi terkini mengenai perbaikan produk, masalah keamanan, *patch*[11] atau *upgrade*, atau permasalahan lain yang sesuai dengan versi perangkat lunak yang digunakan; dan
3) migrasi data, dalam hal LJKNB melakukan perubahan yang mendasar atau besar terhadap perangkat lunak dan/atau perangkat keras yang mengakibatkan terjadinya migrasi data maka LJKNB perlu memiliki kebijakan dan prosedur mengenai penanganan migrasi data;

c. penanganan kejadian atau permasalahan, dimana LJKNB harus memelihara sarana yang diperlukan untuk menangani permasalahan yang paling sedikit terdiri atas:
1) fungsi *helpdesk,* yang bertugas menanggapi dan menangani permasalahan terkait Teknologi Informasi di LJKNB; dan
2) penanganan penggunaan *super user*[12] yaitu pengguna yang memiliki kewenangan sangat luas, yang berisi paling sedikit mengenai:

---

[11] Sekumpulan kode yang ditambahkan pada perangkat lunak untuk memperbaiki suatu kesalahan, biasanya merupakan koreksi yang bersifat sementara di antara dua keluaran versi perangkat lunak.
[12] *User id* yang memiliki kewenangan sangat luas.

a) penetapan dan kriteria pihak yang memiliki hak akses *super user*;

b) mekanisme pengelolaan *password*[13] *super user* yang meliputi penyimpanan dan penggantian *password*;

d. pengendalian pertukaran informasi, yang paling sedikit terdiri atas:

1) permintaan dan pemberian informasi oleh pihak internal dan eksternal; dan

2) pengiriman informasi melalui media seperti surat elektronik, diska lepas (*flashdisk*), cakram padat (*compact disk*), salinan cetak (*hardcopy*);

e. fungsi kendali mutu, yang berfungsi untuk melakukan penilaian kualitas perangkat lunak dan perangkat keras; dan

f. mekanisme pemusnahan serta penghapusan perangkat lunak dan perangkat keras.

24. Dalam menyusun kebijakan dan prosedur mengenai pengelolaan Pusat Data sebagaimana dimaksud pada angka 23 huruf a angka 1), LJKNB harus memperhatikan hal-hal berikut:

a. bangunan harus:

1) berada dalam lokasi yang aman secara geografis; dan

2) memiliki akses jalan darat yang memadai;

b. akses fisik ke Pusat Data harus dibatasi dan dikendalikan dengan baik;

c. pengendalian faktor lingkungan antara lain:

1) memastikan tersedianya sumber listrik yang cukup, stabil, dan tersedianya sumber alternatif listrik untuk mengantisipasi tidak berfungsinya sumber listrik utama;

2) memastikan tersedianya alat detektor api dan asap, alat pemadam api, alat pengukur suhu dan kelembaban, dan pipa pembuangan air;

3) memperhatikan tata ruang diantaranya:

a) menghindari penempatan ruangan di bawah area perpipaan seperti kamar mandi dan dapur;

---

[13] Kode atau simbol khusus untuk mengamankan sistem komputer yaitu untuk mengidentifikasi pihak yang mengakses data, program atau aplikasi komputer yang digunakan.

b) menghindari penggunaan jendela ruangan yang secara langsung menghadap ke sinar matahari, kecuali jendela ruangan tersebut memiliki media penutup yang memadai untuk mencegah paparan sinar matahari ke dalam ruangan;
c) penggunaan lantai yang ditinggikan;
d) ketersediaan pintu darurat; dan
e) manajemen perangkat pendukung seperti ketersediaan rak dengan bahan yang tidak mudah terbakar, penempatan kabel dan infrasturuktur jaringan lainnya, dan lain-lain;

d. aktivitas operasional Pusat Data antara lain terkait:
1) penjadwalan tugas yang harus dilaksanakan pada Pusat Data harus dipastikan berjalan secara efektif dan aman dari perubahan yang tidak sah;
2) pengoperasian tugas oleh operator Teknologi Informasi harus dibatasi sesuai kewenangan;
3) pendistribusian hasil informasi yang diproduksi oleh sistem (*output)* harus dilakukan dengan aman untuk menghindari terbukanya informasi yang rahasia;
4) proses rekam cadang;
5) pemantauan terhadap perangkat keras dan perangkat lunak; dan
6) pengaktifan jejak audit, dan

e. perjanjian dengan pihak penyedia jasa Teknologi Informasi, dalam hal penyediaan dan pengelolaan Pusat Data dilakukan oleh pihak penyedia jasa Teknologi Informasi yang menyangkut kinerja, reputasi pihak penyedia jasa, dan kelangsungan penyediaan layanan.

25. Dalam menyusun kebijakan dan prosedur mengenai pengelolaan Pusat Pemulihan Bencana sebagaimana dimaksud pada angka 23 huruf a angka 2), LJKNB harus memperhatikan hal-hal berikut:
a. penempatan Pusat Pemulihan Bencana tidak berlokasi di wilayah rawan gempa, banjir, atau petir dan terhubung dengan infrastruktur komunikasi dan listrik yang berbeda dengan Pusat

Data, serta fasilitas lain yang diperlukan untuk tetap berjalannya suatu sistem;

b. sistem di Pusat Pemulihan Bencana harus kompatibel dengan sistem yang digunakan pada Pusat Data dan harus disesuaikan jika terjadi perubahan pada Pusat Data;

c. memperhitungkan waktu tempuh untuk terjaminnya proses *recovery*; dan

d. perjanjian dengan pihak penyedia jasa Teknologi Informasi, dalam hal penyediaan dan pengelolaan Pusat Pemulihan Bencana dilakukan oleh pihak penyedia jasa Teknologi Informasi yang menyangkut kinerja, reputasi pihak penyedia jasa, dan kelangsungan penyediaan layanan.

26. Dalam menyusun kebijakan dan prosedur mengenai pengelolaan Pangkalan Data sebagaimana dimaksud pada angka 23 huruf a angka 3), LJKNB harus memperhatikan hal-hal berikut:

a. ketersediaan sumber daya manusia yang memiliki kompetensi dalam pengelolaan Pangkalan Data khususnya terkait pengaksesan, pemeliharaan, penanganan permasalahan, dan administrasi Pangkalan Data; dan

b. terdapat mekanisme rekam cadang data dimana:

1) lokasi rekam cadang data harus disimpan di lingkungan yang aman dan memiliki lokasi yang berbeda dari lokasi Pusat Data;

2) rekam cadang data dilakukan secara menyeluruh (*full system backup*) dan berkala atau dilakukan dalam hal terjadi perubahan sistem yang mendasar;

3) rekam cadang data harus memenuhi standar sistem pengamanan yang memadai;

4) harus dilakukan uji *restore* secara berkala untuk memastikan rekam cadang data dapat digunakan pada saat diperlukan (kondisi darurat); dan

5) terdapat mekanisme pemusnahan dan/atau penghapusan media rekam cadang data.

27. Kebijakan dan prosedur aspek jaringan komunikasi sebagaimana dimaksud pada angka 1 huruf d mencakup paling sedikit:

a. pengukuran kinerja dan perencanaan kapasitas jaringan;

b. pengamanan jaringan;
c. manajemen jaringan;
d. prosedur penanganan masalah jaringan;
e. mekanisme penggunaan jaringan komunikasi antara lain terkait jaringan internet, intranet, dan jaringan tanpa kabel;
f. prosedur penyelesaian masalah;
g. fasilitas untuk rekam cadang dan pemulihan; dan
h. perjanjian dan kontrak yang memuat pemenuhan tingkat layanan sesuai dengan *service level agreement* dengan pihak penyedia jasa Teknologi Informasi, dalam hal penyediaan dan pengelolaan jaringan komunikasi dilakukan oleh pihak penyedia jasa Teknologi Informasi.

28. Kebijakan aspek pengamanan informasi sebagaimana dimaksud pada angka 1 huruf e meliputi paling sedikit:
    a. tujuan pengamanan informasi;
    b. komitmen manajemen terhadap pengamanan informasi;
    c. kerangka acuan dalam menetapkan pengendalian dan penanganan permasalahan pengamanan informasi;
    d. kepatuhan terhadap ketentuan internal dan ketentuan peraturan perundang-undangan mengenai pengamanan informasi;
    e. pelatihan dan peningkatan kesadaran atas pentingnya pengamanan informasi;
    f. tugas dan tanggung jawab pihak-pihak dalam pengamanan informasi;
    g. analisis dampak pengamanan informasi terhadap kelangsungan bisnis dan kegiatan usaha LJKNB;
    h. sanksi atas pelanggaran kebijakan pengamanan informasi; dan
    i. dokumen atau ketentuan lain yang mendukung kebijakan pengamanan informasi.
29. Prosedur aspek pengamanan informasi sebagaimana dimaksud pada angka 1 huruf e meliputi paling sedikit:
    a. pengelolaan aset, yang meliputi paling sedikit:
        1) aset LJKNB yang terkait dengan informasi dilakukan identifikasi, ditentukan pemilik/penanggungjawabnya, dan dicatat agar dapat dilindungi secara tepat;

2) aset yang terkait dengan informasi dapat berupa data (*hardcopy* atau *softcopy)*, perangkat lunak, perangkat keras, jaringan, peralatan pendukung (misalnya sumber daya listrik dan *air conditioner*), dan sumber daya manusia termasuk kualifikasi dan keterampilan; dan

3) informasi perlu diklasifikasikan agar dapat dilakukan pengamanan yang memadai sesuai dengan klasifikasinya.
Contoh klasifikasi:
   a) informasi rahasia, misalnya data dan/atau informasi pribadi konsumen;
   b) informasi internal, misalnya peraturan mengenai kepegawaian; dan
   c) informasi biasa, misalnya informasi produk keuangan yang ditawarkan kepada konsumen;

b. pengelolaan sumber daya manusia, yang meliputi paling sedikit:
   1) sumber daya manusia baik pegawai LJKNB, konsultan, pegawai honorer, dan pegawai dari pihak penyedia jasa Teknologi Informasi yang memiliki akses terhadap informasi harus memahami tanggung jawab terhadap pengamanan informasi;
   2) peran dan tanggung jawab sumber daya manusia baik pegawai LJKNB, konsultan, pegawai honorer, dan pegawai dari pihak penyedia jasa Teknologi Informasi yang memiliki akses terhadap informasi harus didefinisikan dan didokumentasikan sesuai dengan kebijakan pengamanan informasi;
   3) dalam perjanjian kerja sama atau kontrak dengan pegawai LJKNB, konsultan, pegawai honorer, dan pegawai dari pihak penyedia jasa Teknologi Informasi harus tercantum ketentuan mengenai pengamanan informasi yang sesuai dengan kebijakan pengamanan informasi LJKNB. Sebagai contoh, perlu adanya klausula yang menyatakan bahwa pegawai LJKNB, konsultan, pegawai honorer, dan pegawai dari pihak penyedia jasa Teknologi Informasi harus menjaga kerahasiaan informasi yang diperolehnya sesuai dengan klasifikasi informasi;

4) selain perjanjian kerja sama antara LJKNB dengan pihak penyedia jasa Teknologi Informasi, semua pegawai dari pihak penyedia jasa Teknologi Informasi yang ditugaskan di LJKNB harus menandatangani suatu perjanjian menjaga kerahasiaan informasi (*non-disclosure agreement*);
5) pelatihan dan/atau sosialisasi tentang pengamanan informasi harus diberikan kepada pegawai LJKNB, konsultan, pegawai honorer, dan pegawai dari pihak penyedia jasa Teknologi Informasi. Pelatihan dan/atau sosialisasi ini diberikan sesuai dengan peran dan tanggung jawab masing-masing pihak;
6) LJKNB menetapkan sanksi atas pelanggaran terhadap kebijakan pengamanan informasi;
7) LJKNB menetapkan prosedur yang mengatur tentang keharusan bagi pegawai LJKNB, konsultan, pegawai honorer dan pegawai dari pihak penyedia jasa Teknologi Informasi untuk mengembalikan aset dan perubahan/penutupan hak akses yang disebabkan karena perubahan tugas atau selesainya masa kerja atau kontrak; dan
8) LJKNB menetapkan pemisahan tugas dan tanggung jawab terkait pengamanan informasi, yaitu memastikan terdapat pemisahan tugas dan tanggung jawab antara sumber daya manusia di operasional LJKNB;

c. pengamanan fisik dan lingkungan, yang meliputi paling sedikit:
1) fasilitas pemrosesan informasi yang penting (misalnya perangkat komputer dan perangkat jaringan) diberikan pengamanan fisik dan lingkungan yang memadai untuk mencegah akses yang tidak terotorisasi, kerusakan, dan gangguan lain;
2) pengamanan fisik dan lingkungan terhadap fasilitas pemrosesan informasi yang penting meliputi antara lain pembatas ruangan, pengendalian akses masuk misalnya penggunaan *access control card*[14], *personal identification*

[14] Perangkat elektronik yang digunakan unttuk memberikan pengamanan akses lingkungan dengan menggunakan kartu.

number[15], atau *biometrics*[16], kelengkapan alat pengamanan di dalam ruangan (misalnya alarm, pendeteksi dan pemadam api, pengukur suhu dan kelembaban udara, atau CCTV) dan pemeliharaan kebersihan ruangan dan peralatan (misalnya dari debu, rokok, makanan, minuman, atau barang mudah terbakar);

3) fasilitas pendukung seperti *air conditioner* dan sumber daya listrik harus dipastikan kapasitas dan ketersediaannya dalam mendukung operasional fasilitas pemrosesan informasi;

4) aset milik penyedia jasa Teknologi Informasi harus diidentifikasikan secara jelas dan diberikan perlindungan yang memadai misalnya dengan menerapkan pengamanan yang cukup, *dual control*[17], atau menempatkan secara terpisah dari aset milik LJKNB; dan

5) pemeliharaan dan pemeriksaan secara berkala terhadap fasilitas pemrosesan informasi dan fasilitas pendukung sesuai dengan prosedur yang telah ditetapkan;

d. pengendalian akses, yang meliputi paling sedikit;

1) pengendalian akses fisik dan *logic*[18];

2) prosedur formal secara tertulis yang telah disetujui oleh manajemen tentang pengadministrasian pengguna yang meliputi pendaftaran, perubahan, dan penghapusan pengguna, baik untuk pengguna internal maupun eksternal LJKNB;

3) pemberian akses mengacu kepada prinsip berdasarkan kebutuhan bisnis dan dengan akses yang seminimal mungkin;

4) penerapan metode identifikasi dan otentikasi sesuai analisis risiko antara lain dapat berupa satu atau kombinasi dari "*what you know*" (antara lain *password*), "*what you have*" (antara lain telepon genggam, kartu

---

[15] Rangkaian digit unik terdiri dari huruf, angka atau kode ASCII yang digunakan untuk mengidentifikasi antara lain pengguna komputer, pengguna ATM, pengguna internet banking, dan pengguna mobile banking.
[16] Pemanfaatan teknologi dengan cara mengidenfitikasi ciri biologis seseorang.
[17] Pengamanan yang dilakukan secara berlapis dengan melibatkan persetujuan 2 (dua) orang atau lebih.
[18] Prinsip dasar dalam pemrosesan secara otomatis

magnetis dengan chip, dan/atau token), "*something you are*" (antara lain *biometric* seperti retina dan sidik jari);

5) prosedur pengendalian melalui pemberian *password* awal (*initial password*) kepada pengguna dengan memperhatikan paling sedikit hal–hal sebagai berikut:
   a) *password* awal harus diganti saat *log-in*[19] pertama kali;
   b) *password* awal diberikan secara aman, misalnya melalui amplop tertutup atau kertas karbon berlapis dua sehingga hanya diketahui oleh pihak yang berhak;
   c) *password* awal bersifat khusus atau unik untuk setiap pengguna dan tidak mudah ditebak;
   d) pemilik *user-id*[20] terutama dari pegawai LJKNB, pegawai honorer, dan pegawai dari pihak penyedia jasa Teknologi Informasi harus menandatangani pernyataan tanggung jawab atau perjanjian penggunaan *user-id* dan *password* saat menerima *user-id* dan *password*; dan
   e) *password* standar (*default password*) yang dimiliki oleh sistem operasi, sistem aplikasi, *database management system*, dan perangkat jaringan diganti oleh LJKNB sebelum diimplementasikan dan sedapat mungkin mengganti *user-id* standar dari sistem (*default user-id*);
6) prosedur yang mewajibkan pengguna untuk:
   a) menjaga kerahasiaan *password*;
   b) menghindari penulisan *password* di kertas dan tempat lain tanpa pengamanan yang memadai;
   c) menggunakan *password* yang berkualitas, yaitu:
      (1) panjang *password* yang memadai sehingga tidak mudah ditebak;
      (2) mudah diingat dan terdiri dari paling sedikit kombinasi 2 tipe karakter (huruf, angka, atau karakter khusus);

---

[19] Proses untuk masuk ke dalam layanan *online* dengan cara memasukkan identitas pengguna untuk mendapatkan hak akses.
[20] Identitas yang dimiliki pengguna yang digunakan untuk masuk ke dalam layanan online.

(3) tidak didasarkan atas data pribadi pengguna seperti nama, nomor telepon, atau tanggal lahir; dan

(4) tidak menggunakan kata yang umum dan mudah ditebak oleh perangkat lunak (untuk menghindari *brute force attack*), misalnya kata 'pass', 'password', 'adm', atau kata umum di kamus;

d) mengubah *password* secara berkala; dan

e) menghindari penggunaan *password* yang sama secara berulang;

7) prosedur untuk menonaktifkan hak akses jika *user-id* tidak digunakan pada waktu tertentu, menetapkan jumlah maksimal kegagalan *password*, dan menonaktifkan pengguna setelah mencapai jumlah maksimal kegagalan *password*;

8) prosedur kaji ulang secara berkala oleh satuan kerja yang tidak terlibat dalam operasional pengendalian akses, terhadap hak akses pengguna untuk memastikan bahwa hak akses sesuai dengan wewenang yang diberikan;

9) sistem operasi, sistem aplikasi, Pangkalan Data, utilitas, dan perangkat lainnya yang dimiliki oleh LJKNB dapat membantu pelaksanaan pengamanan *password*, sebagai contoh:

a) memaksa pengguna untuk mengubah *password* setelah jangka waktu tertentu dan menolak apabila pengguna memasukkan *password* yang sama dengan yang digunakan sebelumnya saat mengganti *password*;

b) menyimpan *password* secara aman (terenkripsi);

c) memutuskan hubungan atau akses pengguna jika tidak terdapat respon selama jangka waktu tertentu;

d) menonaktifkan atau menghapus hak akses pengguna jika pengguna tidak melakukan *log-in* melebihi jangka waktu tertentu misalnya karena cuti, rotasi, dan/atau mutasi; dan

e) prosedur pembatasan akses paling sedikit melalui penggunaan password dan pengaturan pihak yang berwenang melakukan akses bagi LJKNB yang menggunakan *file sharing*;

e. pengamanan operasional Teknologi Informasi, yang meliputi paling sedikit:
   1) ketersediaan rekam cadang dan prosedur pemulihan yang teruji sesuai dengan tingkat kepentingannya bagi data, informasi, dan perangkat lunak yang telah dibuat;
   2) adanya proses antisipasi dan pengendalian pengamanan yang memadai atas kelemahan sistem operasi, sistem aplikasi, Pangkalan Data, dan jaringan, antara lain ancaman dari pihak yang tidak berwenang seperti *virus, trojan horse, worms, spyware, Denial-of-Service (DoS), war driving, spoofing*, dan *logic bomb*;
   3) perlindungan terhadap jejak audit atau *log* dari gangguan dan akses tidak sah;
   4) sinkronisasi antara penunjuk waktu dari seluruh Sistem Elektronik LJKNB dengan sumber penunjuk waktu akurat yang disepakati; dan
   5) pemeliharaan catatan perangkat lunak yang digunakan dan pemantauan secara berkala atas Sistem Elektronik dan kemungkinan permasalahan yang timbul;
f. pemantauan pengamanan informasi yang dilakukan sesuai dengan risiko atau tingkat kritikalitas informasi; dan
g. penanganan insiden dalam pengamanan informasi, yang meliputi paling sedikit;
   1) cakupan penanganan insiden yang meliputi paling sedikit:
      a) pihak yang harus melaporkan insiden;
      b) jenis insiden yang harus dilaporkan;
      c) alur pelaporan insiden;
      d) analisis atas insiden; dan
      e) pendokumentasian bukti terkait insiden dan tindak lanjut yang akan dilakukan; dan
   2) identifikasi, pelaporan, pemrosesan tindak lanjut, dokumentasi, dan evaluasi atas insiden yang terjadi.

30. Kebijakan dan prosedur aspek Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 1 huruf f mencakup paling sedikit:
    a. analisis terhadap Rencana Pemulihan Bencana;
    b. jenis prosedur Rencana Pemulihan Bencana;
    c. komponen prosedur Rencana Pemulihan Bencana;
    d. penetapan kejelasan tanggung jawab bagi pihak terkait dalam penyelenggaraan Rencana Pemulihan Bencana;
    e. uji coba Rencana Pemulihan Bencana; dan
    f. pengkinian Rencana Pemulihan Bencana.
31. Analisis terhadap Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 30 huruf a merupakan analisis terhadap kemungkinan timbulnya risiko yang dapat disebabkan oleh faktor antara lain:
    a. faktor kebakaran;
    b. faktor bencana alam seperti banjir dan gempa;
    c. faktor gangguan teknis seperti kerusakan perangkat keras, perangkat lunak, gangguan listrik, gangguan transmisi data, dan
    d. faktor manusia seperti kesalahan manusia (*human erro*r) dan/atau sabotase.
32. Jenis prosedur Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 30 huruf b paling sedikit mencakup:
    a. prosedur tanggap darurat, untuk mengendalikan sistem pada saat terjadi gangguan/bencana, mengurangi dampak kerugian, serta menentukan status keadaan bencana;
    b. prosedur pemulihan sistem yang memungkinkan kegiatan operasional LJKNB dapat kembali ke kondisi normal; dan
    c. prosedur sinkronisasi data digunakan untuk memastikan kesamaan antara data mesin yang digunakan untuk operasional dengan rekam cadang data, serta untuk memastikan semua data hasil pemrosesan bisnis selama masa pemulihan telah masuk ke dalam sistem.
33. Komponen prosedur Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 30 huruf c mencakup paling sedikit:

a. sumber daya manusia, yaitu Rencana Pemulihan Bencana harus dapat menjelaskan komposisi, wewenang, dan tanggung jawab setiap sumber daya manusia yang berkaitan dengan penyelenggaraan Teknologi Informasi dan memiliki alur komunikasi yang memadai;
b. sumber daya Teknologi Informasi dan aplikasi inti LJKNB, yaitu LJKNB harus memiliki prosedur dan dokumentasi yang lengkap untuk memulihkan aplikasi utama yang terkait dengan kegiatan usaha LJKNB maupun operasional LJKNB lainnya; dan
c. fasilitas komunikasi, guna memastikan tersedianya alternatif jalur komunikasi yang dapat digunakan di lingkungan internal dan/atau eksternal pada saat terjadinya gangguan atau bencana.

34. Penetapan kejelasan tanggung jawab bagi pihak terkait dalam penyelenggaraan Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 30 huruf d meliputi paling sedikit mengenai tanggung jawab:
    a. manajemen;
    b. satuan kerja penyelenggara Teknologi Informasi; dan
    c. satuan kerja pendukung, seperti satuan kerja yang membawahkan fungsi logistik.
35. Tanggung jawab manajemen sebagaimana dimaksud pada angka 34 huruf a mencakup paling sedikit:
    a. menetapkan kebijakan dan prosedur tertulis Rencana Pemulihan Bencana;
    b. menelaah dan menyetujui Rencana Pemulihan Bencana;
    c. melakukan evaluasi terhadap kelayakan Rencana Pemulihan Bencana milik pihak penyedia jasa Teknologi Informasi, dalam hal LJKNB menggunakan jasa pihak penyedia jasa Teknologi Informasi; dan
    d. menetapkan tingkat gangguan dan bencana serta pemulihannya.
36. Tanggung jawab satuan kerja penyelenggaraan Teknologi Informasi sebagaimana dimaksud pada angka 34 huruf b mencakup paling sedikit:
    a. efektivitas penyelenggaraan Rencana Pemulihan Bencana;

b. penentuan skenario pemulihan yang akan digunakan apabila terjadi gangguan atau bencana berdasarkan prioritisasi atas sistem yang dianggap kritis; dan
c. evaluasi laporan mengenai setiap tahapan dalam pengujian dan pelaksanaan Rencana Pemulihan Bencana.

37. Tanggung jawab satuan kerja pendukung sebagaimana dimaksud pada angka 34 huruf c mencakup paling sedikit:
    a. penerapan Rencana Pemulihan Bencana; dan
    b. mendukung satuan kerja yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi.
38. Uji coba Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 30 huruf e mencakup paling sedikit:
    a. frekuensi uji coba;
    b. ruang lingkup uji coba;
    c. skenario uji coba; dan
    d. analisis, laporan, dan dokumentasi hasil uji coba.
39. Dalam hal LJKNB menggunakan pihak penyedia jasa Teknologi Informasi, pelaksanaan uji coba Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 30 huruf e harus melibatkan pihak penyedia jasa Teknologi Informasi yang bersangkutan.
40. LJKNB harus melakukan pengkinian Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 30 huruf f untuk meyakinkan kesesuaian proses bisnis, sumber daya manusia, dan sumber daya Teknologi Informasi dengan kondisi eksternal dan/atau internal saat ini dan mendatang.
41. Kebijakan dan prosedur aspek penggunaan pihak penyedia jasa Teknologi Informasi sebagaimana dimaksud pada angka 1 huruf g mencakup paling sedikit:
    a. penetapan kriteria penggunaan pihak penyedia jasa Teknologi Informasi, yang berisi paling sedikit mengenai kriteria penyelenggaraan Teknologi Informasi yang dapat dilakukan secara mandiri (*inhouse*) atau melalui pihak penyedia jasa Teknologi Informasi;
    b. prinsip penggunaan pihak penyedia jasa Tekonologi Informasi, yang paling sedikit berisi informasi mengenai:
        1) persetujuan dari manajemen;

2) tanggung jawab tetap berada pada LJKNB;
3) tidak menghambat proses pengawasan oleh Otoritas Jasa Keuangan;
4) kerja sama yang dilakukan harus dituangkan dalam perjanjian tertulis;
5) ruang lingkup perjanjian kerja sama, yang berisi paling sedikit tentang:
    a) cakupan pekerjaan;
    b) biaya dan jangka waktu perjanjian kerja sama;
    c) kepemilikan dan hak cipta;
    d) batasan risiko yang ditanggung oleh LJKNB dan pihak penyedia jasa Teknologi Informasi, termasuk yang diakibatkan perubahan antara lain:
        (1) ruang lingkup perjanjian kerja sama;
        (2) ruang lingkup bisnis dan organisasi pihak penyedia jasa Teknologi Informasi; dan
        (3) aspek hukum antara lain regulasi, hak cipta, dan paten;
    e) larangan bagi pihak penyedia jasa Teknologi Informasi untuk menggunakan atau mengungkapkan informasi yang dimiliki LJKNB;
    f) *service level agreement* yang memuat standar kinerja dari pihak penyedia jasa Teknologi Informasi antara lain mengenai tingkat pelayanan yang diperjanjikan dan target kinerja;
    g) klausula yang menyatakan bahwa:
        (1) *service level agreement* tetap berlaku dalam hal terjadi perubahan kepemilikan pada LJKNB atau pihak penyedia jasa Teknologi Informasi;
        (2) pihak penyedia jasa Teknologi Informasi tidak dapat memodifikasi perangkat lunak yang telah disepakati dalam perjanjian tanpa persetujuan dari kedua belah pihak;
        (3) pihak penyedia jasa Teknologi Informasi harus melakukan *transfer of knowledge* kepada LJKNB;

(4) terdapat jaminan yang menyatakan bahwa pihak penyedia jasa Teknologi Informasi tetap mendukung jasa yang diberikan kepada LJKNB selama jangka waktu tertentu setelah implementasi;

(5) hanya dapat melakukan pengalihan sebagian kegiatan (subkontrak) berdasarkan persetujuan LJKNB yang dibuktikan dengan dokumen tertulis;

(6) tidak berkeberatan dalam hal Otoritas Jasa Keuangan dan/atau pihak lain yang sesuai dengan ketentuan peraturan perundang-undangan berwenang untuk melakukan pemeriksaan, akan melakukan pemeriksaan terhadap kegiatan penyediaan jasa Teknologi Informasi yang diberikan; dan

(7) kemungkinan menghentikan, mengubah, membuat perjanjian baru, atau mengambil alih kegiatan yang diselenggarakan oleh pihak penyedia jasa Teknologi Informasi, serta mengakhiri perjanjian sebelum jangka waktu berakhirnya perjanjian, termasuk dalam hal ini atas permintaan Otoritas Jasa Keuangan;

h) jaminan ketersediaan akses ke kode sumber dalam hal:

(1) perangkat lunak dinilai penting oleh LJKNB;

(2) diperlukan modifikasi yang tidak dapat dilakukan oleh pihak penyedia jasa Teknologi Informasi; dan/atau

(3) penyedia jasa Teknologi Informasi tidak dapat memberikan layanan lagi;

i) kesediaan pihak penyedia jasa Teknologi Informasi untuk memberikan dokumen teknis kepada LJKNB terkait dengan jasa yang dikerjakan oleh pihak penyedia jasa Teknologi Informasi antara lain mengenai diagram alur (*flowchart*) dan petunjuk pelaksanaan (*manual book*) dari perangkat lunak;

j) sanksi dan/atau penalti terhadap pembatalan dan/atau pelanggaran perjanjian kerja sama; dan

k) kepatuhan terhadap ketentuan dan peraturan perundang-undangan termasuk penyelesaian sengketa dalam hal terjadi perselisihan;

6) mekanisme uji tuntas, yang meliputi analisis paling sedikit atas:

a) eksistensi, riwayat, kualifikasi, latar belakang, dan reputasi pihak penyedia jasa Teknologi Informasi;

b) kondisi keuangan pihak penyedia jasa Teknologi Informasi;

c) kemampuan dan efektivias pemberian jasa, termasuk dukungan purna jual; dan

d) penerapan manajemen risiko pihak penyedia jasa Teknologi Informasi; dan

7) penggunaan pihak penyedia jasa Teknologi Informasi harus memberikan manfaat yang lebih besar dibandingkan dengan biaya yang dikeluarkan LJKNB; dan

c. penentuan pihak penyedia jasa Teknologi Informasi, yang berisi paling sedikit mengenai mekanisme seleksi.

42. Kebijakan dan prosedur aspek Layanan Keuangan Elektronik sebagaimana dimaksud pada angka 1 huruf h memuat paling sedikit:

a. cakupan dan deskripsi Layanan Keuangan Elektronik; dan

b. tanggung jawab dan kewenangan pengelolaan Layanan Keuangan Elektronik.

VI. KECUKUPAN PROSES IDENTIFIKASI, PENGUKURAN, PENGENDALIAN, DAN PEMANTAUAN RISIKO PENGGUNAAN TEKNOLOGI INFORMASI

1. Proses identifikasi, pengukuran, pengendalian, dan pemantauan risiko dilakukan paling sedikit terhadap aspek:

a. manajemen;

b. pengembangan dan pengadaan

c. operasional Teknologi Informasi;

d. jaringan komunikasi;

e. pengamanan informasi;

f. Rencana Pemulihan Bencana;

g. penggunaan pihak penyedia jasa Teknologi Informasi; dan
h. Layanan Keuangan Elektronik, bagi LJKNB yang menyelenggarakan Layanan Keuangan Elektronik.

2. LJKNB harus memiliki pendekatan manajemen risiko yang terpadu atau terintegrasi untuk dapat melakukan identifikasi, pengukuran, pengendalian, dan pemantauan risiko secara efektif.
3. Proses identifikasi risiko sebagaimana dimaksud pada angka 1 mencakup paling sedikit langkah sebagai berikut:
   a. pengumpulan data atau informasi mengenai aktivitas terkait penyelenggaraan Teknologi Informasi yang berpotensi menimbulkan atau meningkatkan risiko, baik dari kegiatan yang sedang atau yang akan berjalan, antara lain data atau informasi yang berasal dari:
      1) sumber daya Teknologi Informasi yang kritikal;
      2) pengaduan atau keluhan yang disampaikan pengguna Teknologi Informasi kepada satuan kerja penyelenggara Teknologi Informasi dan/atau *help desk*;
      3) temuan audit terkait penyelenggaraan Teknologi Informasi;
      4) hasil uji tuntas terhadap kinerja pihak penyedia jasa Teknologi Informasi; dan
      5) hasil penilaian sendiri yang dilakukan oleh satuan kerja penyelenggara Teknologi Informasi terkait penyelenggaraan Teknologi Informasi, jika ada; dan
   b. analisis risiko yang berkaitan dengan dampak potensial dari setiap risiko, antara lain *fraud* pada pemrograman, kegagalan sistem, bencana alam, kesalahan pemilihan teknologi yang digunakan, dan kemungkinan atas munculnya *virus*, *trojan horse, worms, spyware, Denial-of-Service (DoS), war driving,* dan *spoofing*.
4. Proses pengukuran risiko sebagaimana dimaksud pada angka 1 dapat dilakukan secara kuantitatif dan/atau kualitatif, berupa metode yang ditetapkan oleh Otoritas Jasa Keuangan dan/atau regulator lain dalam rangka penilaian risiko maupun metode yang dikembangkan sendiri oleh LJKNB.
5. Proses pengukuran risiko harus secara jelas memuat proses validasi, frekuensi validasi, persyaratan dokumentasi data dan informasi,

persyaratan evaluasi terhadap asumsi yang digunakan, sebelum suatu model diaplikasikan oleh LJKNB.

6. Proses pengendalian risiko sebagaimana dimaksud pada angka 1 memperhatikan kategori berikut:
   a. *accept*, yaitu LJKNB memutuskan untuk menerima risiko jika besarnya dampak yang ditimbulkan masih dalam batas toleransi;
   b. *control*, yaitu LJKNB memutuskan untuk mengurangi dampak yang ditimbulkan maupun kemungkinan terjadinya risiko;
   c. *avoid*, yaitu LJKNB memutuskan untuk tidak melakukan suatu aktivitas atau memilih alternatif aktivitas lain yang menghasilkan *output* yang sama untuk menghindari terjadinya risiko; atau
   d. *transfer*, yaitu LJKNB memutuskan untuk mengalihkan seluruh atau sebagian tanggung jawab penyelenggaraan Teknologi Informasi kepada pihak penyedia jasa Teknologi Informasi.
7. LJKNB harus mengambil langkah penanganan terhadap proses pengendalian Risiko untuk setiap kategori sebagaimana dimaksud pada angka 6 termasuk pencegahan terjadinya kerugian risiko yang lebih besar.
8. Pengendalian risiko dapat dilakukan oleh LJKNB, antara lain dengan cara menerapkan kebijakan, prosedur, struktur organisasi termasuk alur kerjanya, dan metode mitigasi risiko lainnya untuk menyerap potensi kerugian.
9. Dalam hal pengembangan dan pengadaan Teknologi Informasi dilakukan oleh pihak penyedia jasa Teknologi Informasi, proses pengendalian risiko yang dilakukan termasuk memastikan adanya perjanjian tertulis berupa *escrow agreement* atas aplikasi atau perangkat lunak yang dianggap penting oleh LJKNB.
10. Proses pemantauan risiko sebagaimana dimaksud pada angka 1 terhadap proses pengendalian risiko sebagaimana dimaksud pada angka 6 dilakukan dengan melakukan evaluasi kesesuaian, kecukupan, dan efektivitas kinerja penyelenggaraan Teknologi Informasi.

11. Tindak lanjut atas hasil evaluasi dapat dituangkan dalam bentuk keputusan maupun tindakan untuk meningkatkan efektivitas penyelenggaraan Teknologi Informasi.

VII. SISTEM PENGENDALIAN INTERNAL ATAS PENGGUNAAN TEKNOLOGI INFORMASI

1. LJKNB melaksanakan sistem pengendalian internal yang memuat paling sedikit:
   a. pengawasan oleh manajemen;
   b. identifikasi dan penilaian risiko;
   c. kegiatan pengendalian dan pemisahan fungsi;
   d. sistem informasi, sistem akuntansi, dan sistem komunikasi; dan
   e. kegiatan pemantauan dan koreksi penyimpangan yang dilakukan oleh:
      1) satuan kerja penyelenggara dan pengguna Teknologi Informasi;
      2) satuan kerja atau fungsi yang membawahkan audit internal; dan/atau
      3) pihak lain.
2. Sistem informasi, sistem akuntansi, dan sistem komunikasi sebagaimana dimaksud pada angka 1 huruf d harus didukung oleh teknologi, sumber daya manusia, dan struktur organisasi LJKNB yang memadai.
3. Kegiatan pemantauan dan koreksi penyimpangan sebagaimana dimaksud pada angka 1 huruf e paling sedikit:
   a. kegiatan pemantauan secara terus menerus;
   b. pelaksanaan fungsi audit internal yang efektif dan menyeluruh; dan
   c. perbaikan terhadap penyimpangan yang diidentifikasi oleh satuan kerja penyelenggara dan pengguna Teknologi Informasi, satuan kerja atau fungsi yang membawahkan audit internal, dan/atau pihak lain.
4. Pelaksanaan fungsi audit internal yang efektif dan menyeluruh sebagaimana dimaksud pada angka 3 huruf b mencakup paling sedikit:

a. latar belakang dan tujuan pelaksanaan audit;
b. tugas dan tanggung jawab auditor;
c. kewenangan auditor;
d. proses audit; dan
e. tindak lanjut atas hasil audit.

VIII. TATA CARA PENYAMPAIAN LAPORAN ATAS KONDISI TERTENTU, PERMOHONAN PERSETUJUAN PENEMPATAN PUSAT DATA DAN/ATAU PUSAT PEMULIHAN BENCANA DI LUAR WILAYAH INDONESIA, LAPORAN KEJADIAN KRITIS, DAN LAPORAN PERKEMBANGAN KONDISI TERKINI TERKAIT TEKNOLOGI INFORMASI

1. LJKNB menyampaikan:
   a. laporan sebagai tindakan tertentu yang harus dilaporkan kepada Otoritas Jasa Keuangan sebagaimana dimaksud dalam Pasal 21 ayat (6) huruf a dan huruf c Peraturan Otoritas Jasa Keuangan Nomor 4/POJK.05/2021 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Lembaga Jasa Keuangan Nonbank;
   b. permohonan persetujuan penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sebagaimana dimaksud dalam Pasal 23 ayat (3) Peraturan Otoritas Jasa Keuangan Nomor 4/POJK.05/2021 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Lembaga Jasa Keuangan Nonbank; dan/atau
   c. laporan kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraan Teknologi Informasi sebagaimana dimaksud dalam Pasal 31 ayat (1) Peraturan Otoritas Jasa Keuangan Nomor 4/POJK.05/2021 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Lembaga Jasa Keuangan Nonbank,

   secara dalam jaringan melalui sistem jaringan komunikasi data Otoritas Jasa Keuangan.
2. LJKNB memastikan bahwa laporan sebagaimana dimaksud pada angka 1 huruf a dan huruf c dan permohonan persetujuan sebagaimana dimaksud pada angka 1 huruf b yang disampaikan

secara dalam jaringan (*online*) sebagaimana dimaksud pada angka 1 adalah benar dan sama dengan dokumen cetak (*hardcopy*) yang disampaikan.

3. Dalam hal sistem jaringan komunikasi data Otoritas Jasa Keuangan sebagaimana dimaksud pada angka 1 belum tersedia atau mengalami gangguan teknis, laporan sebagaimana dimaksud pada angka 1 huruf a dan huruf c dan permohonan persetujuan sebagaimana dimaksud pada angka 1 huruf b disampaikan kepada Otoritas Jasa Keuangan secara luar jaringan (*offline*) dengan cara:
   a. diserahkan langsung; atau
   b. dikirim melalui perusahaan jasa pengiriman.
4. Dalam hal terjadi gangguan teknis sebagaimana dimaksud pada angka 3, Otoritas Jasa Keuangan mengumumkan melalui situs web (*website*) Otoritas Jasa Keuangan.
5. Penyampaian laporan secara luar jaringan (*offline*) sebagaimana dimaksud pada angka 3 harus disampaikan dalam bentuk data elektronik (*softcopy*) dengan menggunakan media berupa *compact disc* (CD) atau media penyimpanan data elektronik lainnya.
6. Penyampaian laporan sebagaimana dimaksud pada angka 3 dilengkapi surat pengantar dalam bentuk salinan cetak (*hardcopy*) yang ditandantangani oleh Direksi.
7. Format permohonan persetujuan sebagaimana dimaksud pada angka 1 huruf b adalah sebagaimana tercantum dalam format 12 Lampiran yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
8. Penyampaian surat pengantar sebagaimana dimaksud pada angka 6, laporan sebagaimana dimaksud pada angka 1 huruf a dan huruf c, serta permohonan persetujuan sebagaimana dimaksud pada angka 1 huruf b ditujukan kepada direktur pengawasan masing-masing LJKNB sebagaimana tercantum dalam format 13 Lampiran yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
9. LJKNB dinyatakan telah menyampaikan laporan sebagaimana dimaksud pada angka 1 huruf a dan huruf c dan/atau permohonan persetujuan sebagaimana dimaksud pada angka 1 huruf b dengan ketentuan sebagai berikut:

a. untuk penyampaian secara dalam jaringan (*online*) melalui sistem jaringan komunikasi data Otoritas Jasa Keuangan, dibuktikan dengan tanda terima dari sistem jaringan komunikasi data Otoritas Jasa Keuangan; atau
b. untuk penyampaian secara luar jaringan (*offline*) dibuktikan dengan tanda terima dari Otoritas Jasa Keuangan.

IX. PENUTUP

Ketentuan dalam Surat Edaran Otoritas Jasa Keuangan ini berlaku sesuai dengan pemberlakuan bagi masing-masing LJKNB dalam Peraturan Otoritas Jasa Keuangan Nomor 4/POJK.05/2021 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Lembaga Jasa Keuangan Nonbank.

Ditetapkan di Jakarta
pada tanggal 24 Agustus 2021

KEPALA EKSEKUTIF PENGAWAS PERASURANSIAN, DANA PENSIUN, LEMBAGA PEMBIAYAAN, DAN LEMBAGA JASA KEUANGAN LAINNYA
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

RISWINANDI

Salinan ini sesuai dengan aslinya
Plh. Direktur Hukum 1
Departemen Hukum

ttd

Evi Maria

LAMPIRAN

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR 22 /SEOJK.05/2021

TENTANG

PENERAPAN MANAJEMEN RISIKO DALAM PENGGUNAAN TEKNOLOGI INFORMASI OLEH LEMBAGA JASA KEUANGAN NONBANK

DAFTAR ISI

FORMAT 1: ORGANISASI DAN MANAJEMEN PENDUKUNG PELAKSANAAN MANAJEMEN RISIKO TEKNOLOGI INFORMASI

(*diisi struktur organisasi dan jumlah sumber daya manusia satuan kerja penyelenggara Teknologi Informasi, data keanggotan dan pelaksanaan rapat komite pengarah Teknologi Informasi*)

FORMAT 2: PENERAPAN KOMPONEN MANAJEMEN RISIKO DALAM PENGGUNAAN TEKNOLOGI INFORMASI

No	Hal	Keterangan
1.	Pengawasan aktif Direksi dan Dewan Komisaris	(diisi penjelasan singkat mengenai pengawasan aktif Direksi dan Dewan Komisaris yang dilakukan LJKNB)
2.	Kecukupan kebijakan dan prosedur penggunaan Teknologi Informasi	(diisi penjelasan singkat mengenai kebijakan dan prosedur penggunaan Teknologi Informasi yang dimiliki LJKNB)
3.	Kecukupan proses identifikasi, pengukuran, pengendalian, dan pemantauan risiko penggunaan Teknologi Informasi	(diisi penjelasan singkat mengenai proses identifikasi, pengukuran, pengendalian, dan pemantauan risiko penggunaan Teknologi Informasi yang dilakukan LJKNB)
4.	Sistem pengendalian internal atas penggunaan Teknologi Informasi	(diisi penjelasan singkat mengenai mekanisme pengendalian risiko dan hasilnya)

FORMAT 3: KEBIJAKAN DAN PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI

DAFTAR KEBIJAKAN PENGGUNAAN TEKNOLOGI INFORMASI

No.	Judul Dokumen[1)]	Deskripsi[2)]	Kategori[3)]	Waktu Kaji Ulang dan Pengkinian[4)]
1.				
2.				
dst.				

Keterangan:

1) Diisi dengan judul dokumen kebijakan
2) Diisi keterangan singkat mengenai dokumen kebijakan
3) Diisi dengan kategori kebijakan yaitu manajemen, pengembangan dan pengadaan, operasional Teknologi Informasi, jaringan komunikasi, pengamanan informasi, Rencana Pemulihan Bencana, penggunaan pihak penyedia jasa Teknologi Informasi, atau Layanan Keuangan Elektronik
4) Diisi tanggal kaji ulang dan pengkinian dokumen kebijakan

DAFTAR PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI

No.	Judul Dokumen[1)]	Deskripsi[2)]	Kategori[3)]	Waktu Kaji Ulang dan Pengkinian[4)]
1.				
2.				
dst.				

Keterangan:

1) Diisi dengan judul dokumen prosedur
2) Diisi keterangan singkat mengenai dokumen prosedur
3) Diisi dengan kategori prosedur yaitu manajemen, pengembangan dan pengadaan, operasional Teknologi Informasi, jaringan komunikasi, pengamanan informasi, Rencana Pemulihan Bencana, penggunaan pihak penyedia jasa Teknologi Informasi, atau Layanan Keuangan Elektronik
4) Diisi tanggal kaji ulang dan pengkinian dokumen prosedur

FORMAT 4: ARSITEKTUR APLIKASI

(*diisi gambar arsitektur aplikasi*)

FORMAT 5: DAFTAR APLIKASI

No.	Nama Aplikasi[1)]	Deskripsi[2)]	Platform[3)]	Lokasi Pusat Data[4)]	Penyelenggara Pusat Data[5)]	Lokasi Pusat Pemulihan Bencana[6)]	Penyelenggara Pusat Pemulihan Bencana[7)]	Pengembang Aplikasi[8)]	Tanggal Implementasi[9)]	Kepemilikan[10)]
1.										
2.										
dst.										

Keterangan:

1) Diisi dengan nama aplikasi
2) Diisi deskripsi mengenai aplikasi
3) Diisi platform yang digunakan untuk melakukan instalasi aplikasi yaitu *mobile* (telepon seluler) dan/atau *personal computer*.
4) Diisi kota lokasi Pusat Data.
5) Diisi penyelenggara penyedia Pusat Data yaitu sendiri (LJKNB yang bersangkutan) atau pihak penyedia jasa Teknologi Informasi (sebutkan nama pihak penyedia jasa Teknologi Informasi).
6) Diisi kota lokasi Pusat Pemulihan Bencana.
7) Diisi penyelenggara penyedia Pusat Pemulihan Bencana yaitu sendiri (LJKNB yang bersangkutan) atau pihak penyedia jasa Teknologi Informasi (sebutkan nama pihak penyedia jasa Teknologi Informasi).
8) Diisi inhouse jika aplikasi dikembangkan oleh LJKNB yang bersangkutan atau pihak penyedia jasa Teknologi Informasi (sebutkan nama pihak penyedia jasa Teknologi Informasi) jika aplikasi dikembangkan oleh pihak penyedia jasa Teknologi Informasi.
9) Diisi dengan tanggal implementasi (*go live*) aplikasi.
10) Diisi sewa atau beli putus.

FORMAT 6: JARINGAN KOMUNIKASI

(*diisi gambar topologi jaringan komunikasi*)

FORMAT 7: PUSAT DATA DAN PUSAT PEMULIHAN BENCANA

PUSAT DATA

Hal	Keterangan
Alamat	
Luas Area	
Kepemilikan	Milik Sendiri/Pihak Penyedia Jasa Teknologi Informasi*)
Pengendalian Faktor Lingkungan	(diisi penjelasan mengenai pengendalian faktor lingkungan sebagaimana dimaksud pada Romawi V angka 24 huruf c)
Pengendalian Fisik	(diisi penjelasan mengenai pengendalian faktor lingkungan sebagaimana dimaksud pada Romawi V angka 24 huruf a, huruf b, dan huruf d)

PUSAT PEMULIHAN BENCANA

Hal	Keterangan
Alamat	
Luas Area	
Kepemilikan	Milik Sendiri/Pihak Penyedia Jasa Teknologi Informasi*)
Lokasi Pusat Pemulihan Bencana Berbeda dengan Pusat Data	Ya/Tidak*)
Pengendalian Faktor Lingkungan	(diisi penjelasan mengenai pengendalian faktor lingkungan sebagaimana dimaksud pada Romawi V angka 24 huruf c)
Pengendalian Fisik	(diisi penjelasan mengenai pengendalian faktor lingkungan sebagaimana dimaksud pada Romawi V angka 24 huruf a, huruf b, dan huruf d)

FORMAT 8: PENGAMANAN TEKNOLOGI INFORMASI

No.	Nama Aset[1)]	Tipe Aset[2)]	Deskripsi[3)]

Keterangan:

1) Diisi dengan nama aset untuk pengamanan Teknologi Informasi, contoh: antivirus merk XYZ, *firewall* merk ABC, dan lain-lain.
2) Diisi dengan tipe aset (*software* atau *hardware*)
3) Diisi keterangan singkat mengenai aset seperti fungsi, jumlah lisensi, versi aset, dan lain-lain)

FORMAT 9: RENCANA PEMULIHAN BENCANA

Hal	Keterangan
Tingkat Bencana dan/atau Gangguan	Bencana kecil (*minor disaster*)/bencana besar (*major disaster*)/bencana katastropik (*catastrophic*)*)
Tanggal Pengujian Rencana Pemulihan Bencana Terakhir	(diisi tanggal pengujian rencana pemulihan bencana terakhir kali)
Daftar Aplikasi dan/atau Sumber Daya Teknologi Informasi yang Diuji Coba	(diisi dengan daftar aplikasi dan/atau sumber daya Teknologi Informasi yang diuji coba)
Hasil Pengujian	(diisi penjelasan singkat mengenai hasil pengujian)
Waktu Pelaksanaan Kaji Ulang	(diisi waktu pelaksanaan kaji ulang)
Hasil Kaji Ulang	(diisi dengan hasil kaji ulang)
Tindak Lanjut Kaji Ulang	(diisi dengan langkah yang perlu dilakukan setelah pelaksanaan kaji ulang)

FORMAT 10: PIHAK PENYEDIA JASA TEKNOLOGI INFORMASI

No.	Nama[1)]	Alamat[2)]	Jasa yang Diberikan[3)]

Keterangan:

1) Diisi dengan nama pihak penyedia jasa Teknologi Informasi
2) Diisi dengan alamat pihak penyedia jasa Teknologi Informasi
3) Diisi dengan daftar jasa yang diberikan pihak penyedia jasa Teknologi Informasi kepada LJKNB

FORMAT 11: BIAYA TEKNOLOGI INFORMASI

No.	Sumber Daya Teknologi Informasi[1)]	Biaya yang Dikeluarkan[2)]

Keterangan:

1) Diisi dengan jenis dan nama sumber daya Teknologi Informasi yang digunakan
2) Diisi dengan nominal biaya yang dikeluarkan dalam satuan rupiah

FORMAT 12: PERMOHONAN PERSETUJUAN PENEMPATAN SISTEM ELEKTRONIK PADA PUSAT DATA DAN/ATAU PUSAT PEMULIHAN BENCANA DI LUAR WILAYAH INDONESIA

PERMOHONAN PERSETUJUAN PENEMPATAN SISTEM ELEKTRONIK PADA PUSAT DATA DAN/ATAU PUSAT PEMULIHAN BENCANA DI LUAR WILAYAH INDONESIA

1. Nama negara tempat rencana lokasi penempatan sistem elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana
   (lampirkan data nama dan alamat serta kepemilikan penyelenggara Pusat Data dan/atau Pusat Pemulihan Bencana yang akan direncanakan)
   .....
2. Nama sistem elektronik yang akan ditempatkan pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia
   .....
3. Deskripsi sistem elektronik yang akan ditempatkan pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia
   .....
   .....
   .....
4. Pemenuhan persyaratan:

Hal	Keterangan
Pemenuhan persyaratan dalam Pasal 21 ayat (2) sampai dengan ayat (4) Peraturan Otoritas Jasa Keuangan Nomor 4/POJK.05/2021 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Lembaga Jasa Keuangan Nonbank (POJK 4/2021)	(diisi analisis dan penjelasan LJKNB atas pemenuhan ketentuan dalam Pasal 21 ayat (2) sampai dengan ayat (4) POJK 4/2021)
Analisis Risiko Negara	(diisi analisis dan penjelasan LJKNB atas risiko negara yang akan dilakukan penempatan sistem elektronik)
Surat pernyataan dari Direksi LJKNB dan pihak penyedia jasa Teknologi Informasi guna memastikan	Ada/Tidak*) (Lampirkan)

Hal	Keterangan
penyelenggaraan Sistem Elektronik di luar wilayah Indonesia tidak mengurangi efektivitas pengawasan Otoritas Jasa Keuangan	
Perjanjian kerja sama antara LJKNB dan pihak penyedia jasa Teknologi Informasi guna memastikan bahwa informasi mengenai rahasia LJKNB hanya diungkapkan sepanjang memenuhi ketentuan peraturan perundang-undangan di Indonesia.	Ada/Tidak*) (Lampirkan)
Perjanjian tertulis dengan penyedia jasa Teknologi Informasi memuat klausula pilihan hukum	Ada/Tidak*) (Lampirkan)
Surat pernyataan tidak keberatan dari otoritas pengawas penyedia jasa Teknologi Informasi di luar wilayah Indonesia bahwa Otoritas Jasa Keuangan diberikan akses untuk melakukan pemeriksaan terhadap pihak penyedia jasa Teknologi Informasi	Ada/Tidak*) (Lampirkan)
Surat pernyataan bahwa LJKNB akan menyampaikan secara berkala hasil penilaian yang dilakukan perusahaan induk, entitas utama,	Ada/Tidak*) (Lampirkan)

Hal	Keterangan
dan/atau entitas lain yang memiliki kegiatan usaha sejenis dalam satu grup LJKNB di luar wilayah Indonesia atas penerapan manajemen risiko pada pihak penyedia jasa Teknologi Informasi	
Analisis yang memuat bahwa manfaat yang diperoleh LJKNB dari rencana penempatan Sistem Elektronik di luar wilayah Indonesia lebih besar daripada beban yang ditanggung oleh LJKNB	(diisi analisis dan penjelasan LJKNB yang memuat bahwa manfaat yang diperoleh LJKNB dari rencana penempatan Sistem Elektronik di luar wilayah Indonesia lebih besar daripada beban yang ditanggung oleh LJKNB)
Rencana LJKNB untuk meningkatkan kemampuan sumber daya manusia LJKNB baik yang berkaitan dengan penyelenggaraan Teknologi Informasi maupun transaksi bisnis atau produk yang ditawarkan	Ada/Tidak*) (Lampirkan)

FORMAT 13: DAFTAR TUJUAN PENYAMPAIAN SURAT PENGANTAR, LAPORAN SEBAGAI TINDAKAN TERTENTU YANG HARUS DILAPORKAN KEPADA OTORITAS JASA KEUANGAN, LAPORAN KEJADIAN KRITIS, PENYALAHGUNAAN, DAN/ATAU KEJAHATAN DALAM PENYELENGGARAAN TEKNOLOGI, DAN PERMOHONAN PERSETUJUAN PENEMPATAN SISTEM ELEKTRONIK PADA PUSAT DATA DAN/ATAU PUSAT PEMULIHAN BENCANA DI LUAR WILAYAH INDONESIA

No.	LJKNB	TUJUAN PENYAMPAIAN
1.	Perusahaan Asuransi, Perusahaan Reasuransi, dan BPJS Kesehatan	Kepala Eksekutif Pengawas Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya Otoritas Jasa Keuangan u.p. Direktur Pengawasan Asuransi dan BPJS Kesehatan Gedung Wisma Mulia 2 Lantai 12 Jalan Jenderal Gatot Subroto Kav. 40 Jakarta 12710
2.	Perusahaan Asuransi Syariah, Perusahaan Reasuransi Syariah, Perusahaan Pembiayaan Syariah, Perusahaan Modal Ventura Syariah, Perusahaan Penjaminan Syariah, dan Perusahaan Penjaminan Ulang Syariah	Kepala Eksekutif Pengawas Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya Otoritas Jasa Keuangan u.p. Direktur IKNB Syariah Gedung Wisma Mulia 2 Lantai 15 Jalan Jenderal Gatot Subroto Kav. 40 Jakarta 12710
3.	Perusahaan Pialang Asuransi, Perusahaan Pialang Reasuransi, dan Perusahaan Penilai Kerugian Asuransi	Kepala Eksekutif Pengawas Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya Otoritas Jasa Keuangan u.p. Direktur Jasa Penunjang IKNB Gedung Wisma Mulia 2 Lantai 12 Jalan Jenderal Gatot Subroto Kav. 40 Jakarta 12710
4.	Dana Pensiun dan BPJS Ketenagakerjaan	Kepala Eksekutif Pengawas Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya Otoritas Jasa Keuangan u.p. Direktur Pengawasan Dana Pensiun dan BPJS Ketenagakerjaan Gedung Wisma Mulia 2 Lantai 12 Jalan Jenderal Gatot Subroto Kav. 40 Jakarta 12710

5.	Perusahaan Pembiayaan, Perusahaan Modal Ventura, dan Perusahaan Pembiayaan Infrastruktur	Kepala Eksekutif Pengawas Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya Otoritas Jasa Keuangan u.p. Direktur Pengawasan Lembaga Pembiayaan Gedung Wisma Mulia 2 Lantai 15 Jalan Jenderal Gatot Subroto Kav. 40 Jakarta 12710
6.	Perusahaan Pergadaian, Perusahaan Penjaminan, Perusahaan Penjaminan Ulang, Lembaga Pembiayaan Ekspor Indonesia, Perusahaan Pembiayaan Sekunder Perumahan, PT Permodalan Nasional Madani (Persero)	Kepala Eksekutif Pengawas Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya Otoritas Jasa Keuangan u.p. Direktur Pengawasan Lembaga Keuangan Khusus Gedung Wisma Mulia 2 Lantai 15 Jalan Jenderal Gatot Subroto Kav. 40 Jakarta 12710
7.	Penyelenggara Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi	Kepala Eksekutif Pengawas Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya Otoritas Jasa Keuangan u.p. Direktur Pengaturan, Perizinan, dan Pengawasan *Financial Technology* Gedung Wisma Mulia 2 Lantai 12 Jalan Jenderal Gatot Subroto Kav. 40 Jakarta 12710

Ditetapkan di Jakarta
pada tanggal 24 Agustus 2021

KEPALA EKSEKUTIF PENGAWAS PERASURANSIAN, DANA PENSIUN, LEMBAGA PEMBIAYAAN, DAN LEMBAGA JASA KEUANGAN LAINNYA
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

RISWINANDI

Salinan ini sesuai dengan aslinya
Plh. Direktur Hukum 1
Departemen Hukum

ttd

Evi Maria