Yth.

1. Direksi Perusahaan Asuransi;
2. Direksi Perusahaan Reasuransi;
3. Direksi Perusahaan Asuransi Syariah;
4. Direksi Perusahaan Reasuransi Syariah;
5. Direksi Perusahaan Pialang Asuransi;
6. Direksi Perusahaan Pialang Reasuransi;
7. Direksi Perusahaan Penilai Kerugian Asuransi;
8. Pengurus Dana Pensiun;
9. Direksi Perusahaan Pembiayaan;
10. Direksi Perusahaan Pembiayaan Syariah;
11. Direksi Perusahaan Modal Ventura;
12. Direksi Perusahaan Modal Ventura Syariah;
13. Direksi Perusahaan Pembiayaan Infrastruktur;
14. Direksi Perusahaan Pergadaian;
15. Direksi Perusahaan Penjaminan;
16. Direksi Perusahaan Penjaminan Syariah;;
17. Direksi Perusahaan Penjaminan Ulang;
18. Direksi Perusahaan Penjaminan Ulang Syariah;
19. Direksi Penyelenggara Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi;
20. Direksi Lembaga Pembiayaan Ekspor Indonesia;
21. Direksi Perusahaan Pembiayaan Sekunder Perumahan;
22. Direksi Badan Penyelenggara Jaminan Sosial Kesehatan;
23. Direksi Badan Penyelenggara Jaminan Sosial Ketenagakerjaan; Dan
24. Direksi PT Permodalan Nasional Madani (Persero),

di tempat.

RANCANGAN

SURAT EDARAN OTORITAS JASA KEUANGAN

NOMOR /SEOJK.05/2021

TENTANG­­

PENERAPAN MANAJEMEN RISIKO DALAM PENGGUNAAN

TEKNOLOGI INFORMASI OLEH LEMBAGA JASA KEUANGAN NONBANK

| *Draft*  BAB I ... | Tanggapan |
| --- | --- |
| 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 pelaksanaan mengenai Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Lembaga Jasa Keuangan Nonbank sebagai berikut: |  |
| 1. KETENTUAN UMUM |  |
| 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. |  |
| 1. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi |  |
| 1. Layanan Keuangan Elektronik adalah layanan bagi konsumen untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi keuangan melalui media elektronik. |  |
| 1. Pemrosesan Transaksi Berbasis Teknologi Informasi adalah kegiatan berupa penambahan, perubahan, penghapusan, dan/atau otorisasi data yang dilakukan pada sistem aplikasi yang digunakan untuk memproses transaksi. |  |
| 1. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik. |  |
| 1. Pusat Data adalah suatu fasilitas yang digunakan untuk menempatkan Sistem Elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data. |  |
| 1. 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. |  |
| 1. Pangkalan Data adalah sekumpulan data komprehensif dan disusun secara sistematis, dapat diakses oleh pengguna sesuai wewenang masing-masing dan dikelola oleh administrator Pangkalan Data. |  |
| 1. 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. |  |
| 1. 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. |  |
| 1. 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. |  |
| 1. CAKUPAN LEMBAGA JASA KEUANGAN NONBANK |  |
| LJKNB sebagaimana dimaksud dalam Romawi I angka 1 meliputi: |  |
| * 1. perusahaan perasuransian, yang terdiri atas: |  |
| 1. perusahaan asuransi; |  |
| 1. perusahaan reasuransi; |  |
| 1. perusahaan asuransi syariah; |  |
| 1. perusahaan reasuransi syariah; |  |
| 1. perusahaan pialang asuransi; |  |
| 1. perusahaan pialang reasuransi; dan |  |
| 1. perusahaan penilai kerugian asuransi, |  |
| sebagaimana dimaksud dalam peraturan perundang-undangan mengenai perasuransian; |  |
| * 1. dana pensiun sebagaimana dimaksud dalam peraturan perundang-undangan mengenai dana pensiun; |  |
| * 1. lembaga pembiayaan, yang terdiri atas: |  |
| 1. perusahaan pembiayaan; |  |
| 1. perusahaan pembiayaan syariah; |  |
| 1. perusahaan modal ventura; |  |
| 1. perusahaan modal ventura syariah; dan |  |
| 1. perusahaan pembiayaan infrastruktur, |  |
| sebagaimana dimaksud dalam peraturan perundang-undangan mengenai lembaga pembiayaan; |  |
| * 1. lembaga jasa keuangan lainnya, yang terdiri atas: |  |
| 1. perusahaan pergadaian sebagaimana dimaksud dalam peraturan perundang-undangan mengenai pergadaian; |  |
| 1. lembaga penjamin, yang terdiri atas: |  |
| 1. perusahaan penjaminan; |  |
| 1. perusahaan penjaminan syariah; |  |
| 1. perusahaan penjaminan ulang; dan |  |
| 1. perusahaan penjaminan ulang syariah, |  |
| sebagaimana dimaksud dalam peraturan perundang-undangan mengenai penjaminan; |  |
| 1. penyelenggara layanan pinjam meminjam uang berbasis teknologi informasi sebagaimana dimaksud dalam peraturan perundang-undangan mengenai layanan pinjam meminjam uang berbasis teknologi informasi; |  |
| 1. lembaga pembiayaan ekspor Indonesia sebagaimana dimaksud dalam peraturan perundang-undangan mengenai lembaga pembiayaan ekspor Indonesia; |  |
| 1. perusahaan pembiayaan sekunder perumahan sebagaimana dimaksud dalam peraturan perundang-undangan mengenai perusahaan pembiayaan sekunder perumahan; |  |
| 1. badan penyelenggara jaminan sosial sebagaimana dimaksud dalam peraturan perundang-undangan mengenai badan penyelenggara jaminan sosial; dan |  |
| 1. PT Permodalan Nasional Madani (Persero) sebagaimana dimaksud dalam peraturan perundang-undangan mengenai PT Permodalan Nasional Madani (Persero), |  |
| yang menggunakan Teknologi Informasi dalam penyelenggaraan usaha. |  |
| 1. RUANG LINGKUP MANAJEMEN RISIKO TEKNOLOGI INFORMASI |  |
| 1. Penerapan manajemen risiko dalam penggunaan Teknologi Informasi paling sedikit mencakup: |  |
| 1. pengawasan aktif Direksi dan Dewan Komisaris; |  |
| 1. kecukupan kebijakan dan prosedur penggunaan Teknologi Informasi; |  |
| 1. kecukupan proses identifikasi, pengukuran, pengendalian, dan pemantauan risiko penggunaan Teknologi Informasi; dan |  |
| 1. sistem pengendalian internal atas penggunaan Teknologi Informasi. |  |
| 1. 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. |  |
| 1. Penerapan manajemen risiko dalam penggunaan Teknologi Informasi sebagaimana dimaksud pada angka 1 harus disesuaikan dengan tujuan, kebijakan usaha, ukuran, dan kompleksitas usaha LJKNB. |  |
| 1. PENGAWASAN AKTIF DIREKSI DAN DEWAN KOMISARIS |  |
| 1. LJKNB 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. |  |
| 1. Tata kelola pelaksanaan wewenang dan tanggung jawab Direksi dan Dewan Komisaris sebagaimana dimaksud pada angka 1 diwujudkan dalam bentuk dokumentasi yang baik atas aspek paling sedikit: |  |
| 1. organisasi dan manajemen pendukung pelaksanaan manajemen risiko teknologi informasi; |  |
| 1. penerapan manajemen risiko dalam penggunaan Teknologi Informasi; |  |
| 1. kebijakan dan prosedur penggunaan Teknologi Informasi; |  |
| 1. arsitektur aplikasi; |  |
| 1. daftar aplikasi; |  |
| 1. jaringan komunikasi; |  |
| 1. Pusat Data dan Pusat Pemulihan Bencana; |  |
| 1. pengamanan teknologi informasi; |  |
| 1. Rencana Pemulihan Bencana; |  |
| 1. pihak penyedia jasa Teknologi Informasi; |  |
| 1. biaya Teknologi Informasi. |  |
| 1. Bagi LJKNB yang memiliki Komite pengarah Teknologi Informasi, pelaksanaan tugas dan tanggung jawab Direksi dibantu oleh Komite pengarah Teknologi Informasi. |  |
| 1. Komite pengarah Teknologi Informasi sebagaiamana dimaksud pada angka 3 dalam menjalankan tugas dan tanggung jawabnya harus melakukan pertemuan secara berkala yang didokumentasikan dalam bentuk risalah rapat. |  |
| 1. Pertemuan secara berkala sebagaimana dimaksud pada angka 4 dapat: |  |
| 1. melibatkan satuan kerja terkait di LJKNB; dan/atau |  |
| 1. dilakukan secara fisik atau virtual. |  |
| 1. Komite pengarah Teknologi Informasi menetapkan jangka waktu pertemuan secara berkala sebagaimana dimaksud pada angka 5 dalam kebijakan secara tertulis. |  |
| 1. KECUKUPAN KEBIJAKAN DAN PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI |  |
| 1. Kebijakan dan prosedur penggunaan Teknologi Informasi meliputi aspek paling sedikit: |  |
| 1. manajemen; |  |
| 1. pengembangan dan pengadaan; |  |
| 1. operasional Teknologi Informasi; |  |
| 1. jaringan komunikasi; |  |
| 1. pengamanan informasi; |  |
| 1. Rencana Pemulihan Bencana; |  |
| 1. penggunaan pihak penyedia jasa Teknologi Informasi; dan |  |
| 1. Layanan Keuangan Elektronik, bagi LJKNB yang menyelenggarakan Layanan Keuangan Elektronik. |  |
| 1. Kebijakan dan prosedur manajemen sebagaimana dimaksud pada angka 1 huruf a meliputi paling sedikit: |  |
| 1. *risk awareness* mengenai penyelenggaraan Teknologi Informasidari manajemen; |  |
| 1. pemahaman yang jelas mengenai *risk appetite* dari LJKNB; |  |
| 1. pemahaman terhadap ketentuan perundang-undangan mengenai Teknologi Informasi; dan |  |
| 1. transparansi dan tanggung jawab mengenai risiko yang signifikan dari setiap aspek terkait penyelenggaraan TI. |  |
| 1. Kebijakan dan prosedur pengembangan dan pengadaan sebagaimana dimaksud pada angka 1 huruf b meliputi paling sedikit: |  |
| 1. tahap pengembangan: |  |
| 1. identifikasi dan analisis kebutuhan pengguna; |  |
| 1. pendefinisian kebutuhan pengguna; |  |
| 1. perancangan sistem; |  |
| 1. pemrograman; |  |
| 1. pengujian; |  |
| 1. implementasi; |  |
| 1. pengkajian ulang paska implementasi; |  |
| 1. pemeliharaan; dan |  |
| 1. pemusnahan. |  |
| 1. tahap pengadaan; |  |
| 1. pedoman pengadaan; |  |
| 1. kontrak pembelian dan lisensi; |  |
| 1. pemeliharaan; |  |
| 1. garansi; |  |
| 1. penyelesaian perselisihan; |  |
| 1. perubahan perjanjian; |  |
| 1. keamanan; dan |  |
| 1. pengalihan sebagian kegiatan (subkontrak) kepada pihak lain. |  |
| 1. Tahap identifikasi dan analisis kebutuhan pengguna sebagaimana dimaksud pada angka 3 huruf a angka 1) paling sedikit terdiri dari: |  |
| 1. penyusunan proposal yang berisi identifikasi kebutuhan pengguna untuk menambah, menyempurnakan, atau memperbaiki suatu sistem, tujuan dan manfaat yang diharapkan, serta bagaimana sistem yang akan dikembangkan dapat mendukung perkembangan usaha LJKNB, pencapaian tujuan bisnis LJKNB dan kelangsungan pelayanan terhadap konsumen LJKNB; |  |
| 1. evaluasi oleh manajemen, satuan kerja penyelenggara Teknologi Informasi, dan/atau satuan kerja pengguna Teknologi Informasi; |  |
| 1. 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; |  |
| 1. studi kelayakan, yang antara lain berupa pertimbangan bisnis LJKNB, kebutuhan fungsional, rencana waktu pelaksanaan, faktor-faktor yang mempengaruhi pengembangan serta analisis biaya dan manfaat; |  |
| 1. 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. |  |
| 1. Tahap pendefinisian kebutuhan pengguna sebagaimana dimaksud pada angka 3 huruf a angka 2) paling sedikit terdiri dari: |  |
| 1. 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; |  |
| 1. analisis kebutuhan yang merupakan proses pemahaman permasalahan dan kebutuhan untuk menentukan solusi yang dapat dikembangkan. |  |
| 1. 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. |  |
| 1. pengelolaan kebutuhan yang merupakan proses untuk mengidentifikasi, mengendalikan, dan menyimpan setiap perubahan terhadap kebutuhan pada saat pengembangan sistem berjalan. |  |
| 1. 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. |  |
| 1. Tahap pemrograman sebagaimana dimaksud pada angka 3 huruf a angka 4) paling sedikit terdiri dari: |  |
| 1. standar pemograman yang meliputi penjabaran tanggung jawab *programmer* dan pihak-hak yang terlibat langsung dalam proses pemrograman yaitu dengan cara: |  |
| * 1. membatasi akses programmer terhadap data, program, utilitasi, dan sistem yang di luar tanggung jawabnya salah satunya dengan pengendalian pengelolaan *library*; dan |  |
| * 1. pengendalian versi yaitu metode yang secara sistematis menyimpan kronologis dari salinan program yang disempurnakan serta menjadi salah satu dokumentasi dalam penyelenggaraan pengembangan. |  |
| 1. 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 pmerograman, format yang digunakan, standar penamaan, dan petunjuk pelaksanaan bagi pengguna akhir. | . |
| 1. Tahap pengujian sebagaimana dimaksud pada angka 3 huruf a angka 5) mencakup antara lain: |  |
| 1. *unit test*, yaitu uji coba yang dilakukan oleh pengembang atas fungsional setiap unit atau sub modul dari sistem yang telah selesai dikembangkan; |  |
| 1. *system integration test*, yaitu pengujian yang dilakukan oleh pengembang terhadap keseluruhan fungsional sistem setelah diintegrasikan menjadi satu kesatuan yang utuh; |  |
| 1. *stress test*, yaitu uji ketahanan yang dilakukan oleh pengembang terhadap kemampuan sistem dalam menangani proses atau transaksi dalam skala atau jumlah yang besar; dan |  |
| 1. *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. |  |
| 1. 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. |  |
| 1. Tahap implementasi sebagaimana dimaksud pada angka 3 huruf a angka 6) harus memperhatikan antara lain: |  |
| 1. pengecekan integritas program berupa pengendalian yang memadai terhadap konversi dari kode sumber ke dalam sistem yang akan diimplementasikan; |  |
| 1. migrasi data dari sistem lama ke sistem baru; |  |
| 1. pengecekan akurasi dan keamanan data hasil migrasi pada sistem baru; |  |
| 1. kemungkinan diberlakukannya *parallel run* antara sistem yang lama dengan yang baru, sampai dipastikan bahwa data pada sistem yang baru telah akurat dan andal; |  |
| 1. kepastian integritas data berupa keakuratan dan keandalan dari Pangkalan Data termasuk data yang tersimpan di dalamnya; |  |
| 1. perbaikan data dan referensi secara langsung (*patching data*) pada saat implementasi harus dihindari karena dapat mempengaruhi integritas data pada Pangkalan Data di *server* produksi; |  |
| 1. pengaturan penyimpanan kode sumber dan Pangkalan Data dari sistem lama; dan |  |
| 1. antisipasi adanya kelemahan sistem operasi, sistem yang dikembangkan, Pangkalan Data dan jaringan, termasuk ancaman dari pihak yang tidak berwenang seperti *virus, trojan horse, worms, spyware, Denial-of-Service* (DoS), *wardriving*, *spoofing* dan *logic bomb*, dengan menguji dan menerapkan pengendalian pengamanan atas sistem yang akan diimplementasikan. |  |
| 1. Tahap pengkajian ulang paska implementasi sebagaimana dimaksud pada angka 3 huruf a angka 7) merupakan proses analisis efektivitas aktivitas manajemen proyek dengan membandingkan antara lain rencana dan realisasi biaya, manfaat yang diperoleh, dan ketepatan jadwal proyek. Hasil analisis harus didokumentasikan dan dailaporkan kepada manajemen. |  |
| 1. 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. |  |
| 1. 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 guna menghindari penyalahgunaan oleh pihak tidak berwenang. |  |
| 1. Pedoman pengadaan sebagaimana dimaksud pada angka 3 huruf b angka 1) harus memperhatikan hal-hal antara lain: |  |
| 1. 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 sistem yang akan diadakan untuk mendukung kebutuhan bisnis LJKNB; |  |
| 1. kesesuaian pihak penyedia jasa Teknologi Informasi, kontrak, lisensi, dan produk yang diperoleh terhadap kebutuhan penyelenggaraan Teknologi Informasi LJKNB; |  |
| 1. kesesuaian spesifikasi penawaran yang diajukan oleh pihak penyedia jasa Teknologi Informasi dengan spesifikasi kebutuhan penyelenggaraan Teknologi Informasi di LJKNB |  |
| 1. perbandingan penawaran yang diajukan oleh pihak penyedia jasa Teknologi Informasi satu dengan penyedia jasa Teknologi Informasi lainnya; dan |  |
| 1. kondisi keuangan pihak penyedia jasa Teknologi Informasi dan komitmen pihak penyedia jasa Teknologi Informasi terhadap pelayanan yang diberikan kepada LJKNB. |  |
| 1. Kontrak pembelian dan lisensi sebagaimana dimaksud pada angka 3 huruf b angka 2) harus memperhatikan hal-hal antara lain: |  |
| 1. penjelasan tertulis bahwa penggunaan perangkat lunak bersifat eksklusif atau tidak; |  |
| 1. informasi dan jumlah pengguna yang dapat menggunakan perangkat lunak; |  |
| 1. daftar entitas terkait lainnya yang dapat menggunakan perangkat lunak tersebut, seperti perusahaan anak atau grup perusahaan; |  |
| 1. 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 |  |
| 1. lokasi penggunaan, apakah lisensi lokasi penggunaan terbatas pada suatu lokasi atau tidak. |  |
| 1. Pemeliharaan sebagaimana dimaksud pada angka 3 huruf b angka 3) mencakup paling sedikit: |  |
| 1. pelatihan oleh pihak penyedia jasa Teknologi Informasi kepada LJKNB; |  |
| 1. pihak penyedia jasa Teknologi Informasi memberikan dokumentasi perangkat lunak, termasuk petunjuk teknis penggunaan perangkat lunak; |  |
| 1. pelaksanaan dan biaya pengkinian dan/atau modifikasi perangkat lunak; dan |  |
| 1. 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; |  |
| 1. kemungkinan pihak penyedia jasa Teknologi Informasi untuk membantu proses konversi data pada saat penggantian sistem pada masa mendatang. |  |
| 1. Garansi sebagaimana dimaksud pada angka 3 huruf b angka 4) memiliki aspek yang mencakup paling sedikit: |  |
| 1. tidak melanggar hak kekayaan intelektual dari pihak lainnya di seluruh dunia; |  |
| 1. tidak mengandung kode rahasia, pembatasan yang tidak diungkapkan, atau pembatasan secara otomatis pada perjanjian; |  |
| 1. berfungsi sesuai spesifikasi dan harus dinyatakan batasan tanggung jawab pihak penyedia jasa Teknologi Informasi dalam hal terjadi permasalahan; |  |
| 1. pemeliharaannya dilakukan oleh pihak penyedia jasa Teknologi Informasi selama jangka waktu yang diperjanjikan; dan |  |
| 1. tetap berlaku dalam hal terjadi penggabungan, peleburan, pengambilalihan, atau perubahan kepemilikan baik pada LJKNB atau pihak penyedia jasa Teknologi Informasi. |  |
| 1. 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. | . |
| 1. Perubahan perjanjian sebagaimana dimaksud pada angka 3 huruf b angka 6) mencakup paling sedikit adanya klausula yang secara jelas menyatakan bahwa pihak penyedia jasa Teknologi Informasi tidak dapat memodifikasi perjanjian tanpa adanya persetujuan dari kedua belah pihak. |  |
| 1. Keamanan sebagaimana dimaksud pada angka 3 huruf b angka 7) mencakup paling sedikit: |  |
| 1. tanggung jawab secara terus menerus dari pihak penyedia jasa Teknologi Informasi untuk melindungi keamanan dan kerahasiaan sumber daya Teknologi Informasi dan data LJKNB; |  |
| 1. larangan bagi pihak penyedia jasa Teknologi Informasi untuk menggunakan atau mengungkapkan informasi yang dimiliki LJKNB tanpa persetujuan LJKNB; |  |
| 1. jaminan dari pihak penyedia jasa Teknologi Informasi bahwa perangkat lunak tidak mengandung *back door* yang memungkinkan akses oleh pihak yang tidak berwenang ke dalam sistem dan data LJKNB; dan |  |
| 1. pernyataan secara eksplisit bahwa pihak penyedia jasa Teknologi Informasi tidak akan menggunakan fitur yang dapat mengakibatkan perangkat lunak tidak berfungsi dengan baik. |  |
| 1. 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: |  |
| 1. hanya dapat melakukan pengalihan sebagian kegiatan (subkontrak) kepada pihak ketiga berdasarkan persetujuan LJKNB yang dibuktikan dengan dokumen tertulis; dan |  |
| 1. bertanggung jawab terhadap perangkat lunak meskipun perangkat lunak dirancang dan/atau dikembangkan oleh pihak lain. |  |
| 1. Kebijakan dan prosedur operasional Teknologi Informasi sebagaimana dimaksud pada angka 1 huruf c meliputi paling sedikit: |  |
| 1. Kebijakan dan prosedur pengelolaan data, yang paling sedikit terdiri atas: |  |
| 1. pengelolaan Pusat Data, bagi LJKNB yang dikenai kewajiban kepemilikan Pusat Data; |  |
| 1. pengelolaan Pusat Pemulihan Bencana, bagi LJKNB yang dikenai kewajiban kepemilikan Pusat Pemulihan Bencana; dan |  |
| 1. pengelolaan Pangkalan Data. |  |
| 1. 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; ~~dan~~ |  |
| 1. 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* atau *upgrade*, atau permasalahan lain yang sesuai dengan versi perangkat lunak yang digunakan; dan |  |
| 1. 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. |  |
| 1. penanganan kejadian atau permasalahan, dimana LJKNB harus memelihara sarana yang diperlukan untuk menangani permasalahan yang paling sedikit terdiri atas: |  |
| 1. fungsi *help desk,* yang bertugas menanggapi dan menangani permasalahan terkait Teknologi Informasi di LJKNB; dan |  |
| 1. penanganan penggunaan *super user* yaitu pengguna yang memiliki kewenangan sangat luas, yang berisi paling sedikit mengenai: |  |
| 1. penetapan dan kriteria pihak yang memiliki hak akses *super user*; |  |
| 1. mekanisme pengelolaan *password super user* yang meliputi penyimpanan dan penggantian *password.* |  |
| 1. pengendalian pertukaran informasi, yang paling sedikit terdiri atas: |  |
| 1. permintaan dan pemberian informasi oleh pihak internal dan eksternal; dan |  |
| 1. pengiriman informasi melalui media seperti surat elektronik, *flashdisk, compactdisk, hardcopy,* internet, dan lain-lain. |  |
| 1. fungsi kendali mutu, yang berfungsi untuk melakukan penilaian kualitas perangkat lunak dan perangkat keras; dan |  |
| 1. mekanisme pemusnahan dan penghapusan perangkat lunak dan perangkat keras. |  |
| 1. Dalam menyusun kebijakan dan prosedur mengenai pengelolaan Pusat Data sebagaimana dimaksud pada angka 22 huruf a angka 1), LJKNB harus memperhatikan hal-hal berikut: |  |
| 1. bangunan harus: |  |
| 1. berada dalam lokasi yang aman secara geografis; dan |  |
| 1. memiliki akses jalan darat yang memadai, |  |
| 1. akses fisik ke Pusat Data harus dibatasi dan dikendalikan dengan baik; |  |
| 1. pengendalian faktor lingkungan meliputi antara lain: |  |
| 1. memastikan tersedianya sumber listrik yang cukup, stabil, dan tersedianya sumber alternatif listrik untuk mengantisipasi tidak berfungsinya sumber listrik utama; |  |
| 1. memastikan tersedianya alat detektor api dan asap, alat pemadam api, dan pipa pembuangan air; |  |
| 1. memperhatikan tata ruang diantaranya: |  |
| 1. menghindari penempatan ruangan di bawah area perpipaan seperti kamar mandi dan dapur; |  |
| 1. 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; dan |  |
| 1. ketersediaan pintu darurat; dan |  |
| 1. manajemen perangkat pendukung seperti ketersediaan rak dengan bahan yang tidak mudah terbakar, penempatan kabel dan infrasturuktur jaringan lainnya, dan lain-lain, |  |
| 1. 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; |  |
| 1. pengoperasian tugas oleh operator Teknologi Informasi harus dibatasi sesuai kewenangan; |  |
| 1. pendistribusian *output* harus dilakukan dengan aman untuk menghindari terbukanya informasi yang rahasia; |  |
| 1. proses rekam cadang; |  |
| 1. pemantauan terhadap perangkat keras dan perangkat lunak; dan |  |
| 1. pengaktifan jejak audit. |  |
| 1. 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. |  |
| 1. Dalam menyusun kebijakan dan prosedur mengenai pengelolaan Pusat Pemulihan Bencana sebagaimana dimaksud pada angka 22 huruf a angka 2), LJKNB harus memperhatikan hal-hal berikut: |  |
| 1. 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; |  |
| 1. sistem di Pusat Pemulihan Bencana harus kompatibel dengan sistem yang digunakan pada Pusat Data dan harus disesuaikan jika terjadi perubahan pada Pusat Data; |  |
| 1. memperhitungkan waktu tempuh untuk terjaminnya proses *recovery*; dan |  |
| 1. 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. |  |
| 1. Dalam menyusun kebijakan dan prosedur mengenai pengelolaan Pangkalan Data sebagaimana dimaksud pada angka 22 huruf a angka 3), LJKNB harus memperhatikan hal-hal berikut: |  |
| 1. ketersediaan sumber daya manusia yang memiliki kompetensi dalam pengelolaan Pangkalan Data khususnya terkait pengaksesan, pemeliharaan, penanganan permasalahan dan administrasi Pangkalan Data. |  |
| 1. terdapat mekanisme rekam cadang data dimana: |  |
| 1. lokasi rekam cadang harus disimpan pada lokasi yang berbeda dari lokasi Pusat Data; |  |
| 1. rekam cadang dilakukan secara menyeluruh (*full system backup*) dan berkala atau dilakukan dalam hal terjadi perubahan sistem yang mendasar; |  |
| 1. rekam cadang harus memenuhi standar sistem pengamanan yang memadai; |  |
| 1. harus dilakukan uji *restore* secara berkala untuk memastikan rekam cadang dapat digunakan pada saat diperlukan (kondisi darurat); dan |  |
| 1. terdapat mekanisme pemusnahan dan/atau penghapusan media rekam cadang. |  |
| 1. Kebijakan dan prosedur jaringan komunikasi sebagaimana dimaksud pada angka 1 huruf d meliputi paling sedikit: |  |
| 1. pengukuran kinerja dan perencanaan kapasitas jaringan; |  |
| 1. pengamanan jaringan; |  |
| 1. manajemen jaringan; |  |
| 1. prosedur penanganan masalah jaringan; |  |
| 1. mekanisme penggunan jaringan komunikasi antara lain terkait jaringan internet, intranet, surat elektronik, dan jaringan tanpa kabel; |  |
| 1. prosedur penyelesaian masalah; |  |
| 1. fasilitas untuk rekam cadang dan pemulihan; dan |  |
| 1. perjanjian dan SLA dengan pihak penyedia jasa Teknologi Informasi, dalam hal penyediaan dan pengelolaan jaringan komunikasi dilakukan oleh pihak penyedia jasa Teknologi Informasi. |  |
| 1. Kebijakan pengamanan informasi sebagaimana dimaksud pada angka 1 huruf e meliputi paling sedikit: |  |
| 1. tujuan pengamanan informasi; |  |
| 1. komitmen manajemen terhadap pengamanan informasi; |  |
| 1. kerangka acuan dalam menetapkan pengendalian dan penanganan permasalahan; |  |
| 1. kepatuhan terhadap ketentuan internal dan ketentuan peraturan perundang-undangan mengenai pengamanan informasi antara lain terkait Undang-Undang mengenai Informasi dan Transaksi Elektronik (UU ITE); |  |
| 1. pelatihan dan peningkatan kesadaran atas pentingnya pengamanan informasi; |  |
| 1. tugas dan tanggung jawab pihak-pihak dalam pengamanan informasi; |  |
| 1. analisis dampak pengamanan informasi terhadap kelangsungan bisnis dan kegiatan usaha LJKNB; |  |
| 1. sanksi atas pelanggaran kebijakan pengamanan informasi; dan |  |
| 1. dokumen atau ketentuan lain yang mendukung kebijakan pengamanan informasi. |  |
| 1. Prosedur pengamanan informasi sebagaimana dimaksud pada angka 1 huruf e meliputi paling sedikit prosedur mengenai: |  |
| 1. pengelolaan aset, yang meliputi paling sedikit: |  |
| 1. aset LJKNB yang terkait dengan informasi dilakukan identifikasi, ditentukan pemilik/penanggung jawabnya, dan dicatat agar dapat dilindungi secara tepat; |  |
| 1. aset yang terkait dengan informasi dapat berupa data yang berbentuk cetak keras (*hardcopy*) dan/atau cetak lunak (*softcopy*), perangkat lunak, perangkat keras, jaringan, peralatan pendukung (misalnya sumber daya listrik dan *air conditioner*), dan sumber daya manusia yang meliputi kualifikasi dan ketrampilan; dan |  |
| 1. informasi perlu diklasifikasikan agar dapat dilakukan pengamanan yang memadai sesuai dengan klasifikasinya.   Contoh klasifikasi:   1. informasi rahasia, misalnya data konsumen; 2. informasi internal, misalnya peraturan mengenai kepegawaian; dan 3. informasi biasa, misalnya informasi produk keuangan yang ditawarkan kepada konsumen. |  |
| 1. pengelolaan sumber daya manusia, yang meliputi paling sedikit; |  |
| 1. sumber daya manusia baik pegawai organik LJKNB, konsultan, pegawai honorer, dan pegawai dari pihak penyedia jasa Teknologi Informasi yang memiliki akses terhadap informasi harus memahami tanggung jawab terhadap pengamanan informasi; |  |
| 1. peran dan tanggung jawab sumber daya manusia baik pegawai organik 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; |  |
| 1. dalam perjanjian kerja sama atau kontrak dengan pegawai organik LJKNB, konsultan, pegawai honorer, dan pegawai dari pihak penyedia jasa Teknologi Informasi harus tercantum ketentuan-ketentuan mengenai pengamanan informasi yang sesuai dengan kebijakan pengamanan informasi LJKNB. Sebagai contoh, perlu adanya klausula yang menyatakan bahwa pegawai organik LJKNB, konsultan, pegawai honorer, dan pegawai dari pihak penyedia jasa Teknologi Informasi harus menjaga kerahasiaan informasi yang diperolehnya sesuai dengan klasifikasi informasi; |  |
| 1. 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*); |  |
| 1. pelatihan dan/atau sosialisasi tentang pengamanan informasi harus diberikan kepada pegawai organik 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; |  |
| 1. LJKNB menetapkan sanksi atas pelanggaran terhadap kebijakan pengamanan informasi; |  |
| 1. 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 |  |
| 1. LJKNB menetapkan pemisahan tugas dan tanggung jawab, yaitu memastikan terdapat pemisahan tugas dan tanggung jawab antara sumber daya manusia di operasional LJKNB, |  |
| 1. 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; |  |
| 1. pengamanan fisik dan lingkungan terhadap fasilitas pemrosesan informasi yang penting meliputi antara lain pembatas ruangan, pengendalian akses masuk misalnya penggunaan *access control card*, *personal identification number*, atau *biometrics*), 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); |  |
| 1. fasilitas pendukung seperti *air conditioner* dan sumber daya listrik harus dipastikan kapasitas dan ketersediaannya dalam mendukung operasional fasilitas pemrosesan informasi; |  |
| 1. aset milik penyedia jasa Teknologi Informasi harus diidentifikasikan secara jelas dan diberikan perlindungan yang memadai seperti misalnya dengan menerapkan pengamanan yang cukup, *dual control*, atau menempatkan secara terpisah dari aset milik LJKNB |  |
| 1. pemeliharaan dan pemeriksaan secara berkala terhadap fasilitas pemrosesan informasi dan fasilitas pendukung sesuai dengan prosedur yang telah ditetapkan. |  |
| 1. pengendalian akses, yang meliputi paling sedikit; |  |
| 1. 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; |  |
| 1. pemberian akses mengacu kepada prinsip berdasarkan kebutuhan bisnis dan dengan akses yang seminimal mungkin; |  |
| 1. penerapan metode identifikasi dan otentikasi sesuai analisis risiko. Metode otentikasi yang digunakan dapat berupa satu atau kombinasi dari “*what you know*” (antara lain *password*), “*what you have*” (antara lain telepon genggam, kartu magnetis dengan chip, dan/atau token), “*something you are*” (antara lain *biometric* seperti retina dan sidik jari); |  |
| 1. prosedur pengendalian melalui pemberian *password* awal (*initial password*) kepada pengguna dengan memperhatikan paling sedikit hal-hal sebagai berikut: |  |
| 1. *password* awal harus diganti saat *login* pertama kali; |  |
| 1. *password* awal diberikan secara aman, misalnya melalui amplop tertutup atau kertas karbon berlapis dua sehingga hanya diketahui oleh pihak yang berhak; |  |
| 1. *password* awal bersifat khusus atau unik untuk setiap pengguna dan tidak mudah ditebak; |  |
| 1. pemilik *user-id* terutama dari pegawai organic 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*; |  |
| 1. *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*). |  |
| 1. prosedur yang mewajibkan pengguna untuk: |  |
| 1. menjaga kerahasiaan *password*; |  |
| 1. menghindari penulisan *password* di kertas dan tempat lain tanpa pengamanan yang memadai |  |
| 1. menggunakan *password* yang berkualitas, yaitu: |  |
| 1. panjang *password* yang memadai sehingga tidak mudah ditebak; |  |
| 1. mudah diingat dan terdiri dari paling sedikit kombinasi 2 tipe karakter (huruf, angka, atau karakter khusus); |  |
| 1. tidak didasarkan atas data pribadi pengguna seperti nama, nomor telepon, atau tanggal lahir; |  |
| 1. 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; |  |
| 1. mengubah *password* secara berkala; dan |  |
| 1. menghindari penggunaan *password* yang sama secara berulang. |  |
| 1. prosedur untuk menonaktifkan hak ases jika *user-id* tidak digunakan pada waktu tertentu, menetapkan jumlah maksimal kegagalan *password*, dan menonaktifkan pengguna setelah mencapai jumlah maksimal kegagalan *password*; |  |
| 1. prosedur kaji ulang secara berkala oleh satuan kerja yang tidak terlibat dalam operasional pengendalian akses, terhadap hak akses pengguna untuk memastikan bahwa hak ases sesuai dengan wewenang yang diberikan; |  |
| 1. sistem operasi, sistem aplikasi, Pangkalan Data, utilitas, dan perangkat lainnya yang dimiliki oleh LJKNB dapat membantu pelaksanaan pengamanan *password*, sebagai contoh: |  |
| 1. memaksa pengguna untuk mengubah *password* setelah jangka waktu tertentu dan menolak apabila pengguna memasukkan *password* yang sama dengan yang digunakan sebelumnya saat mengganti *password*; |  |
| 1. menyimpan *password* secara aman (terenkripsi); |  |
| 1. memutuskan hubungan atau akses pengguna jika tidak terdapat respon selama jangka waktu tertentu; |  |
| 1. menonaktifkan atau menghapus hak akses pengguna jika pengguna tidak melakukan *log-in* melebihi jangka waktu tertentu misalnya karena cuti, rotasi, dan/atau mutasi; dan |  |
| 1. prosedur pembatasan akses paling sedikit melalui penggunaan password dan pengaturan pihak yang berwenang melakukan akses bagi LJKNB yang menggunakan *file sharing.* |  |
| 1. 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; |  |
| 1. adanya proses antisipasi dan pengendalian pengamanan yang memadai atas kelemahan sistem operasi, sistem aplikasi, Pangkalan Data, dan jaringan, termasuk ancaman dari pihak yang tidak berwenang seperti *virus, trojan horse, worms, spyware, Denial-of-Service (DoS), war driving, spoofing*, dan *logic* *bomb*; |  |
| 1. perlindungan terhadap jejak audit atau *log* dari gangguan dan akses tidak sah; |  |
| 1. sinkronisasi antara penunjuk waktu dari seluruh sistem elektronik LJKNB dengan sumber penunjuk waktu akurat yang disepakati; dan |  |
| 1. pemeliharaan catatan perangkat lunak yang digunakan dan pemantauan secara berkala atas Sistem Elektronik dan kemungkinan persamalahan yang timbul |  |
| 1. pemantauan pengamanan informasi yang dilakukan sesuai dengan risiko atau tingkat kritikalitas informasi; |  |
| 1. penanganan insiden dalam pengamanan informasi, yang meliputi paling sedikit; |  |
| 1. cakupan penanganan insiden yang meliputi paling sedikit: |  |
| 1. siapa yang harus melaporkan insiden; |  |
| 1. jenis insiden yang harus dilaporkan; |  |
| 1. alur pelaporan insiden; |  |
| 1. analisis atas insiden; dan |  |
| 1. pendokumentasian bukti terkait insiden dan tindak lanjut yang akan dilakukan, |  |
| 1. identifikasi, pelaporan, pemrosesan tindak lanjut, dokumentasi, dan evaluasi atas insiden yang terjadi; |  |
| 1. Kebijakan dan prosedur Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 1 huruf f meliputi paling sedikit: |  |
| 1. analisis terhadap Rencana Pemulihan Bencana; |  |
| 1. jenis prosedur Rencana Pemulihan Bencana antara lain mencakup; |  |
| 1. komponen prosedur Rencana Pemulihan Bencana; |  |
| 1. penetapan kejelasan tanggung jawab bagi pihak-pihak terkait dalam penyelenggaraan Rencana Pemulihan Bencana; |  |
| 1. uji coba Rencana Pemulihan Bencana; dan |  |
| 1. pengkinian Rencana Pemulihan Bencana. |  |
| 1. Analisis terhadap Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 29 huruf a merupakan analisis terhadap kemungkinan timbulnya risiko yang dapat disebabkan oleh faktor antara lain: |  |
| 1. faktor kebakaran; |  |
| 1. faktor bencana alam seperti banjir dan gempa; |  |
| 1. faktor gangguan teknis seperti kerusakan perangkat keras, perangkat lunak, gangguan listrik, gangguan transmisi data, dan lain-lain; dan |  |
| 1. faktor manusia seperti sabotase. |  |
| 1. Jenis-jenis prosedur dalam Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 29 huruf b mencakup antara lain: |  |
| 1. prosedur tanggap darurat, untuk mengendalikan sistem pada saat terjadi gangguan/bencana, mengurangi dampak kerugian, serta menentukan status keadaan bencana; |  |
| 1. prosedur pemulihan sistem yang memungkinkan kegiatan operasional LJKNB dapat kembali ke kondisi normal; dan |  |
| 1. prosedur sinkronisasi data digunakan untuk memastikan kesamaan antara data mesin yang digunakan untuk operasional dengan data rekam cadang, serta untuk memastikan semua data hasil pemrosesan bisnis selama masa pemulihan telah masuk ke dalam sistem. |  |
| 1. Prosedur Rencana Pemulihan Bencana mencakup komponen sebagaimana dimaksud pada angka 29 huruf c paling sedikit sebagai berikut: |  |
| 1. 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; |  |
| 1. sumber daya Teknologi Informasi dan aplikasi inti LJKNB, yaitu LJKNB harus memiliki prosedur dan dokumentasi yang lengkap untuk memulihkan aplikasi-aplikasi utama yang terkait dengan kegiatan usaha LJKNB maupun operasional LJKNB lainnya; |  |
| 1. fasilitas komunikasi, guna memastikan tersedianya alternatif jalur komunikasi yang dapat digunakan di lingkungan internal dan/atau eksternal pada saat terjadinya gangguan atau bencana. |  |
| 1. Penetapan kejelasan tanggung jawab bagi pihak-pihak terkait dalam penyelenggaraan Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 29 huruf d meliput paling sedikit mengenai tanggung jawab: |  |
| 1. manajemen; |  |
| 1. satuan kerja penyelenggara Teknologi Informasi; dan |  |
| 1. satuan kerja pendukung, seperti satuan kerja yang membawahkan fungsi logistik. |  |
| 1. Tanggung jawab manajemen terkait penyelenggaraan Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 33 huruf a paling sedikit meliputi: |  |
| 1. menetapkan kebijakan dan prosedur tertulis Rencana Pemulihan Bencana; |  |
| 1. menelaah dan menyetujui Rencana Pemulihan Bencana; |  |
| 1. melakukan evaluasi terhadap kelayakan Rencana Pemulihan Bencana milik pihak penyedia jasa Teknologi Informasi, dalam hal LJKNB menggunakan jasap ihak penyedia jasa Teknologi Informasi; dan |  |
| 1. menetapkan tingkat gangguan dan bencana serta pemulihannya. |  |
| 1. Tanggung jawab satuan kerja yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi sebagaimana dimaksud pada angka 33 huruf b paling sedikit meliputi: |  |
| 1. tanggung jawab penuh terhadap efektivitas penyelenggaraan Rencana Pemulihan Bencana; |  |
| 1. penentuan skenario pemulihan yang akan digunakan apabila terjadi gangguan atau bencana berdasarkan prioritisasi atas sistem yang dianggap kritis; dan |  |
| 1. evaluasi laporan mengenai setiap tahapan dalam pengujian dan pelaksanaan Rencana Pemulihan Bencana; |  |
| 1. Tanggung jawab satuan kerja pendukung sebagaimana dimaksud pada angka 33 huruf c paling sedikit meliputi: |  |
| 1. tanggung jawab terhadap penerapan Rencana Pemulihan Bencana; dan |  |
| 1. mendukung satuan kerja yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi. |  |
| 1. Uji coba Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 29 huruf e mencakup paling sedikit: |  |
| 1. frekuensi uji coba |  |
| 1. ruang lingkup uji coba; |  |
| 1. skenario uji coba; dan |  |
| 1. analisis, laporan, dan dokumentasi hasil uji coba. |  |
| 1. Dalam hal LJKNB menggunakan pihak penyedia jasa Teknologi Informasi, pelaksanaan uji coba sebagaimana dimaksud pada angka 29 huruf e harus melibatkan pihak penyedia jasa Teknologi Informasi yang bersangkutan. |  |
| 1. LJKNB harus melakukan pengkinian Rencana Pemulihan Bencana sebagaimana dimaksud pada angka 31 huruf e untuk meyakinkan kesesuaian proses bisnis, sumber daya manusia, dan sumber daya Teknologi Informasi dengan kondisi eksternal dan/atau internal saat ini dan mendatang. | . |
| 1. Kebijakan dan prosedur penggunaan pihak penyedia jasa Teknologi Informasi sebagaimana dimaksud pada angka 1 huruf g mencakup paling sedikit: |  |
| 1. 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; |  |
| 1. prinsip-prinsip penggunaan pihak penyedia jasa Tekonologi Informasi, yang paling sedikit berisi informasi mengenai: |  |
| 1. persetujuan dari manajemen; |  |
| 1. tanggung jawab tetap berada pada LJKNB; |  |
| 1. tidak menghambat proses pengawasan oleh Otoritas Jasa Keuangan; |  |
| 1. kerja sama yang dilakukan harus dituangkan dalam perjanjian tertulis; |  |
| 1. ruang lingkup perjanjian kerja sama, yang berisi paling sedikit tentang: |  |
| 1. cakupan pekerjaan; |  |
| 1. biaya dan jangka waktu perjanjian kerja sama; |  |
| 1. kepemilikan dan hak cipta; |  |
| 1. batasan risiko yang ditanggung oleh LJKNB dan pihak penyedia jasa Teknologi Informasi, termasuk yang diakibatkan perubahan antara lain: |  |
| 1. ruang lingkup perjanjian kerja sama; |  |
| 1. ruang lingkup bisnis dan organisasi pihak penyedia jasa Teknologi Informasi; |  |
| 1. aspek hukum antara lain regulasi, hak cipta, dan paten, |  |
| 1. larangan bagi pihak penyedia jasa Teknologi Informasi untuk menggunakan atau mengungkapkan informasi yang dimiliki LJKNB; |  |
| 1. *service level agreement* yang memuat standar kinerja dari pihak penyedia jasa Teknologi Informasi antara lain mengenai tingkat pelayanan yang diperjanjian dan target kinerja; |  |
| 1. klausula yang menyatakan bahwa: |  |
| 1. *service level agreement* tetap berlaku dalam hal terjadi perubahan kepemilikan pada LJKNB atau pihak penyedia jasa Teknologi Informasi; |  |
| 1. pihak penyedia jasa Teknologi Informasi tidak dapat memodifikasi perangkat lunak yang telah disepakati dalam perjanjian tanpa persetujuan dari kedua belah pihak; |  |
| 1. pihak penyedia jasa Teknologi Informasi harus melakukan *transfer of knowledge* kepada LJKNB; |  |
| 1. terdapat jaminan yang menyatakan bahwa pihak penyedia jasa Teknologi Informasi tetap mendukung jasa yang diberikan kepada LJKNB selama jangka waktu tertentu setelah implementasi; |  |
| 1. hanya dapat melakukan pengalihan sebagian kegiatan (subkontrak) berdasarkan persetujuan LJKNB yang dibuktikan dengan dokumen tertulis; |  |
| 1. 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 |  |
| 1. 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 |  |
| 1. jaminan ketersediaan akses ke kode sumber dalam hal: |  |
| 1. perangkat lunak dinilai penting oleh LJKNB; |  |
| 1. diperlukan modifikasi yang tidak dapat dilakukan oleh pihak penyedia jasa Teknologi Informasi; dan/atau |  |
| 1. penyedia jasa Teknologi Informasi tidak dapat memberikan layanan lagi, |  |
| 1. 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; |  |
| 1. sanksi dan/atau penalti terhadap pembatalan dan/atau pelanggaran perjanjian kerja sama; |  |
| 1. kepatuhan terhadap ketentuan dan peraturan perundang-undangan termasuk penyelesaian sengketa dalam hal terjadi perselisihan; |  |
| 1. mekanisme uji tuntas, yang meliputi analisis paling sedikit atas: |  |
| 1. eksistensi, riwayat, kualifikasi, latar belakang, dan reputasi pihak penyedia jasa Teknologi Informasi; |  |
| 1. kondisi keuangan pihak penyedia jasa Teknologi Informasi; |  |
| 1. kemampuan dan efektivias pemberian jasa, termasuk dukungan purna jual; dan |  |
| 1. penerapan manajemen risiko pihak penyedia jasa Teknologi Informasi; |  |
| 1. penggunaan pihak penyedia jasa Teknologi Informasi harus memberikan manfaat yang lebih besar dibandingkan dengan biaya yang dikeluarkan LJKNB; dan |  |
| 1. penentuan pihak penyedia jasa Teknologi Informasi, yang berisi paling sedikit mengenai mekanisme seleksi. |  |
| 1. Kebijakan dan prosedur Layanan Keuangan Elektronik sebagaimana dimaksud pada angka 1 huruf h memuat paling sedikit: |  |
| 1. cakupan dan deskripsi Layanan Keuangan Elektronik; dan |  |
| 1. tanggung jawab dan kewenangan pengelolaan Layanan Keuangan Elektronik. |  |
| 1. KECUKUPAN PROSES IDENTIFIKASI, PENGUKURAN, PENGENDALIAN, DAN PEMANTAUAN RISIKO PENGGUNAAN TEKNOLOGI INFORMASI |  |
| 1. Proses identifikasi, pengukuran, pengendalian, dan pemantauan risiko penggunaan Teknologi Informasi dilakukan paling sedikit terhadap aspek: |  |
| 1. manajemen; |  |
| 1. pengembangan dan pengadaan; |  |
| 1. operasional Teknologi Informasi; |  |
| 1. jaringan komunikasi; |  |
| 1. pengamanan informasi; |  |
| 1. Rencana Pemulihan Bencana; |  |
| 1. penggunaan pihak penyedia jasa Teknologi Informasi; dan |  |
| 1. Layanan Keuangan Elektronik, bagi LJKNB yang menyelenggarakan Layanan Keuangan Elektronik. |  |
| 1. LJKNB harus memiliki pendekatan manajemen risiko yang terpadu atau terintegrasi untuk dapat melakukan identifikasi, pengukuran, pengendalian, dan pemantauan risiko secara efektif. |  |
| 1. Proses identifikasi risiko sebagaimana dimaksud pada Romawi VI angka 1 mencakup paling sedikit langkah – langkah sebagai berikut: |  |
| 1. 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; |  |
| 1. pengaduan atau keluhan yang disampaikan pengguna Teknologi Informasi kepada satuan kerja penyelenggara Teknologi Informasi dan/atau *help desk*; |  |
| 1. temuan audit terkait penyelenggaraan Teknologi Informasi; |  |
| 1. hasil uji tuntas terhadap kinerja pihak penyedia jasa Teknologi Informasi; dan |  |
| 1. hasil penilaian sendiri yang dilakukan oleh satuan kerja penyelenggara Teknologi Informasi terkait penyelenggaraan Teknologi Informasi, jika ada, dan |  |
| 1. analisis risiko yang berkaitan dengan dampak potensial dari setiap risiko, seperti *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*. |  |
| 1. Proses pengukuran risiko sebagaimana dimaksud pada Romawi VI angka 1 memperhatikan kategori berikut: |  |
| 1. *accept*, yaitu LJKNB memutuskan untuk menerima risiko jika besarnya dampak yang ditimbulkan masih dalam batas toleransi; |  |
| 1. *control*, yaitu LJKNB memutuskan untuk mengurangi dampak yang ditimbulkan maupun kemungkinan terjadinya risiko; |  |
| 1. *avoid*, yaitu LJKNB memutuskan untuk tidak melakukan suatu aktivitas atau memilih alternatif aktivitas lain yang menghasilkan *output* yang sama untuk menghindari terjadinya risiko; |  |
| 1. *transfer*, yaitu LJKNB memutuskan untuk mengalihkan seluruh atau sebagian tanggung jawab penyelenggaraan Teknologi Informasi kepada pihak penyedia jasa Teknologi Informasi. |  |
| 1. Proses pengendalian risiko sebagaimana dimaksud pada Romawi VI angka 1 dilakukan secara keseluruhan dengan memperhatikan paling sedikit: |  |
| 1. hasil identifikasi risiko sebagaimana dimaksud pada romawi VI angka 3; |  |
| 1. kategori pengukuran risiko sebagaimana dimaksud pada romawi VI angka 4; dan |  |
| 1. peraturan perundang-undangan. |  |
| 1. 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. |  |
| 1. Proses pemantauan risiko sebagaimana dimaksud pada Romawi VI angka 1 terhadap proses pengendalian risiko sebagaimana dimaksud pada Romawi VI angka 5 dengan melakukan evaluasi kesesuaian, kecukupan, dan efektivitas kinerja penyelenggaraan Teknologi Informasi. |  |
|  |  |
| 1. SISTEM PENGENDALIAN INTERNAL ATAS PENGGUNAAN TEKNOLOGI INFORMASI |  |
| 1. LJKNB harus melaksanakan sistem pengendalian internal yang memuat paling sedikit: |  |
| 1. pengawasan oleh manajemen; |  |
| 1. identifikasi dan penilaian risiko; |  |
| 1. kegiatan pengendalian dan pemisahan fungsi; |  |
| 1. sistem informasi, sistem akuntansi, dan sistem komunikasi; dan |  |
| 1. kegiatan pemantauan dan koreksi penyimpanganyang dilakukan oleh: |  |
| 1. satuan kerja penyelenggara dan pengguna Teknologi Informasi; |  |
| 1. satuan kerja atau fungsi yang membawahkan audit internal; dan/atau |  |
| 1. pihak lain. |  |
| 1. Sistem informasi, sistem akuntansi, dan sistem komunikasi sebagaimana dimaksud pada Romawi VII angka 1 harus didukung oleh teknologi, sumber daya manusia, dan struktur organisasi LJKNB yang memadai. |  |
| 1. Kegiatan pemantauan dan koreksi penyimpangan sebagaimana dimaksud pada Romawi VII angka 1 huruf e paling sedikit: |  |
| 1. kegiatan pemantauan secara terus menerus; |  |
| 1. pelaksanaan fungsi audit internal yang efektif dan menyeluruh; dan |  |
| 1. 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. |  |
| 1. Pelaksanaan fungsi audit internal yang efektif dan menyeluruh sebagaimana dimaksud pada romawi VII angka 3 mencakup paling sedikit: |  |
| 1. latar belakang dan tujuan pelaksanaan audit; |  |
| 1. tugas dan tanggung jawab auditor; |  |
| 1. kewenangan auditor; |  |
| 1. proses audit; dan |  |
| 1. tindak lanjut atas hasil audit. |  |
|  |  |
| 1. 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: |  |
| 1. laporan sebagaimana dimaksud dalam Pasal 21 ayat (6) huruf a; |  |
| 1. permohonan persetujuan penempatan Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sebagaimana dimaksud dalam Pasal 23 ayat (3); dan/atau |  |
| 1. 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 (*online*) melalui sistem jaringan komunikasi data Otoritas Jasa Keuangan. |  |
| 1. 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: |  |
| 1. diserahkan langsung; atau |  |
| 1. dikirim melalui perusahaan jasa pengiriman. |  |
| 1. Penyampaian laporan sebagaimana dimaksud pada angka 2 dilengkapi surat pengantar dalam bentuk cetak (*hardcopy*) yang ditandantangani oleh Direksi. |  |
| 1. Selain penyampaian laporan sebagaimana dimaksud pada angka 1, LJKNB dapat menyampaikan laporan perkembangan kondisi terkini terkait Teknologi Informasi. |  |
| 1. Laporan sebagaimana dimaksud pada angka 1 huruf b dan angka 4 adalah sebagaimana diatur pada lampiran. |  |
| 1. Penyampaian surat pengantar sebagaimana dimaksud pada angka 3, laporan sebagaimana dimaksud pada angka 1 huruf a dan huruf c, permohonan persetujuan sebagaimana dimaksud pada angka 1 huruf b, dan/atau laporan sebagaimana dimaksud pada angka 4 ditujukan kepada direktur pengawasan masing-masing LJKNB. |  |
| 1. LJKNB dinyatakan telah menyampaikan laporan sebagaimana dimaksud pada angka 1 huruf a dan huruf c, permohonan persetujuan sebagaimana dimaksud pada angka 1 huruf b, dan/atau laporan sebagaimana dimaksud pada angka 4, dengan ketentuan sebagai berikut: |  |
| 1. untuk penyampaian secara dalam jaringan (*online*) melalui sistem jariangan komunikasi data Otoritas Jasa Keuangan, dibuktikan dengan tanda terima dari sistem jariangan komunikasi data Otoritas Jasa Keuangan; atau |  |
| 1. untuk penyampaian secara luar jaringan (*offline*) dibuktikan dengan tanda terima dari Otoritas Jasa Keuangan. |  |
| 1. PENUTUP |  |
| Ketentuan dalam Surat Edaran Otoritas Jasa Keuangan ini berlaku sesuai dengan pemberlakuan 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  KEPALA EKSEKUTIF PENGAWAS PERUSAHAAN PERASURANSIAN, DANA PENSIUAN, LEMBAGA PEMBIAYAAN, DAN LEMBAGA JASA KEUANGAN LAINNYA  OTORITAS JASA KEUANGAN,  RISWINANDI |  |