Yth.

1. Penyelenggara Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi; dan
2. Pengguna Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi,

di tempat.

SALINAN

SURAT EDARAN OTORITAS JASA KEUANGAN

NOMOR 18 /SEOJK.02/2017

TENTANG

TATA KELOLA DAN MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA LAYANAN PINJAM MEMINJAM UANG BERBASIS TEKNOLOGI INFORMASI

Sehubungan dengan berlakunya Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi, perlu untuk mengatur ketentuan pelaksanaan mengenai Tata Kelola Dan Manajemen Risiko Teknologi Informasi Pada Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi dalam Surat Edaran Otoritas Jasa Keuangan sebagai berikut:

I. KETENTUAN UMUM

1. Otoritas Jasa Keuangan yang selanjutnya disingkat OJK adalah lembaga yang independen, yang mempunyai fungsi, tugas, dan wewenang pengaturan, pengawasan, pemeriksaan, dan penyidikan sebagaimana dimaksud dalam Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan.
2. Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi adalah penyelenggaraan layanan jasa keuangan untuk mempertemukan pemberi pinjaman dengan penerima pinjaman dalam rangka melakukan perjanjian pinjam meminjam dalam mata uang rupiah secara langsung melalui sistem elektronik dengan menggunakan jaringan internet.
3. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengelola, menganalisis, menyimpan, menampilkan, mengumumkan,

mengirimkan, dan/atau menyebarkan informasi elektronik di bidang layanan jasa keuangan.

4. Penyelenggara Sistem Elektronik adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.
5. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi di bidang layanan jasa keuangan.
6. Penyelenggara Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi yang selanjutnya disebut Penyelenggara adalah badan hukum Indonesia yang menyediakan, mengelola, dan mengoperasikan Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi.
7. Pengguna Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi untuk selanjutnya disebut sebagai Pengguna adalah pemberi pinjaman dan penerima pinjaman yang menggunakan Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi.
8. Direksi:
   a. bagi Penyelenggara yang berbentuk badan hukum perseroan terbatas adalah direksi sebagaimana dimaksud dalam Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas; atau
   b. bagi Penyelenggara yang berbentuk badan hukum koperasi adalah pengurus sebagaimana dimaksud dalam Undang-Undang Nomor 25 Tahun 1992 Tentang Perkoperasian.
9. Komisaris:
   a. bagi Penyelenggara yang berbentuk badan hukum perseroan terbatas adalah komisaris sebagaimana dimaksud dalam Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas; atau
   b. bagi Penyelenggara yang berbentuk badan hukum koperasi adalah pengawas sebagaimana dimaksud dalam Undang-Undang Nomor 25 Tahun 1992 tentang Perkoperasian.
10. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya sebagaimana dimaksud dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

11. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
12. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi, atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi sebagaimana dimaksud dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
13. Penyelenggara Tanda Tangan Elektronik adalah badan hukum yang berfungsi sebagai pihak terpercaya yang memfasilitasi pembuatan Tanda Tangan Elektronik.
14. Pusat Data adalah suatu fasilitas yang digunakan untuk menempatkan Sistem Elektronik dan komponen terkaitnya untuk keperluan penempatan penyimpanan dan pengolahan data.
15. Pusat Pemulihan Bencana adalah suatu fasilitas yang digunakan untuk memulihkan kembali data atau informasi serta fungsi-fungsi penting Sistem Elektronik yang terganggu atau rusak akibat terjadinya bencana yang disebabkan oleh alam atau manusia
16. Rencana Pemulihan Bencana adalah dokumen yang berisikan rencana dan langkah-langkah untuk menggantikan dan/atau memulihkan kembali akses data, perangkat keras dan perangkat lunak yang diperlukan, agar Penyelenggara dapat menjalankan kegiatan operasional bisnis yang kritikal setelah adanya gangguan dan/atau bencana.

II. PERAN DAN TANGGUNG JAWAB DIREKSI

1. Direksi melakukan pengawasan terhadap risiko Teknologi Informasi dan memastikan fungsi Teknologi Informasi mampu untuk mendukung strategi dan tujuan bisnis dari Penyelenggara.
2. Direksi bertanggungjawab terhadap risiko Teknologi Informasi yang timbul dari kegiatan yang paling sedikit meliputi:
    a. pengambilan keputusan yang terkait dengan Teknologi Informasi;
    b. pengalihkelolaan Teknologi Informasi;
    c. pengamanan Teknologi Informasi;

d. perlindungan data dan informasi; dan/atau
e. pengelolaan layanan Teknologi Informasi.

3. Direksi menyusun kerangka kerja manajemen risiko Teknologi Informasi.
4. Direksi bertanggungjawab terhadap pelaksanaan manajemen risiko Teknologi Informasi agar aman, dapat dipercaya, berkelanjutan, dan stabil.
5. Direksi bertanggung jawab terhadap kualitas informasi produk dan layanan yang disampaikan kepada Pengguna dengan memperhatikan prinsip yang paling sedikit meliputi:
   a. keterbukaan;
   b. akurat;
   c. objektif;
   d. terpercaya;
   e. ketersediaan;
   f. mudah dipahami;
   g. integritas; dan
   h. kelengkapan.

III. PUSAT DATA DAN PUSAT PEMULIHAN BENCANA

A. Penempatan Pusat Data dan Pusat Pemulihan Bencana

Penyelenggara menempatkan Sistem Elektronik pada Pusat Data dan Pusat Pemulihan Bencana di wilayah Indonesia sesuai peraturan perundang-undangan yang berlaku.

B. Rencana Pemulihan Bencana

1. Penyelenggara harus menyusun Rencana Pemulihan Bencana agar kelangsungan operasional Penyelenggara dapat tetap berjalan saat terjadi bencana dan/atau gangguan pada sarana Teknologi Informasi yang digunakan oleh Penyelenggara.
2. Penyelenggara dapat melakukan uji coba atas Pusat Pemulihan Bencana terhadap seluruh aplikasi dan infrastruktur yang kritikal sesuai dengan Rencana Pemulihan Bencana.
3. Penyelenggara melakukan kaji ulang Rencana Pemulihan Bencana paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
4. Penyelenggara menyampaikan laporan tahunan terkait dengan Rencana Pemulihan Bencana dan Pusat Pemulihan Bencana kepada Kepala Eksekutif Pengawas Perasuransian, Dana

Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya.

IV. TATA KELOLA SISTEM ELEKTRONIK DAN TEKNOLOGI INFORMASI

A. Rencana Strategis Sistem Elektronik

1. Penyelenggara mendaftarkan diri sebagai Penyelenggara Sistem Elektronik pada Kementerian Komunikasi dan Informatika Republik Indonesia.
2. Penyelenggara harus menyusun dan memiliki rencana strategis Sistem Elektronik yang mendukung rencana bisnis Penyelenggara.
3. Rencana strategis Sistem Elektronik sebagaimana dimaksud pada angka 1 harus dicantumkan dalam rencana bisnis Penyelenggara.
4. Rencana strategis Sistem Elektronik Penyelenggara antara lain terkait kebijakan, prosedur, dan standar paling sedikit meliputi aspek:
   a. manajemen;
   b. pengembangan dan perencanaan;
   c. operasional Teknologi Informasi;
   d. jaringan komunikasi;
   e. pengamanan informasi;
   f. rencana pemulihan bencana;
   g. layanan Pengguna; dan
   h. penggunaan pihak penyedia jasa Teknologi Informasi.
5. Kebijakan, prosedur, dan standar yang sudah disusun harus disosialisasikan kepada pegawai serta pihak yang berkepentingan.
6. Kebijakan, prosedur, dan standar yang sudah disusun harus dilakukan *review* secara berkala untuk memastikan efektivitas dan kecukupannya.

B. Sumber Daya Manusia.

1. Penyelenggara wajib memiliki sumber daya manusia yang memiliki keahlian dan/atau latar belakang di bidang Teknologi Informasi.

2. Penyelenggara harus menyusun perencanaan sumber daya manusia dan kebutuhan kompetensinya di bidang Teknologi Informasi.
3. Penyelenggara harus memastikan bahwa kompetensi yang dibutuhkan dapat dipenuhi dengan baik guna menjamin keberlangsungan operasional dari Penyelenggara.
4. Penyelenggara harus meningkatkan kualitas dan kemampuan sumber daya manusia Penyelenggara baik melalui kegiatan pendidikan dan pelatihan yang berkaitan dengan penyelenggaraan Teknologi Informasi maupun proses bisnis dan layanan yang ditawarkan.

C. Pengelolaan Perubahan Teknologi Informasi

1. Penyelenggara harus memiliki prosedur yang mengelola setiap perubahan yang terjadi pada proses bisnis dan Sistem Elektronik.
2. Penyelenggara harus menentukan pembagian tanggung jawab dalam mengelola setiap perubahan yang terjadi pada proses bisnis dan Sistem Elektronik.
3. Penyelenggara harus memastikan setiap perubahan yang terjadi pada proses bisnis dan Sistem Elektronik telah mendapat persetujuan secara formal.
4. Penyelenggara harus mampu mengendalikan setiap perubahan yang terjadi pada proses bisnis dan Sistem Elektronik.
5. Penyelenggara harus mendokumentasikan serta menyampaikan kepada Kepala Eksekutif Pengawas Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya secara berkala setiap 3 (tiga) bulan paling lambat pada tanggal 30 atau dalam hal terjadi perubahan pada proses bisnis dan Sistem Elektronik.
6. Dalam hal tanggal 30 sebagaimana dimaksud pada angka 5 jatuh pada hari libur, maka penyampaian dilakukan paling lambat 1 (satu) hari kerja berikutnya.
7. Penyelenggara harus melakukan pemisahan antara zona operasional dan pengembangan guna memastikan setiap perubahan yang terjadi tidak mengganggu operasional Sistem Elektronik.

8. Penyelenggara harus memastikan personil yang mengakses zona operasional terdokumentasi dan telah mendapat persetujuan Direksi.

V. ALIH KELOLA TEKNOLOGI

1. Penyelenggara dapat menggunakan penyedia alih kelola Teknologi Informasi untuk mendukung kegiatan bisnis Penyelenggara.
2. Penyedia alih kelola Teknologi Informasi antara lain penyedia yang bergerak di bidang jasa pengembangan sistem, jasa pemeliharaan, jasa pendukung operasional, jasa administrasi jaringan, jasa pemulihan bencana, dan komputasi awan (*cloud computing*).
3. Dalam hal Penyelenggara menggunakan pihak penyedia alih kelola Teknologi Informasi, Penyelenggara memiliki tanggung jawab sepenuhnya terhadap risiko yang terjadi dari dan pada Teknologi Informasi yang dialihkelolakan.
4. Penggunaan penyedia alih kelola Teknologi Informasi harus memperhatikan prinsip kehati-hatian, keberlangsungan, dan manajemen risiko yang paling sedikit meliputi:
   a. risiko yang berkaitan dengan penggunaan dan/atau akuisisi dari Sistem Elektronik dengan mempertimbangkan kemampuan dan keandalan;
   b. risiko yang berkaitan dengan rekam jejak, keberlangsungan bisnis, dan neraca keuangan dari penyedia jasa;
   c. memastikan bahwa syarat dan ketentuan kontraktual yang mengatur peran, hubungan, kewajiban, dan tanggung jawab semua pihak diatur sepenuhnya dalam perjanjian yang paling sedikit mencakup target kinerja, tingkat layanan, ketersediaan, keandalan, kapasitas, kepatuhan, audit, keamanan, perencanaan penanggulangan bencana, kemampuan pemulihan bencana, fasilitas pengolahan cadangan, dan pilihan hukum (*choice of law*);
   d. memastikan bahwa penyedia layanan jasa Teknologi Informasi dapat memberikan akses terhadap informasi kepada semua pihak yang ditentukan oleh Penyelenggara serta lembaga pengawas dan pengatur sektor untuk tujuan pengaturan, audit, atau kepatuhan; dan

e. mampu melakukan pengawasan dan evaluasi atas pelaksanaan kegiatan Penyelenggara yang diselenggarakan oleh pihak penyedia jasa secara berkala yang menyangkut kinerja, reputasi penyedia jasa, dan kelangsungan penyediaan layanan.

5. Penyelenggara memastikan pihak penyedia jasa Teknologi Informasi:
   a. memiliki tenaga ahli yang memiliki keandalan dengan didukung oleh sertifikat keahlian secara akademis dan/atau secara profesional sesuai dengan keperluan penyelenggaraan Teknologi Informasi;
   b. menerapkan prinsip pengendalian Teknologi Informasi secara memadai yang dibuktikan dengan hasil audit yang dilakukan pihak independen;
   c. sebagai pihak terafiliasi, menjaga keamanan seluruh informasi termasuk rahasia Penyelenggara dan data pribadi nasabah;
   d. melaporkan kepada Penyelenggara setiap kejadian kritis yang dapat mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelancaran operasional Penyelenggara;
   e. menyampaikan hasil audit Teknologi Informasi yang dilakukan oleh auditor independen secara berkala kepada Kepala Eksekutif Pengawas Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya melalui Penyelengggara yang bersangkutan;
   f. menyediakan Rencana Pemulihan Bencana yang teruji dan memadai;
   g. mematuhi klausula mengenai pemutusan perjanjian sebelum jangka waktu berakhir (*early termination*) sebagaimana dimuat dalam perjanjian antara Penyelenggara dengan penyedia alih kelola Teknologi Informasi; dan
   h. memenuhi tingkat layanan sesuai dengan *service level agreement* antara Penyelenggara dan pihak penyedia jasa Teknologi Informasi.

6. Penyelenggara menyampaikan kepada Kepala Eksekutif Pengawas Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya hasil penilaian atas penerapan manajemen risiko pada pihak penyedia jasa Teknologi Informasi secara berkala setiap 3 (tiga) bulan paling lambat pada tanggal 30.

7. Dalam hal tanggal 30 sebagaimana dimaksud pada angka 6 jatuh pada hari libur, maka penyampaian dilakukan paling lambat 1 (satu) hari kerja berikutnya.
8. Penyelenggara memastikan pemusnahan data dan informasi pada saat pergantian penyedia alih kelola Teknologi Informasi sesuai dengan Surat Edaran OJK ini.
9. Penyelenggara menyusun laporan penggunaan alih kelola dan menyampaikan kepada Kepala Eksekutif Pengawas Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya.

VI. PENGELOLAAN DATA DAN INFORMASI

1. Penyelenggara dilarang untuk menyebarkan data dan informasi pribadi Pengguna kepada pihak lainnya.
2. Data dan informasi pribadi Pengguna sebagaimana dimaksud pada angka 1 paling sedikit meliputi:
   a. data dan informasi yang melekat dan dapat diidentifikasi:
      1) perseorangan seperti:
         a. nama;
         b. alamat domisili;
         c. kartu identitas (KTP, SIM, Paspor);
         d. Nomor Pokok Wajib Pajak (NPWP);
         e. tanggal lahir dan/atau umur;
         f. alamat *email;*
         g. IP address;
         h. nomor telepon;
         i. nomor rekening;
         j. nama ibu kandung;
         k. nomor kartu kredit;
         l. identitas digital (Biometrik);
         m. tanda tangan;
         n. riwayat pendidikan;
         o. riwayat pekerjaan;
         p. rekening koran;
         q. daftar harta kekayaan;
         r. data dan informasi terkait lainnya;

2) korporasi:
   a) nama korporasi;
   b) alamat;
   c) nomor telepon;
   d) susunan direksi dan komisaris termasuk dokumen identitas berupa KTP/Paspor/izin tinggal;
   e) susunan pemegang saham;
   f) nomor rekening;
   g) rekening koran;
   h) daftar aset;
   i) dokumen perusahaan;
   j) data dan informasi terkait lainnya;

b. data dan informasi non-publik yang bersifat material:
   1) laporan keuangan;
   2) kinerja usaha;
   3) keputusan manajemen;
   4) jumlah pelanggan;
   5) data dan informasi terkait lainnya;

c. data dan informasi terkait transaksi keuangan; dan

d. data dan informasi terkait kontrak/perjanjian.

3. Larangan sebagaimana dimaksud pada angka 1 dikecualikan dalam hal:
   a. Pengguna memberikan persetujuan tertulis; dan/atau
   b. diwajibkan oleh peraturan perundang-undangan yang berlaku.
4. Dalam hal Pengguna memberikan persetujuan tertulis sebagaimana dimaksud pada angka 3 huruf a, Penyelenggara dapat memberikan data dan/atau informasi pribadi Pengguna dan memastikan pihak ketiga dimaksud tidak memberikan dan/atau menggunakan data dan/atau informasi pribadi Pengguna untuk tujuan selain yang disepakati antara Penyelenggara dengan pihak lainnya.
5. Tata cara persetujuan tertulis dari Pengguna dapat dinyatakan dalam bentuk antara lain:
   a. pilihan setuju atau tidak setuju; atau
   b. memberikan tanda persetujuan,

   dalam dokumen dan/atau perjanjian produk dan/atau layanan.

6. Data dan informasi sebagaimana dimaksud pada angka 2 harus diamankan melalui metode yang dapat memastikan proses pembacaan data dilakukan oleh pihak yang terotorisasi.
7. Data dan informasi Pengguna yang diperoleh dan dimanfaatkan oleh Penyelenggara harus memenuhi kriteria sebagai berikut:
    a. penyampaian batasan pemanfaatan data dan informasi kepada Pengguna serta memperoleh persetujuan dari Pengguna;
    b. penyampaian setiap perubahan tujuan pemanfaatan data dan informasi kepada Pengguna (apabila ada); dan
    c. media dan metode yang dipergunakan dalam memperoleh data dan informasi terjamin kerahasiaan, keamanan serta keutuhannya.
8. Data atau informasi Pengguna yang dimusnahkan oleh Penyelenggara harus memenuhi kriteria sebagai berikut:
    a. memperhatikan aspek retensi berdasarkan peraturan perundang-undangan yang berlaku dan kepentingan audit serta pemeriksaan dari otoritas pengawas dan pengatur sektor; dan
    b. memastikan tidak ada data dan informasi yang tertinggal, terkorelasi dan dapat dimanfaatkan kembali.
9. Penyelenggara mencegah adanya akses yang tidak sah terhadap data dan informasi.
10. Penyelenggara wajib menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi, data transaksi, dan data keuangan yang dikelolanya sejak data diperoleh hingga data tersebut dimusnahkan.

VII. PENGELOLAAN RISIKO TEKNOLOGI INFORMASI

1. Penyelenggara harus melaksanakan identifikasi, penilaian, dan mitigasi risiko yang paling sedikit mempertimbangkan:
    a. aset yang dimiliki;
    b. bisnis proses yang dilaksanakan;
    c. klasifikasi data dan informasi;
    d. penanggung jawab risiko;
    e. batasan risiko yang dapat diterima; dan
    f. penentuan penilaian dampak dan kemungkinan munculnya risiko.
2. Penyelenggara menentukan toleransi risiko yang menjadi acuan terhadap pengelolaan risiko.

3. Penyelenggara harus mengidentifikasi kemungkinan munculnya kekurangan dan/atau kecacatan dalam Sistem Elektronik sejak tahap perancangan, pengembangan, dan pengoperasian untuk mengantisipasi kegagalan pada Sistem Elektronik.
4. Untuk memastikan risiko Sistem Elektronik dapat terukur dan terkendali dengan baik maka Penyelenggara menetapkan kerangka kerja manajemen risiko Teknologi Informasi.
5. Penyelenggara melakukan pembaharuan berkala dan pemantauan analisa risiko untuk memastikan setiap perubahan pada Sistem Elektronik, infrastruktur Teknologi Informasi, atau operasional Teknologi Informasi dapat teridentifikasi.

VIII. PENGAMANAN SISTEM ELEKTRONIK

Penyelenggara memastikan pengamananan Sistem Elektronik dilaksanakan secara efektif dan berkesinambungan dengan memperhatikan hal-hal sebagai berikut:

1. Penyelenggara harus menyusun, menetapkan, dan mensosialisasikan kebijakan, prosedur, dan standar pengamanan Sistem Elektronik secara berkelanjutan;
2. pengamanan Sistem Elektronik harus memenuhi unsur kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*);
3. pengamanan Sistem Elektronik harus memperhatikan aspek teknologi, sumber daya manusia, dan pemanfaatan Teknologi Informasi;
4. pengamanan Sistem Elektronik yang diterapkan harus didasarkan pada hasil penilaian risiko;
5. ketersediaan manajemen penanganan insiden dalam pengamanan Sistem Elektronik.
6. pemantauan, penilaian, dan penanganan celah keamanan Teknologi Informasi secara rutin dan berkala terhadap Sistem Elektronik yang mendukung proses bisnis Penyelenggara dengan memperhatikan manajemen risiko;
7. Penyelenggara memastikan bahwa akses terhadap data dan informasi oleh pihak internal maupun eksternal memenuhi prinsip kehati-hatian dan prinsip akses terbatas.

IX. PENANGANAN INSIDEN DAN KETAHANAN TERHADAP GANGGUAN

Dalam hal penanganan insiden dan ketahanan terhadap gangguan, Penyelenggara:

1. memastikan prosedur penanganan insiden dan ketahanan terhadap gangguan yang terjadi paling sedikit mencakup:
   a. klasifikasi insiden;
   b. langkah-langkah penanganan insiden;
   c. pencatatan insiden; dan
   d. basis data masalah dan insiden;
2. menyusun dan menguji secara berkala rencana dan langkah spesifik yang perlu diambil ketika sebuah insiden dapat memberikan dampak signifikan pada operasional atau bisnis Penyelenggara;
3. memiliki perencanaan dan metode penyampaian informasi mengenai gangguan kepada pihak eksternal terkait untuk dapat menyelesaikan insiden dan/atau gangguan yang terjadi;
4. memiliki perencanaan dan metode untuk mengkomunikasikan insiden atau gangguan yang terjadi apabila hal tersebut memiliki imbas kepada pelanggan atau stakeholder lainnya;
5. menyediakan prosedur dan media bagi Pengguna untuk mengajukan keluhan perihal layanan yang diberikan oleh Penyelenggara;
6. menyediakan metode penyampaian informasi cadangan yang terpisah dan berbeda dari Sistem Elektronik yang dipergunakan untuk operasionalnya untuk mengantisipasi keadaan bencana.

X. PENGGUNAAN TANDA TANGAN ELEKTRONIK

1. Perjanjian Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi yang ditandatangani menggunakan Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sama dengan perjanjian yang ditandatangani dengan tinta basah.
2. Penyelenggara harus memiliki pegawai yang bertanggungjawab mengelola pemenuhan perjanjian Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi dengan menggunakan Tanda Tangan Elektronik.
3. Dalam rangka penggunaan Tanda Tangan Elektronik, Penyelenggara bekerjasama dengan Penyelenggara Tanda Tangan Elektronik.

4. Penyelenggara Tanda Tangan Elektronik sebagaimana dimaksud pada angka 3 memenuhi kualifikasi paling sedikit sebagai berikut:
   a. terdaftar di Kementerian Komunikasi dan Informatika Republik Indonesia;
   b. memiliki standar keamanan dan Teknologi Informasi sesuai dengan peraturan perundang-undangan yang berlaku;
   c. menyampaikan laporan berkala perihal kinerja dan hasil audit kepada Penyelenggara;
   d. memiliki kemampuan untuk mengamankan data Penyelenggara dan Pengguna dengan metode enkripsi dan menerapkan prinsip hak akses minimum;
   e. memiliki metode untuk menerbitkan, menghapus, dan mengganti Sertifikat Elektronik atas permintaan masing-masing Penyelenggara atau Pengguna;
   f. memiliki metode untuk melakukan verifikasi terhadap Tanda Tangan Elektronik yang sudah dibubuhkan serta Sertifikat Elektronik yang diterbitkan;
   g. dapat melakukan proses penandaan waktu untuk setiap proses penandatanganan elektronik; dan
   h. dapat melakukan proses pencabutan dan penerbitan ulang Sertifikat Elektronik yang bermasalah atas permintaan masing-masing Penyelenggara atau Pengguna.
5. Kualifikasi sebagaimana dimaksud pada angka 4 huruf b sampai dengan huruf h dibuktikan dengan hasil audit teknologi informasi yang dilakukan oleh auditor independen yang terpercaya dan memiliki reputasi internasional.
6. Kepala Eksekutif Pengawas Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya memberikan persetujuan atas pelaksanaan kerja sama antara Penyelenggara dengan Penyelenggara Tanda Tangan Elektronik sebagaimana dimaksud pada angka 3.
7. Dalam hal pemanfaatan Tanda Tangan Elektronik, Penyelenggara memperhatikan paling sedikit hal-hal sebagai berikut:
   a. proses integrasi antara Sistem Elektronik milik Penyelenggara dengan Penyelenggara Tanda Tangan Elektronik harus tetap dapat menjaga keaslian identitas para pihak yang melaksanakan Transaksi Elektronik;

b. proses integrasi antara Sistem Elektronik milik Penyelenggara dengan Penyelenggara Tanda Tangan Elektronik memastikan aspek keamanan dan tata kelola yang dimiliki oleh Penyelenggara tetap terjaga;
c. proses pengolahan, penyimpanan, serta pemanfaatan data Transaksi Elektronik harus memperhatikan prinsip integritas dari Transaksi Elektronik itu tetap terjaga; dan
d. menyampaikan hak dan tanggung jawab dari Pengguna yang memiliki dan mempergunakan Tanda Tangan Elektronik.

XI. KETERSEDIAAN LAYANAN DAN KEGAGALAN TRANSAKSI

1. Penyelenggara menetapkan dan menjalankan prosedur dan sarana untuk pengamanan Sistem Elektronik dalam menghindari gangguan, kegagalan, dan kerugian.
2. Penyelenggara menyediakan sistem pengamanan yang mencakup prosedur, sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian.
3. Dalam hal terjadi kegagalan atau gangguan sistem yang berdampak serius sebagai akibat perbuatan dari pihak lain terhadap Sistem Elektronik, Penyelenggara mengamankan data dan melaporkan kepada Kepala Eksekutif Pengawas Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya serta mengumumkan kepada Pengguna paling lambat 1 (satu) jam setelah terjadinya kegagalan atau gangguan sistem.
4. Penyelenggara memiliki saluran komunikasi alternatif untuk memastikan kelangsungan pelayanan kepada Pengguna.
5. Penyelenggara harus melakukan pemantauan dan evaluasi secara terus menerus agar keberlangsungan operasional dan layanan Teknologi Informasi berjalan dengan baik.

XII. KETERBUKAAN INFORMASI PRODUK DAN LAYANAN

1. Penyelenggara harus mencantumkan informasi produk dan layanan pada Sistem Elektronik yang digunakan oleh Penyelenggara.
2. Pencantuman informasi produk dan layanan harus memperhatikan paling sedikit hal-hal sebagai berikut:
   a. risiko yang terdapat pada produk dan layanan;
   b. uraian pokok produk yang ditawarkan;

c. pusat pengaduan; dan/atau

d. biaya yang timbul sehubungan dengan produk dan layanan.

XIII. RETENSI

Penyelenggara wajib menampilkan kembali data dan informasi secara utuh sesuai dengan format awal dengan tetap memperhatikan masa retensi berdasarkan ketentuan peraturan perundang-undangan yang berlaku.

XIV. PENUTUP

Ketentuan dalam Surat Edaran OJK ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 18 April 2017

WAKIL KETUA DEWAN KOMISIONER
OTORITAS JASA KEUNGAN

ttd

RAHMAT WALUYANTO

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Yuliana