PT. BPR PUSKOPAT
Kantor: Jalan Jendral Sudirman No 550 D KM 3,5 Palembang Telp (0711) 313077

SURAT KEPUTUSAN (SK) DIREKSI
PT. BPR PUSKOPAT

Nomor. 053/SK-DIREKSI/VII/2023

Tentang:

STANDAR PROSEDUR OPERASI (SPO) TEKNOLOGI INFORMASI

Menimbang :

1. Bahwa perlu segera mengeluarkan Surat Keputusan mengenai Standar Prosedur Operasi Teknologi Informasi.
2. Bahwa perlu segera mengimplementasikan sebagai pedoman pelaksanaan Unit Teknologi Informasi.
3. Bahwa untuk mengurangi risiko Bank wajib menerapkan prinsip kehati-hatian *(prudent)*.

Mengingat :

1. Akte Pendirian PT. BPR Puskopat nomor 133 tanggal 26 September 2007.
2. Keputusan Deputi Gubernur Bank Indonesia tentang pemberian izin usaha Nomor : 10/68/KEP.GBI/DpG/2008 tanggal 22 Oktober 2008

MEMUTUSKAN

MENETAPKAN:

1. Melakukan Standar Prosedur Operasi (SPO) dalam Unit Kerja Teknologi Informasi PT. BPR Puskopat sesuai dengan Ketentuan Peraturan Otoritas Jasa Keuangan.
2. Surat Keputusan ini berlaku sejak hari / tanggal ditetapkan. Dan Apabila dikemudian hari ternyata terdapat kekeliruan dalam surat keputusan ini, maka akan dibuat perbaikan atau perubahan sebagaimana mestinya.

Ditetapkan di: Palembang
Hari/ Tanggal: Jumat/ 21 Juli 2023

D I R E K S I
PT. Bank Perkreditan Rakyat Puskopat

Direktur Utama Yang Membawahkan Fungsi Kepatuhan	Direktur Bisnis
Dedy Mas Putra, ST., MM.	**Devid Arsiel, SE**

DIREKSI PT. BPR PUSKOPAT

Tembusan: 1. Dewan Komisaris
2. Arsip

Standar Prosedur Operasi (SPO)

TEKNOLOGI INFORMASI

PT BPR PUSKOPAT

21 Juli 2023

BAB I
PENDAHULUAN

LATAR BELAKANG

Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, memproses, mengumumkan, menganalisis dan atau menyebarkan informasi atau sebuah study perancangan, implementasi, pengembangan, dukungan atau managemen sistem informasi berbasis komputer terus pada aplikasi perangkat keras dan perangkat lunak.

Fungsi Kebijakan Teknologi Informasi pada PT. BPR Puskopat.

Kebijakan Teknologi Informasi PT. BPR Puskopat mempunyai fungsi yang sangat penting, yaitu untuk digunakan sebagai panduan dalam pelaksanaan semua kegiatan yang terkait dengan operasional perusahaan agar dapat berjalan baik/terhindar dari kesalahan. Dengan adanya Kebijakan Teknologi Informasi pada PT. BPR Puskopat diharapkan seluruh pejabat/karyawan yang menjalankan roda perusahaan dapat menerapkan setiap aturan secara lebih konsisten, disiplin dan berkesinambungan.

Tujuan Penyusunan Kebijakan Teknologi Informasi pada PT. BPR Puskopat

Tujuan penyusunan Kebijakan Teknologi Informasi pada PT. BPR Puskopat, yaitu untuk memberikan acuan atau panduan kepada pejabat/karyawan dalam proses penyelenggaraan informasi agar dapat berjalan secara efektif dan efisien. Disamping itu, dengan menerapkan kebijakan Teknologi Informasi ini secara konsekuen dan konsisten, diharapkan penyalahgunaan wewenang / kesalahan oleh pihak-pihak yang tidak bertanggungjawab dalam pelaksanaan operasional dapat dihindari.

Dasar Hukum Kebijakan Teknologi Informsi PT. BPR Puskopat.

Dasar hukum penyusunan Kebijakan Teknologi Informasi di PT. BPR Puskopat, adalah :

1. Peraturan Otoritas Jasa Keuangan Nomor 75/POJK.03/2016 tanggal 23 Desember 2016 tentang Standar Penyelenggara Teknologi Informasi Bagi Bank Perkreditan Rakyat.
2. Surat Edaran Otoritas Jasa Keuangan Nomor 15/SEOJK.03/2017 tanggal 06 April 2017 tentang Standar Penyelenggaraan Teknologi Informasi bagi Bank Perkreditan Rakyat

Ruang Lingkup Penyelenggaraan Teknologi Informasi

BPR yang memiliki modal inti kurang dari Rp 50 miliar, wajib menyelenggarakan teknologi informasi paling kurang berupa:

- Aplikasi Inti Perbankan (*Core Banking System*), dan
- Pusat Data (*Data Center*)

Sedangkan BPR yang memiliki modal inti paling sedikit Rp 50 miliar, wajib menyelenggarakan teknologi informasi paling kurang berupa:

- Aplikasi Inti Perbankan (*Core Banking System*),
- Pusat Data (*Data Center*), dan
- Pusat Pemulihan Bencana (*Disaster Recovery Center*)

Pusat data dan pusat pemulihan bencana wajib berada di wilayah Indonesia. Pusat pemulihan bencana wajib ditempatkan di lokasi dengan karakteristik risiko yang berbeda dengan Pusat data.

Kajian Berkala Kebijakan Teknologi Informasi PT. BPR Puskopat.

Perubahan/perbaikan terhadap kebijakan Teknologi Informasi, tidak terlepas dari hasil kajian berkala atas kebijakan-kebijakan yang ditetapkan oleh Otoritas Jasa Keuangan dan lembaga-lembaga keuangan lainnya dan akan dilakukan setiap saat atau disesuaikan dengan perubahan kebijakan Otoritas Jasa Keuangan terkait Teknologi Informasi

BAB II
KEBIJAKAN DAN PROSEDUR PENYELENGGARA TEKNOLOGI INFORMASI

2.1 WEWENANG DAN TANGGUNGJAWAB

I. DEWAN DIREKSI

a. Menetapkan rencana pengembangan dan pengadaan Teknologi Informasi BPR.
b. Menetapkan Kebijakan dan prosedur terkait penyelenggaraan Teknologi Informasi yang memadai.
c. Memantau kecukupan kinerja penyelenggaraan Teknologi Informasi dan upaya peningkatan.
d. memastikan bahwa:
   1. Teknologi Informasi yang digunakan mendukung perkembangan usaha, pencapaian tujuan bisnis dan kelangsungan pelayanan terhadap nasabah BPR.
   2. Terdapat kegiatan peningkatan kompetensi sumber daya manusia yang terkait dengan penyelenggaraan dan penggunaan Teknologi Informasi.
   3. Tersedianya sistem pengelolaan pengamanan informasi (information security management system) yang efektif dan dikomunikasikan kepada satuan kerja penyelenggara dan pengguna Teknologi Informasi.
   4. Kebijakan dan prosedur penyelenggaraan Teknologi Informasi diterapkan secara efektif.

II. DEWAN KOMISARIS

a. Mengarahkan dan memantau rencana pengembangan dan pengadaan Teknologi Informasi BPR yang bersifat mendasar.
b. Mengevaluasi pertanggungjawaban Direksi terkait penyelenggaraan Teknologi Informasi BPR

III. SATUAN KERJA TEKNOLOGI INFORMASI

1. Membantu Direksi dan Dewan Komisaris dalam penyelenggaran Teknologi Informasi terkait dengan perencanaan, pelaksanaan dan pemantauan.
2. Mendukung pengembangan dan/atau pengadaan Teknologi Informasi.
3. Mendukung implementasi, operasional, dan pemeliharaan Teknologi Informasi dan,
4. Melakukan upaya penyelesaian permasalahan terkait operasional Teknologi Informasi, yang tidak dapat diselesaikan oleh satuan kerja pengguna Teknologi Informasi.

IV. PENGGUNA TI

1. Bertanggungjawab atas integritas data/informasi (kelengkapan,akurasi,kebenaram dan keaslian)
2. Bertanggung jawab atas kerahasiaan penggunaan aplikasi TI dalam proses pekerjaan

3. Melaporkan kepada Fungsi TI jika terjadi gangguan atau eror pada aplikasi TI
4. Melaporkan kepada Direksi atau Fungsi TI apabila diduga adanya penggunaan aplikasi oleh pihak yang tidak berwenang atau adanya ancaman serangan terhadap TI yang digunakan oleh BPR
5. Mematuhi dan menerapkan prosedur pengamanan yang telah ditentukan

2.2 PENGEMBANGAN DAN PENGGADAAN TEKNOLOGI INFORMASI

Dalam Menjalankan Teknologi Informasi diperlukan sistem elektronik yang memadai. Adapun Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik,

Dalam melakukan pengembangan dan pengadaan Teknologi Informasi BPR dan wajib melakukan langkah-langkah pengendalian untuk menghasilkan sistem dan data yang terjaga kerahasiaan *(confidentiality)*, integritas *(integrity)*, dan ketersediaan *(availability)*, serta mendukung pencapaian tujuan BPR antara lain meliputi:

a. menetapkan dan menerapkan prosedur pengembangan dan pengadaan Sistem Elektronik secara konsisten
b. menerapkan manajemen proyek dalam pengembangan dan pengadaan Sistem Elektronik;
c. melakukan testing yang memadai pada saat pengembangan dan pengadaan Sistem Elektronik termasuk uji coba dengan melibatkan satuan kerja pengguna, untuk memastikan keakuratan dan berfungsinya Sistem Elektronik sesuai kebutuhan pengguna serta kesesuaian satu sistem dengan sistem yang lain;
d. melakukan dokumentasi terhadap pengadaan, pengembangan, dan pemeliharaan Sistem Elektronik
e. memiliki manajemen perubahan Sistem Elektronik;
f. memastikan Sistem Elektronik BPR mampu menampilkan kembali informasi secara utuh.

2.3 OPERASIONAL TEKNOLOGI INFORMASI

A. AKTIVITAS PENGELOLA USER

I. PENGELOLA USER

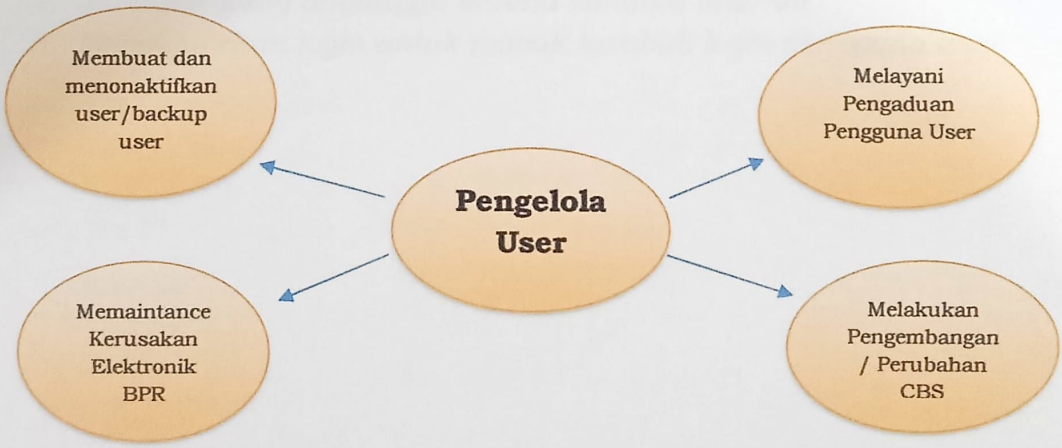
Pengelola User adalah Pengguna yang diberikan hak untuk mengelola *Core Banking System(CBS)* BPR sesuai dengan Kebutuhan BPR dan pengembangan bisnis.

Setiap pengelolaan dilakukan sesuai dengan Ketentuan dan Aturan yang berlaku. Adapun pengelola User pada CBS BPR adalah ***Staf IT dan pengembangan bisnis***

II. TUGAS DAN WEWENANG PENGELOLA USER

1. Melakukan perubahan-perubahan terkait Core Banking System sesuai dengan Ketentuan Internal yang berlaku dengan melampiri Berita Acara dari Unit IT dan Pengembangan Bisnis yang diketahui oleh Kabag Umum dan SDM.
2. Melakukan perubahan-perubahan atau pengembangan terkait Core Banking System sesuai dengan Kebutuhan BPR dengan melengkapi analisa dari Unit IT dan pengembangan bisnis yang disetujui oleh Direksi.
3. Melakukan koordinasi ke vendor terkait permasalahan Core Banking System (CBS) yang tidak BPR dapat diselesaikan oleh pengelola User melalui Helpdesk.
4. Melayani pengaduan dari semua pengguna dan melaksanakan sistem pelayanan bantuan permasalahan operasional sistem terkait Core Banking System bagi semua pengguna.
5. Melakukan tugas lain yang diperintahkan oleh Atasan dalam bidang IT dan pengembangan bisnis.
6. Melakukan pengaktifan dan pengnonaktifan Aktivitas Backup User dan aktivitas pengguna user pada saat Kepala Bagian dalam kondisi berhalangan hadir.

Gambar A.2 Flowchart



III. TEKNIS PENGELOLA USER

A. PERMINTAAN USER/PENONAKTIFAN USER

I. Permintaan User

- *Mengajukan permohonan dengan melampirkan laporan internal dari Kepala Bagian di fungsi terkait kepada Direksi*
- *Pengelola User bertindak sesuai dengan terkait Hasil Keputusan Direksi*

- *User dibuat setelah Staff IT dan Pengembangan bisnis mendapatkan lembaran persetujuan dari Direksi*

II. Penonaktifan User

a. *Kepala Bagian bertugas menonaktifkan user apabila pengguna user berhalangan hadir atau tidak digunakan lagi.*
b. *Staff IT dan pengembangan bisnis tetap memperhatikan aktivitas user pengguna yang dinonaktifkan*

B. *PERUBAHAN/PENAMBAHAN MENU PADA CBS PENGGUNA USER*

- *Pengelola user menerima Instruksi dari Direksi berupa lembaran persetujuan untuk melakukan perubahan/penambahan menu pada CBS Pengguna User*

C. *PERBAIKAN KERUSAKAN CBS*

- *Pengelola user menerima Instruksi dari Direksi berupa lembaran persetujuan untuk melakukan perbaikan kerusakan CBS Pengguna User*

D. *PELAYANAN PENGADUAN PENGGUNA USER*

- *Permasalahan seputar Teknologi Informasi dan Elektronik pengelola dapat segera melakukan penyelesaian terkait pengaduan pengguna user dengan diketahui Kepala Bagian Umum dan SDM seperti antara lain :*
  1. *Jaringan yang terganggu karena kendala internal*
  2. *Mengeluarkan login untuk masuk kembali login pengguna user*

B. AKTIVITAS PENGGUNA USER

I. PENGGUNA USER

Pengguna User adalah Pengguna yang diberikan hak untuk menggunakan atau memanfaatkan user sesuai dengan jabatan dan kewenangan.

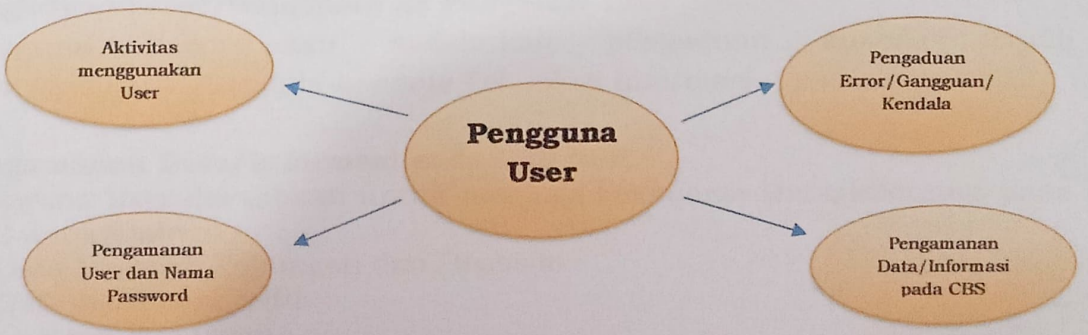
Adapun Pengguna User adalah Sebagai Berikut :

No	Departemen	Jabatan
1	Direktur Operasional Kepatuhan	Direktur Utama
2	Direktur Bisnis	Direktur
3	Bagian Operasional	Kepala Bagian Operasional, Inklusi Keuangan dan Literasi
4	Unit Customer Service	Customer Service
5	Unit Kas	Kepala Seksi Pelayanan Marketing dan Administrasi Dana
6	Unit Kas	Teller
7	Bagian Marketing	Kepala Seksi Penagihan dan Administasi Umum
8	Unit Marketing	Kepala Bagian Bisnis
9	Unit Marketing	Kepala Seksi Bisnis
10	Unit Marketing	Account Officer
11	Unit Marketing	Account Officer
12	Unit Back Office	Kepala Bagian Umum dan SDM
13	Unit Back Office	Kepala Bagian Akuntansi
14	Unit Back Office	Staf Akutansi
15	Unit Back Office	Staf IT dan Pengembangan Bisnis
16	Unit EDP	
17	Kepatuhan,Manrisk dan APU PPT	Kepala Bagian Manrisk, Kepatuhan, APU PPT
18	SPI	Kepala Bagian SPI

II. TUGAS DAN WEWENANG PENGGUNA USER

1. Menggunakan User sesuai dengan user yang disediakan dan kewenangan yang diberikan
2. Melakukan pengaduan sebagai pengguna user ke bagian pengelola user apabila terdapat kendala/gangguan/error pada Core Banking System BPR
3. Menjaga kerahasiaan *Core Banking Sytem* (CBS) yang digunakan atau bertanggungjawab atas integritas data/informasi.
4. Menjaga kerahasiaan *Password* pada *User* yang digunakan atau mematuhi dan menerapkan prosedur pengamanan yang telah ditentukan

Gambar A.2 Flowchart

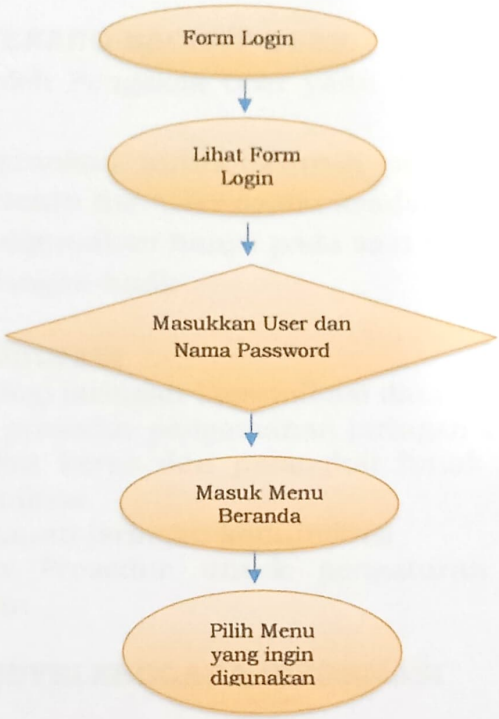


III. TEKNIS PENGGUNA USER

1. Aktivitas menggunakan User

a. Membuka User dengan memasukkan user dan nama password
b. Menggunakan menu sesuai dengan tampilan pada menu pengguna user
c. Melakukan proses penginputan sesuai dengan jabatan atau fungsi pengguna user
d. Melakukan persetujuan sesuai dengan limit yang sudah ditetapkan apabila pengguna user adalah Kepala Bagian atau Direksi

Gambar B. III1



2. Pengamanan User dan Nama Password

Pengguna User wajib menjaga dan merahasiaakan User dan Nama Password sendiri namun dapat diketahui oleh Kepala Bagian

3. Pengaduan Error/Gangguan ke Pengelola User

Pengguna User akan melakukan pengaduan apabila terjadi Error/gangguan/kendala-kendala Teknologi Informasi.

4. Pengamanan Data/Informasi pada CBS BPR

Pengguna User diwajibkan untuk menjaga keamanan Data/Informasi pada CBS antara lain :

1. Data Nasabah Tabungan dan Deposito
2. Data Nasabah Kredit
3. Laporan Keuangan

C. AKTIVITAS BACKUP USER

I. BACKUP USER

Backup User adalah Pengguna yang diberikan hak sebagai cadangan /pengganti daalam menggunakan user apabila pengguna pada fungsi tertentu *Backup User* berhalangan hadir

Adapun yang dapat digunakan / tersedia adalah sebagai berikut :

No	Departemen	Nama User
1	Unit Customer Service	Admin_Backup
2	Unit Back Office	Akuntansi_Backup
3	Unit Kas	Teller_Backup

II. TUGAS DAN WEWENANG BACKUP USER

1. User dikelola oleh Pengelola User yaitu ***Staff TI dan pengembangan bisnis***
2. User tidak digunakan untuk seluruh pengguna namun hanya pada departemen tertentu dan user dalam keadaan non aktif.
3. User aktif dan digunakan hanya pada saat pengguna dalam departemen tertentu berhalangan hadir

2.4 JARINGAN KOMUNIKASI

1. Struktur /topologi jaringan komunikasi data
2. Kebijakan dan prosedur pengamanan jaringan komunikasi
3. Daftar perangkat keras dan perangkat lunak yang digunakan untuk jaringan komunikasi
4. Sistem pemantauan jaringan komunikasi
5. Kebijakan dan Prosedur untuk pengaturan pengamanan jaringan komunikasi data

2.5 PENGAMANAN PENYELENGGARA INFORMASI

BPR wajib menerapkan upaya pengamanan yang diperlukan untuk mencegah gangguan keamanan dalam penyelenggaraan Teknologi Informasi yang berpotensi merugikan BPR, dan/atau nasabahnya. Oleh karena itu, BPR wajib menjaga kerahasiaan *(confidentiality)*,integritas *(integrity)*,ketersediaan *(availability)*, dan dapat ditelusurinya suatu informasi elektronik dan/atau dokumen elektronik yang terkait dengan nasabah dan seluruh aktivitas BPR sesuai dengan ketentuan peraturan perundang-undangan.

BPR wajib melakukan pengendalian otorisasi *(authorization of control)* dalam penyelenggaraan Teknologi Informasi, yaitu dengan cara menetapkan limit wewenang bagi setiap pengguna aplikasi sesuai dengan ketentuan yang berlaku.

Sebagai penyelenggara teknologi informasi, BPR harus dapat:

1. Menjamin perolehan, penggunaan, pemanfaatan, dan/atau pengungkapan data pribadi nasabah dilakukan berdasarkan persetujuan nasabah yang bersangkutan, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan; dan

2. Menjamin penggunaan atau pengungkapan data pribadi nasabah dilakukan berdasarkan persetujuan nasabah yang bersangkutan dan sesuai dengan tujuan yang disampaikan kepada nasabah pada saat perolehan data.

2.6 RENCANA PEMULIHAN BENCANA

A. Kebijakan dan Prosedur rencana pemulihan bencana :
   1. BPR memiliki rencana pemulihan bencana untuk pengamanan Teknologi Informasu jika suatu waktu terjadi bencana
   2. Analisa terhadap rencana pemulihan
   3. Komponen prosedur rencana pemulihan bencana
      3.1 Pusat Pemulihan Bencana sebagai bentuk antisipasi pengamanan Teknologi Informasi yang bersifat data
      3.2 Spesifikasi cadangan data dan perangkat keras
      3.3 Kelengkapan Pengamanan fisik pada pusat pemulihan bencana
B. Dokumentasi agar pemulihan bencana bisa lebih efektif dan efisien
C. Uji Coba rencana pemulihan bencana jika diperlukan untuk mengetahui pemulihan bencana sudah sesuai dengan yang diharapkan
D. Pemeliharaan rencana pemulihan bencana agar tidak terjadi dikemudian hari

2.7 KERJASAMA DENGAN PENYEDIA JASA TI

Dalam hal penyelenggaraan teknologi informasi yang dilakukan dengan cara bekerjasama dengan Penyedia Jasa (vendor), maka vendor yang ditunjuk harus berbentuk **badan hukum dan berkedudukan di Indonesia**.
BPR bertanggung jawab terhadap penyelenggaraan Teknologi Informasi dan diwajibkan:

1. melakukan pengawasan terhadap penyelenggaraan Teknologi Informasi BPR yang diselenggarakan oleh pihak penyedia jasa Teknologi Informasi.
2. memantau reputasi pihak penyedia jasa Teknologi Informasi dan kelangsungan penyediaan layanan kepada BPR.
3. memilih pihak penyedia jasa Teknologi Informasi berdasarkan analisis manfaat dan biaya dengan melibatkan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi.
4. memberikan akses kepada Otoritas Jasa Keuangan terhadap Pangkalan Data secara tepat waktu baik untuk data terkini maupun untuk data yang telah lalu.
5. memastikan penyedia jasa Teknologi Informasi:
   - memiliki tenaga ahli yang didukung dengan sertifikat keahlian sesuai dengan keperluan penyelenggaraan Teknologi Informasi.
   - menerapkan prinsip pengendalian Teknologi Informasi secara memadai yang dibuktikan dengan hasil audit yang dilakukan pihak independen.
   - menyediakan akses bagi auditor intern BPR, auditor ekstern yang ditunjuk oleh BPR, dan Otoritas Jasa Keuangan untuk memperoleh data dan informasi yang diperlukan secara tepat waktu setiap kali dibutuhkan.

- menyatakan tidak berkeberatan dalam hal Otoritas Jasa Keuangan dan/atau pihak lain yang berwenang sesuai dengan ketentuan peraturan perundang-undangan melakukan pemeriksaan terhadap kegiatan penyediaan jasa yang diberikan.
- sebagai pihak terafiliasi, menjaga keamanan seluruh informasi termasuk rahasia bank dan data pribadi nasabah.
- melaporkan kepada BPR setiap kejadian kritis yang dapat mengakibatkan kerugian keuangan dan/atau mengganggu kelangsungan operasional BPR.
- menyediakan Rencana Pemulihan Bencana yang teruji dan memadai;
- bersedia untuk menyepakati kemungkinan penghentian perjanjian kerja sama sebelum berakhirnya jangka waktu perjanjian *(early termination)* dalam hal perjanjian kerja sama tersebut menyebabkan atau diindikasikan akan menyebabkan kesulitan pelaksanaan tugas pengawasan Otoritas Jasa Keuangan dan,
- memenuhi tingkat layanan sesuai dengan perjanjian tingkat layanan (*service level agreement*) antara BPR dan pihak penyedia jasa Teknologi Informasi.

2.8 AUDIT INTERN TEKNOLOGI INFORMASI

Untuk menilai kepatuhan terhadap ketentuan, BPR wajib melakukan audit penyelenggaraan teknologi informasi sedikitnya 1(satu) kali dalam setahun. Dalam rangka pelaksanaan fungsi audit intern, BPR wajib memastikan tersedianya jejak audit (audit trail) terhadap seluruh kegiatan penyelenggaraan Teknologi Informasi untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lainnya

BAB IV
PELAPORAN

A. Laporan Rutin

BPR wajib menyampaikan laporan kepada Otoritas Jasa Keuangan mengenai pelaksanaan fungsi audit intern bagi BPR, mengacu pada jangka waktu penyampaian laporan pelaksanaan dan pokok-pokok hasil audit intern BPR, disampaikan paling lambat pada tanggal 31 Januari untuk audit yang dilaksanakan atas periode akhir tahun sebelumnya. Dan apabila jatuh pada hari Sabtu, Minggu, atau hari libur nasional maka laporan wajib disampaikan paling lambat pada hari kerja berikutnya.

B. Laporan Insidentil

1. BPR wajib menyampaikan laporan kepada Otoritas Jasa Keuangan mengenai kondisi terkini penyelenggaraan Teknologi Informasi BPR :
   a. Paling lambat 1 (satu) tahun sejak Peraturan Otoritas Jasa Keuangan ini berlaku;
   b. Paling lambat 10 (sepuluh) hari kerja sejak Teknologi Informasi efektif beroperasi dalam hal jangka waktu sebagaimana dimaksud pada huruf a terlampaui dan terjadi perubahan mendasar dalam penyelenggaraan Teknologi Informasi.
2. BPR wajib menyampaikan laporan realisasi kerja sama dengan penyedia jasa Teknologi Informasi sebagaimana dimaksud dalam Pasal 2 ayat (2) paling lambat 10 (sepuluh) hari kerja sejak penyelenggaraan Teknologi Informasi BPR oleh penyedia jasa Teknologi Informasi efektif beroperasi
3. BPR wajib melaporkan kepada Otoritas Jasa Keuangan mengenai kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraan Teknologi Informasi yang dapat atau telah mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelancaran operasional BPR dan wajib disampaikan melalui surat elektronik (e-mail) atau telepon paling lambat 1 (satu) hari setelah kejadian kritis, penyalahgunaan dan/atau kejahatan diketahui, yang diikuti dengan laporan tertulis paling lambat 7 (tujuh) hari kerja sejak kejadian kritis, penyalahgunaan dan/atau kejahatan diketahui.