I. KATA PENGANTAR

Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan / atau menyebarkan informasi. Fungsi dari suatu kebijakan Teknologi Informasi pada perusahaan adalah pada prinsipnya untuk membantu karyawan dalam penggunaan sistem komputer perusahaan, peralatan dan fasilitas-fasilitas yang ada sudah sesuai dengan penggunaannya.

Kegagalan dalam penggunaan yang tidak sebagaimana mestinya dalam mematuhi kebijakan tersebut, baik sadar atau tidak, dapat menimbulkan resiko sehingga dapat mempengaruhi kelangsungan kegiatan operasional dan dapat menimbulkan kerugian akibat tidak berjalannya operasional.

Untuk alasan ini maka semua karyawan sebagai pemakai computer harus menggunakan computer sesuai dengan pedoman dalam melakukan aktifitas mereka. SPO yang telah dijalankan dalam penyelenggaraan teknologi informasi dan tata cara penggunaan teknologi informasi di PT. BPR Karya Bakti Sejahtera. Kebijakan dan Prosedur ini di berlakukan kepada seluruh karyawan dan staff di PT. BPR Karya Bakti Sejahtera.

II. LATAR BELAKANG & TUJUAN

1. Kesiapan dan kecepatan dalam bertindak bagi seluruh karyawan dalam menghadapi gangguan operasional.
2. Mengetahui dan memahami tugas, peran dan tanggung jawab masing-masing lini terkait sehingga dalam pelaksanaannya tidak terjadi kepanikan dan keraguan yang dapat mengakibatkan kerugian yang lebih besar baik kepada karyawan maupun perusahaan.
3. Memudahkan koordinasi dalam pelaksanaannya.
4. Tetap dapat melayani nasabah selama terjadi gangguan atau kejadian kritis.
5. Mengetahui serta memahami prosedur penyelamatan dan pemulihan atas dokumen (Hard copy) dan data komputer.

BAB 1
ASSET IT

I. RUANG LINGKUP

Bab ini mencakup pengadaan, penggunaan, pemeliharaan, penghapusan, dan pelaporan Asset IT perusahaan BPR KBS.

II. TANGGUNG JAWAB

1. Divisi IT bertanggung jawab atas pengelolaan Asset IT di perusahaan BPR KBS.
2. Bagian Operasional bertanggung jawab atas pengelolaan keuangan terkait pengadaan dan penghapusan Asset IT di perusahaan BPR KBS.

III. PENGADAAN ASSET IT

1. Setiap permintaan untuk pembelian atau penyewaan Asset IT harus diajukan melalui formulir permintaan Asset IT yang telah disetujui.
2. Sistem pengadaan Asset IT harus disesuaikan dengan anggaran perusahaan BPR KBS.
3. Sebelum membeli atau menyewa Asset IT, Divisi IT harus melakukan penilaian kebutuhan dan kelayakan Asset IT tersebut.
4. Setiap Asset IT harus dicatat dan dimasukkan ke dalam database Asset IT di BPR KBS.

IV. PENGGUNAAN ASSET IT

1. Setiap Asset IT harus dipelihara secara teratur untuk memastikan kinerja yang optimal.
2. Depertemen IT harus memiliki jadwal pemeliharaan rutin dan perawatan untuk setiap asset IT.
3. Setiap perbaikan dan perawatan asset IT harus dicatat dan dimasukkan ke dalam database Asset IT di BPR KBS.

V. PENGHAPUSAN ASSET IT

1. Setiap Asset IT yang sudah tidak berguna dan tidak bisa diperbaiki harus dihapus dari database Asset IT di BPR KBS.
2. Departemen IT harus membersihkan/menghapus kode Asset IT dari setiap barang yang akan dibuang dan mengupdate data Asset IT yang telah dibuang.
3. Bagian Operasional harus mengevaluasi nilai Asset IT yang sudah tidak diperlukan lagi dan membuat keputusan tentang penghapusan atau penjualan.

BAB 2
BACKUP DATA

I. RUANG LINGKUP

Bab ini mencakup backup data dari seluruh perangkat di seluruh area kantor dan pusat data perusahaan.

II. TANGGUNG JAWAB

Staff IT bertanggung jawab untuk memastikan bahwa backup data dilakukan sesuai dengan standar dan kebijakan perusahaan. Staff IT juga harus memastikan bahwa seluruh karyawan memahami kebijakan backup data dan tindakan yang harus diambil jika terjadi kehilangan data.

III. PERSYARATAN

1. Seluruh data yang disimpan di perangkat perusahaan harus di backup secara teratur dan disimpan pada lokasi yang aman.
2. Backup data harus dilakukan dengan metode yang aman dan terenkripsi untuk melindungi kerahasian dan integritas data.
3. Backup data harus dilakukan dengan jadwal rutin dan disimpan dalam periode waktu yang ditentukan.
    a. Jadwal backup mingguan secara manual untuk semua CPU dan Laptop kantor via remote atau dari CPU masing masing dilakukan oleh Staff IT.
    b. Jadwal backup bulanan secara manual untuk Server Corsys, Synology, dan Server Cadangan.

IV. PROSEDUR

1. Penentuan Kebutuhan Backup
    - Perlu dilakukan analisis kebutuhan backup untuk menentukan jenis data yang perlu di backup dan frekuensi backup data.
    - Setiap perangkat dan sistem harus memiliki prosedur backup data yang terdokumentasi.
2. Pelaksanaan Backup Data
    - Backup data harus diuji dan diverifikasi secara berkala untuk memastikan keaslian dan integritas data.
    - Backup data harus disimpan di lokasi yang aman dan terenkripsi untuk melindungi kearahasiaan dan integritas data.

3. Penanganan Kehilangan Data
   - Setiap kehilangan data harus dilaporkan segera kepada PIC IT.
   - PIC IT harus memulai proses pemulihan data dari backup data yang ada.

BAB 3
JARINGAN KOMPUTER & MIKROTIK

I. RUANG LINGKUP

Bab ini mencakup instalasi, pengaturan, dan pemeliharaan jaringan komputer di seluruh area kantor dan pusat data perusahaan.

II. TANGGUNG JAWAB

PIC IT bertanggung jawab untuk memastikan bahwa jaringan dioperasikan sesuai standar dan kebijakan perusahaan. Pengelola jaringan juga harus memastikan bahwa semua karyawan memahami kebijakan keamanan jaringan dan tindakan yang harus diambil jika terjadi pelanggaran.

III. PERSYARATAN

1. Setiap staff IT harus mengikuti pelatihan keamanan jaringan dan SPO ini.
2. Setiap karyawan yang terlibat dalam pengoperasian jaringan harus memiliki hak akses yang sesuai dengan tanggung jawab mereka.
3. Setiap perangkat lunak dan perangkat keras jaringan harus diperbarui secara teratur untuk menghindari kerentanan keamanan.
4. Seluruh data yang ditransmisikan melalui jaringan harus dienkripsi dengan protocol keamanan yang tepat.
5. Setiap pelanggaran terhadap kebijakan keamanan jaringan harus dilaporkan segera kepada pengelola jaringan.

IV. PROSEDUR

a. Instalasi dan Pengaturan
   - Sebelum melakukan instalasi jaringan, perlu dilakukan analisis kebutuhan untuk menentukan jenis jaringan yang paling tepat untuk perusahaan.
   - Setiap perangkat keras dan perangkat lunak jaringan harus diinstal dan dikonfigurasi sesuai dengan standar perusahaan.
   - Setiap pengguna harus diberikan hak akses sesuai dengan tanggung jawab mereka.

b. Pemeliharaan dan Pemantauan
- Jaringan harus dipantau secara teratur untuk mengidentifikasi dan menangani masalah dengan cepat.
- Perangkat lunak antivirus dan firewall harus diperbarui secara teratur untuk melindungi jaringan dari ancaman keamanan.
- Seluruh pengguna harus mematuhi kebijakan keamanan jaringan, termaksud penggunaan sandi yang aman dan menjaga kerahasiaan sandi.

c. Pemulihan Bencana
- Perlu ada rencana pemulihan bencana yang jelas dan terstruktur untuk mengatasi kegagalan jaringan.
- Rencana pemulihan bencana harus disimpan di lokasi yang mudah diakses oleh pengelola jaringan dan seluruh pengguna jaringan.
- Pengujian berkala harus dilakukan untuk memastikan rencana pemulihan bencana berfungsi dengan baik.

BAB 4
PEMELIHARAAN ASSET IT

I. RUANG LINGKUP

SOP ini berlaku untuk semua komputer yang digunakan di perusahaan.

II. TANGGUNG JAWAB

1. Divisi IT bertanggung jawab atas pelaksaan pemeliharaan komputer.
2. Seluruh karyawan bertanggung jawab atas melaporkan segala kerusakan atau masalah pada komputer yang digunakan.

III. PROSEDUR

1. Pemeliharaan rutin dibagi dalam 2 jenis yaitu Hardware dan Software.
   - ***Pemeliharaan Hardware dilakukan setiap 3 bulan sekali***. Seperti membersihkan kipas processor di setiap CPU, cek hdd, cek memory, cek power supplay, cek monitor, cek keyboard, cek printer, cek mouse, dan cek kabel jaringan.
   - ***Pemeliharaan Software dilakukan setiap 1 bulan sekali***. Seperti memeriksa Operating System (windows), Microsoft Office, Aplikasi Corsys, Aplikasi Tracking, Email, Sharing Folder Synologi, dan update antivirus.
2. Pemeliharaan meliputi:
   - Membersihkan komponen dalam komputer;
   - Membersihkan keyboard, Mouse, Monitor dan Printer;
   - Memeriksa dan memperbarui program antivirus;
   - Memeriksa dan memperbarui sistem operasi yang terpasang;
3. Karyawan diwajibkan untuk mengaktifkan program antivirus dan firewall yang terpasang pada komputer yang digunakan, serta tidak diizinkan mengunduh atau memasang program atau aplikasi yang tidak terkait dengan pekerjaan.
4. Setiap Karyawan diwajibkan untuk melaporkan kerusakan atau masalah pada komputer yang digunakan kepada divisi IT segera setelah masalah terjadi.
5. Jika diperlukan perbaikan atau penggantian komponen, divisi IT akan mengambil tindakan secepatnya mungkin untuk memperbaiki atau mengganti komponen yang rusak.

BAB 5
COREBANKING SYSTEM

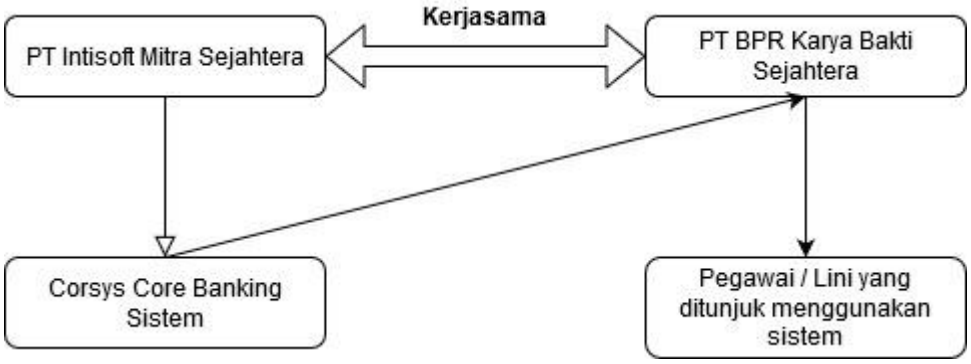
I. BPR KBS menggunakan aplikasi inti Perbankan yang telah diperbaharui sebelumnya dengan menggunakan Aplikasi Core Banking System Corsys milik PT. Intisoft Mitra Sejahtera.

II. BPR KBS dan PT. Intisoft Mitra Sejahtera selaku penyedia jasa teknologi informasi melakukan kerjasama dalam penyelenggaraan Teknologi Informasi dalam bentuk kerjasama secara tertulis.

III. Corsys dilakukan di kantor pusat BPR KBS dan kantor cabang (bila ada).

IV. Penggunaan sistem dilakukan oleh lini ataupun pegawai ditunjuk dan berkepentingan dalam pengelolaan BPR dan yang telah diberikan wewenang dan tanggung jawab sesuai dengan kebutuhan kerja dalam BPR KBS.

Bagan lingkup Teknologi Informasi BPR KBS :



BAB 6
WEWENANG & TANGGUNG JAWAB

Dalam penyelenggaraan Teknologi Informasi BPR KBS, Direksi dan Komisaris harus memastikan penyelenggaraan Teknologi Informasi sudah berjalan dengan baik sesuai dengan visi dan misi perusahaan. Keberhasilan Teknologi Informasi BPR KBS sangat tergantung pada komitmen Direksi dan Komisaris dan seluruh pegawai terhadap penyelenggaraan Teknologi Informasi.

I. Wewenang dan Tanggung jawab Direksi BPR KBS :
   a) Menetapkan rencana pengembangan dan pengadaan Teknologi Informasi.
   b) Menetapkan kebijakan dan prosedur terkait penyelenggaraan Teknologi Informasi yang memadai dan mengomunikasikannya secara efektif, baik pada satuan kerja penyelenggara maupun pengguna Teknologi Informasi.
   c) Memantau kecukupan kinerja penyelenggaraan Teknologi Informasi dan upaya peningkatannya.
   d) Memastikan bahwa:
      - Teknologi Informasi yang digunakan mendukung perkembangan usaha, pencapaian tujuan bisnis dan kelangsungan pelayanan terhadap nasabah BPR KBS.
      - Terdapat kegiatan peningkatan kompetensi sumber daya manusia yang terkait dengan penyelenggaraan dan penggunaan Teknologi Informasi.
      - Tersedianya sistem pengelolaan pengamanan informasi (information security management system) yang efektif dan dikomunikasikan kepada satuan kerja penyelenggara dan pengguna Teknologi Informasi.
      - Kebijakan dan prosedur penyelenggaraan Teknologi Informasi diterapkan secara efektif.

II. Wewenang dan Tanggung jawab Komisaris
   a) Mengarahkan dan memantau pengembangan pengadaan Teknologi Informasi BPR KBS.
   b) Mengevaluasi pertanggungjawaban Direksi terkait Penyelenggaraan Teknologi Informasi BPR KBS.

III. Wewenang dan Tanggung Jawab Pegawai secara umum
   a) Membantu Direksi dan Dewan Komisaris dalam penyelenggaraan Teknologi Informasi terkait dengan perencanaan, pelaksanaan dan pemantauan.
   b) Mendukung pengembangan dan atau pengadaan Teknologi Informasi.
   c) Mendukung implementasi, operasional, dan pemeliharaan Teknologi Informasi.
   d) Melakukan upaya penyelesaian permasalahan terkait operasional Teknologi Informasi, yang tidak dapat diselesaikan oleh satuan kerja pengguna Teknologi Informasi.

BAB 7
PENGEMBANGAN DAN PENGADAAN TEKNOLOGI INFORMASI

BPR KBS menetapkan dan mengembangkan sistem dengan spesifikasi yang telah disepakati dengan kesepakatan tentang jadwal, biaya dalam kesepakatan atau komitmen yang tertuang dalam dokumen assessment (perjanjian kerjasama). Dengan memiliki komitmen pengembangan dalam teknologi informasi dengan bentuk secara Continual Development (Pengembangan dengan system berkelanjutan).

1. Adapun Sistem dalam pengembangan dan pengadaan (pencegahan kerusakan / ganguan sistem komputer) yang dilakukan di PT. BPR Karya Bakti Sejahtera, yaitu :
    a. Pengujian secara berkala untuk memastikan server core banking System utama, client berfungsi dengan baik. Langkah-langkah pengujian adalah sebagai berikut:
        - Hidupkan UPS kemudian nyalakan komputer server, pastikan komputer melakukan proses *booting* sampai dengan keluar menu *user log on*
        - Cek konfigurasi sistem, pastikan sesuai dengan konfigurasi minimum yang dipersyaratkan oleh vendor, yaitu dengan cara :
            - Klik tombol **Start** > **Setting** > **Control Panel**.
            - Tampil kotak menu **Control Panel**, Klik **System**. Tampil **System Properties** yang menampilkan informasi Sistem Operasi, Jenis Procesor dan besarnya memory.
            - Klik Administratif **Tools** > **Event Viewer** > **Aplication** / **System** / **Security Log**, pastikan tidak ada *message error*.
        - Cek kapasitas *hard disk*, pastikan kapasitas *hard disk* yang tersisa minimal sebesar 1x memory komputer, yang akan digunakan sebagai *swap file*,yaitu dengan cara :
            - Klik kanan tombol **Start**>**Explorer**
            - Tampil *Windows Explorer*, klik kanan *local hardisk* (C:)>**Property**.

- Tampil *Local Disk* (C:) **properties**, menampilkan kapasitas hard disk yang terpakai (berwarna biru) dan kapasitas hard disk yang tidak terpakai (berwarna ungu)

b. Pastikan komputer bebas dari virus, yang akan menginfeksi dan merusak file sistem dan work station, dengan menginstall anti virus dan melakukan proses scanning terhadap hard disk maupun disket secara berkala dan terus mengupdate anti virus yang digunakan.

c. Lakukan *back-up* data transaksi harian, dan pastikan integritas data yang telah dibackup, dengan cara :

1. Backup data Corsys :
   - Dilakukan setiap hari pada jam tutup operasional.
   - Backup data pada saat sebelum EOD (end of day) dan BOD (beginning of day) Core Banking System.
2. Backup dengan eksternal hard disk dan Dropbox:
   - Dilakukan setiap hari setelah closing corebanking system.
   - Lakukan backup dengan Dropbox.
   - Lakukan *backup* dengan eksternal hard disk, untuk memastikan proses *backup* telah berjalan baik.
3. Klik kanan tombol **Start**>**Explorer**
4. Tampil *Windows Explorer*, klik drive dimana file backup berada. Contoh file berada di drive D, maka klik Local Drive (D:)
5. Buka file Backup data, klik data yang diinginkan kemudian copy ke eksternal hard disk.
6. Eksternal hard disk yang dimiliki 1 buah yang disimpan dalam khasanah.

BAB 8
OPERASIONAL DALAM TEKNOLOGI INFORMASI

Dalam operasional teknologi informasi di BPR KBS menerapkan standar penyelenggaraan teknologi informasi untuk memastikan informasi di komputer lengkap, akurat, terkini, terjaga integritasnya dan terhindar dari segala bentuk kesalahan ataupun kecurangan, penyalahgunaan, perusakan data dan memastikan operasional teknologi informasi stabil, aman, dan efisien secara keseluruhan. Melakukan print hard copy pada setiap transaksi di dukung oleh sarana operasional yang memadai.

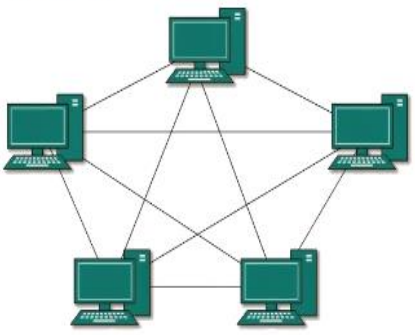
Sarana dan fasilitas yang ada di PT. BPR Karya Bakti Sejahtera, antara lain :

1. Sarana Penunjang operasional berupa :
   - Listrik 15.400 VA.
   - UPS (Uninterruptible Power Supply) 2 unit untuk server dan Teller.
   - CCTV.
   - Alarm.
2. Sarana komunikasi berupa :
   - Line telepon yang tersambung dengan PABX.
   - Jaringan internet Telkom Indihome.
3. Sarana Hardware dan software komputer :
   - PC Client dan PC Server
   - Laptop
   - Mikrotik
   - Printer dan Scanner
   - OS Windows
   - Windows Office
   - Corebanking System

BAB 9
JARINGAN KOMUNIKASI TEKNOLOGI INFORMASI

Pengoperasian dalam akses jaringan komunikasi harus diawasi secara baik dan benar di karenakan merupakan pintu utama untuk masuk ke dalam sistem informasi BPR, jika tidak dikelola dengan baik maka akan terjadi ancaman keamanan informasi. Dalam memantau dan melakukan pengendalian di jaringan komunikasi BPR harus memperhatikan pemeliharaan perangkat lunak jaringan komunikasi dan tranmisi data termasuk proses dalam keadaan darurat. Jaringan komunikasi yang di design secara dinamis di PT. BPR Karya Bakti Sejahtera agar dapat mengantisipasi pengembangan di masa yang akan datang. Design Jaringan Komunikasi yang dipakai oleh PT. BPR Karya Bakti Sejahtera yaitu menggunakan Topologi Mesh yang merupakan bentuk topologi yang cocok bagi jaringan komunikasi yang menghubungkan banyak komputer. Bentuk topologi ini dapat berfungsi sebagai jalur rekam cadang saat jalur lain mengalami masalah. Bentuk Jaringan Topologi Mesh di PT. BPR Karya Bakti Sejahtera sebagai berikut :

Topologi *Mesh*



Adapun pemanfaatan jaringan komunikasi yang digunakan, dengan sarana jaringan komunikasi antara lain :

1. Sarana Jaringan komunikasi yang digunakan di PT. BPR Karya Bakti Sejahtera, yaitu :
    a. Jaringan Internet :
        - LAN (Local Area Network).

- Komunikasi utama : Jaringan internet Indihome
- Komunikasi privat : VPN-IP (Sharing Bandwitdh Perbarindo)

b. Jaringan telepon :

PT BPR Karya Bakti Sejahtera memiliki 2 nomor telepon yang terhubung dengan PABX.

2. Pencegahan kerusakan sistem jaringan komunikasi data/internet dan telepon, yaitu dengan cara :
   a. Pemasangan kabel jaringan komunikasi harus dilakukan dengan benar.
   b. Secara rutin dan berkala harus dilakukan pemeriksaan terhadap semua jaringan komunikasi.
   c. Untuk mencegah terjadinya gangguan karena petir PT. BPR Karya Bakti Sejahtera memasang anti petir pada PABX.
   d. Penempatan Router/modem harus disimpan pada ruangan server dengan sistem pendingin yang baik.
   e. Harus dilakukan pengecekan secara berkala atas semua perangkat keras tersebut.
   f. Pastikan ruangan komunikasi data dalam keadaan tertutup.
   g. Pastikan hanya petugas yang ditunjuk dan bertugas/berkepentingan yang boleh berada pada ruangan tersebut.
3. Apabila terjadi gangguan, maka perbaikan pada sistem komunikasi perlu dilakukan pengecekan dengan cara membuka network internet access pada komputer kemudian klik open network and sharing center, kemudian klik local area connection dan klik/pilih diagnose apabila pada trouble shooting terdapat masalah maka akan terlihat trouble shooter dan dapat dipastikan bahwa komunikasi terputus, yang kemungkinan penyebabnya :
   a. Internal kantor :
      - Kabel putus.
      - Sering terinjak-injak.
      - Usia perangkat.
      - *Gateway* tidak sesuai dengan *IP Router*.

- Dsb.

b. Eksternal :

- Ada perbaikan jaringan kabel telepon oleh pihak vendor.
- Jaringan primer/ sekunder Telkom terputus, yang diakibatkan misalnya : ada penggalian/ pemasangan pipa PAM/ saluran air, terbakar, kebakaran, kerusakan pada STO Telkom, dsb.
- Kotak Terminal mengalami gangguan, misalnya : kena petir, dirusak, dsb.

4. Gangguan yang di khawatirkan dapat terjadi pada perangkat keras dalam Jaringan komunikasi :
   - Petir.
   - Tegangan listrik yang tidak stabil.
   - Bencana alam.
   - Dsb.
5. Pengaturan pengamanan jaringan data menggunakan konfigurasi pada perangkat miktorik dan menginstall antivirus serta mengupdate windows security secara berkala.

Setelah diketahui penyebabnya, petugas berwenang membuat pencatatan dalam buku service/perbaikan dan melaporkan kepada Direksi dan kemudian menghubungi pihak vendor agar segera ditangani dengan baik dan secara tepat waktu.

BAB 10
PENGAMANAN TEKNOLOGI INFORMASI

Pengamanan informasi sangat bergantung pada pengamanan terhadap semua aspek dan komponen teknologi informasi terkait kebocoran, kerusakan, ketidakakuratan, ketersediaan, atau gangguan informasi sangat bergantung pada pengamanan terhadap semua aspek dan komponen teknologi informasi terkait.

1. Kebijakan dalam pengamanan teknologi informasi perlu ditetapkan untuk :
   a. Mencegah gangguan yang dapat merugikan penyelenggaraan teknologi informasi harus di terapkan secara baik dan benar.
   b. Menjaga kerahasiaan, integritas, ketersediaan dan menelusuri informasi teknologi yang terkait pada nasabah dan hubungan dengan aktivitas BPR.
   c. Memperhatikan aspek SDM, proses dan teknologi.
   d. Penyelenggaraan teknologi informasi dan pengendalian otorisasi dalam implementasi dan pengendalian pengamanan informasi.
   e. Adanya komitmen Direksi dan tanggung jawab pihak-pihak dalam pengamanan informasi yang sejalan dengan strategi dan tujuan bisnis.
   f. Adanya dokumentasi dan ketentuan lain yang mendukung kebijakan pengamanan informasi.
2. Prosedur pengamanan Teknologi Informasi yang dilakukan di PT. BPR Karya Bakti Sejahtera untuk menjaga segala bentuk informasi intern, rahasia bank ataupun hal lainnya dilakukan dengan cara :
   a. Pengamanan segala aset yang berupa data (hardcopy maupun softcopy), maupun perangkat keras ataupun lunak, dicatat dengan baik dan adanya pencatatan pada lini terkait yang berkaitan dengan nilai, sensitivitas, ketentuan di BPR baik secara tertulis hardcopy maupun softcopy.
   b. Pengamanan dalam sumber daya manusia di BPR baik itu pegawai ataupun kerjasama dengan pihak lain dilakukan dengan cara adanya tanggung jawab, keterikatan terhadap kerja dengan perjanjian secara tertulis yang berkaitan dengan ketentuan di BPR.

c. Adanya sanksi atas pelanggaran pengamanan teknologi informasi.

d. Dilakukannya pemeliharaan dan pemeriksaan segala aset maupun sumber daya manusia secara berkala.

e. Melaporkan segala kendala kepada Staff IT oleh pihak-pihak terkait apabila ditemukan kendala untuk dapat ditangani secepatnya dengan cara :

- Pihak terkait membuat laporan secara lisan atau tertulis mengenai kendala teknologi informasi yang sedang dialami.
- Staff IT segera merespon laporan tersebut dan mencari solusi.
- Apabila kendala yang dialami cukup berat, maka staff IT akan meminta persetujuan atasan untuk melakukan tindakan perbaikan.

3. Adanya sarana pengamanan peraturan Teknologi Informasi pada PT. BPR Karya Bakti Sejahtera, meliputi :

a. Data di Server, PC dan Laptop :

- Semua data perusahaan harus tersimpan di server sesuai dengan nama masing-masing.
- Tidak menyimpan data pribadi di komputer server.
- Tidak menyimpan data yang tidak ada hubungannya dengan pekerjaan di server.

b. Untuk Internet, Email dan Jaringan :

- Tidak browsing ke situs-situs yang berbau Pornografi dan Crack
- Tidak mendownload software yang tidak ada hubunganya dengan pekerjaan dan menginstallnya ke dalam komputer.

c. Untuk komputer dimasing-masing divisi :

- Dilarang merubah isi konfigurasi PC
- Dilarang merubah *IP Address* di masing-masing PC tanpa persetujuan IT
- Dilarang merubah nama komputer
- Dilarang menginstall program (software), games atau meng-upgrade program yang sudah terinstall di masing-masing komputer.

d. Untuk Penggunaan Level User Password.

Pengertian Password atau kata sandi adalah kumpulan karakter atau *string* yang digunakan oleh pengguna sebuah sistem/ aplikasi yang mendukung banyak pengguna (*multiuser*) untuk memverifikasi identitas dirinya kepada sistem aplikasi tersebut. Kata sandi juga dapat diartikan sebagai kata rahasia yang digunakan sebagai pengenal. Penggunaan level password tertinggi / teratas di gunakan oleh administrator server & Dewan Direksi. Dalam hal ini penggunaannya untuk memonitoring pengguna / user dalam penggunaan aplikasi sistem dan memverifikasi transaksi tertentu dalam jumlah nominal yang cukup besar.

e. Sistem pengamanan pada perangkat di PT. BPR Karya Bakti Sejahtera menggunakan Windows Defender yang selalu *up to date.*

f. Komputer yang sudah terhubung dengan Corsys Core Banking system mempunyai nama user dan password yang sudah disesuaikan dengan tugas masing masing karyawan.

4. Pemeliharaan Corsys Core Banking System.

Untuk pemeliharaan / maintenance sistem aplikasi di PT. BPR Karya Bakti Sejahtera adalah dengan melakukan pemeliharaan basis data dalam hal ini diperbantukan oleh pihak kedua yaitu PT Intisoft Mitra Sejahtera dalam hal ini yang bekerjasama dalam penggunaan sistem aplikasi dan juga melakukan backup / membuat file cadangan ke media eksternal, contohnya hard disk eksternal kapasitas besar dan Dropbox.

5. Pemberian, Perubahan dan Penghapusan Akses Pengguna

Dalam rangka menjamin kelancaran dalam setiap proses dan transaksi di PT. BPR Karya Bakti Sejahtera, maka setiap karyawan yang diberikan wewenang oleh pimpinan untuk memperoleh user Id dan akses kepada Corebanking, wajib menjaga dan menjamin kerahasiaan user id dan password yang diberikan. Atasan akan memberikan akses Corebanking kepada karyawan sesuai dengan ruang lingkup pekerjaan masing – masing.

Apabila terdapat mutasi atau rolling jabatan, maka atasan akan memberikan instruksi perubahan akses Corebanking menyesuaikan kepada ruang lingkup pekerjaannya yang baru.

Jika terdapat karyawan yang resign atau mengundurkan diri, maka wajib dilakukan penghapusan akses penggunan dengan dihapusnya user ID yang bersangkutan maksimal H+1 dari tanggal terakhir bekerja.

6. Security Awareness Program

   Sejak awal karyawan PT. BPR Karya Bakti Sejahtera telah dilatih dan dibimbing untuk selalu meningkatkan kehati-hatian dan tanggung jawab terhadap segala kerahasiaan data.

7. Tim penanganan Insiden dalam Pengamanan Informasi

   Staff bagian IT memiliki tanggung jawab penuh atas penanganan informasi di PT. BPR Karya Bakti Sejahtera dengan melakukan koordinasi dengan bagian - bagian terkait.

8. Klasifikasi Data

   Corebanking pada PT. BPR Karya Bakti Sejahtera telah mengklasifikasikan data sesuai dengan jenis produk dan kebutuhan. Sehingga data yang ditampilkan bisa sesuai dengan kebutuhan pengguna.

9. Penggunaan Emergency User

   Dalam hal terdapat situasi khusus dimana terdapat karyawan yang berhalangan hadir, maka atasan akan mengintruksikan pembuatan Emergency User untuk menunjang kelancaran proses transaksi pada hari tersebut. Kemudian jika karyawan yang dimaksud sudah kembali melaksanakan pekerjaannya, maka emergency user wajib dihapus dan tidak boleh dipergunakan.

10. Pencegahan penggunaan perangkat lunak illegal.

    Staff IT wajib menjamin setiap perangkat lunak yang digunakan di PT. BPR Karya Bakti Sejahtera bersifat legal, dengan cara membeli lisensi setiap perangkat lunak yang akan digunakan apabila perangkat lunak tersebut tidak open source.

11. Sanksi

    Apabila terdapat pihak-pihak yang melanggar prosedur dalam pengamanan informasi, maka akan diberikan sanksi teguran. Akan tetapi jika pelanggaran kembali dilakukan, maka akan diberikan sanksi lain yang disesuaikan ketentuan yang berlaku berupa SP 1 sd 3 sampai dengan pemutusan hubungan kerja.

BAB 11
RENCANA PEMULIHAN TEKHNOLOGI INFORMASI

Adanya gangguan / kerusakan yang disebabkan oleh alam maupun manusia berdampak pada kemampuan teknologi informasi yang dimiliki BPR dalam hal pelayanan terhadap nasabah sehingga risiko operasional dan risiko reputasi dapat di minimalisir secara tepat waktu, baik dan benar. Untuk dapat meminimalisir risiko tersebut diharapkan proses manajemen yang dilakukan secara menyeluruh dapat berfungsi dengan baik walaupun menghadapi ganguan / kerusakan.

1. Kebijakan yang dilakukan oleh BPR dalam mengahadapi gangguan / kerusakan yang terjadi dengan dilakukannya Rencana Pemulihan Bencana, seperti :
    a. Penganalisaan kemungkinan adanya risiko karena faktor kebakaran, alam, banjir, gempa, faktor teknis perangkat keras / lunak dan faktor manusia (sabotase).
    b. Adanya prosedur dalam Pemulihan Bencana Teknologi Informasi.
    c. Penetapan tanggung jawab bagi pihak terkait.
2. Prosedur yang ditetapkan dalan Rencana Pemulihan Teknologi Informasi di PT. BPR Karya Bakti Sejahtera, yaitu :
    a. UPS (Uninterruptible Power Supply) :
        - Lindungi semua perangkat komputer dengan menggunakan *power conditioning* seperti UPS yang memiliki desain *redundant* untuk memastikan perangkat kritis tidak terpengaruh atau terganggu pada saat genset dalam masa start up.
        - Spesifikasi :
            - Daya 1200 VA
            - Jumlah baterai 2 buah
        - Terhadap UPS, harus dilakukan perawatan yang baik dan berkala, seperti :
            - Lakukan pengecekan rutin terutama daya simpan battery/ aki kering UPS minimal 3 bulan sekali.
            - Baterai diganti setelah 1 tahun pemakaian

b. Pencegahan dan perbaikan dari sisi keamanan kantor, dengan menggunakan :

1. CCTV

   Untuk keamanan PT. BPR Karya Bakti Sejahtera, menggunakan CCTV yang terpasang pada setiap sudut ruangan kantor.

   a. Spesifikasi sebagai berikut :
      - 6 Kamera indoor
      - 2 Kamera Outdoor (1 dipakai di indoor)
      - 1 IP CAM di lantai 3
      - 1 unit DVR dan hard disk 1 Terabyte
      - CCTV dapat merekam selama 15 hari

   b. Pencegahan dan perbaikan dari sisi keamanan :
      - Divisi IT melakukan pemeriksaan rutin atas CCTV tersebut.
      - Secara otomatis melakukan perekaman CCTV setiap hari, dan apabila tidak ada kejadian penting selama 2 minggu perekaman akan terhapus otomatis.
      - CCTV terhubung dengan Handphone Direksi dan bagian berwenang sehingga dapat memonitor apabila terjadi gangguan di malam hari, misalnya alarm yang berbunyi di malam hari.
      - Apabila terjadi gangguan pada CCTV maka divisi IT melaporkan kepada Direksi dan kemudian melakukan perbaikan secepatnya.

2. Keamanan

   PT. BPR Karya Bakti Sejahtera memasang sistem keamanan G4S dimana terpasang sensor gerak dan password untuk menonaktifkan alarm dan apabila terjadi keadaan yang mendesak dengan cepat menghubungi ke karyawan yang tempat tinggal terdekat untuk mengecek kantor, atau dapat dilakukan pengecekan oleh pejabat/petugas melalui HP yang terhubung dengan CCTV agar dapat ditangani lebih lanjut.

Pengecekan alarm dan sensor gerak harus dilakukan minimal 1x dalam seminggu dan dibuat log book untuk hasil pengecekan dan disetujui oleh salah satu Direksi.

PIC dalam Tim IT wajib memastikan keamanan serta kerahasiaan data serta dokumen perusahaan, baik yang terdapat di dalam Corebanking System , komputer, laptop, eksternal hardisk & Synologi ataupun dalam bentuk fisik berkas. Data-data yang bersifat rahasia tidak boleh dibawa keluar dari lingkungan kantor PT. BPR Karya Bakti Sejahtera. Adapun pada saat-saat terdesak yang mengharuskan data tersebut dibawa keluar lingkungan kantor, wajib mendapatkan persetujuan salah satu Direksi.

3. Prosedur dalam Pemulihan Bencana Teknologi Informasi.
    a. Membentuk tim perencana. Tim yang dibentuk terdiri dari pengambil keputusan dari setiap unit usaha atau area operasional, bertanggung jawab atas semua aktivitas pemulihan bencana, perencanaan dan melaporkan perkembangan yang terjadi setiap bulannya pada Direksi.
    b. Melakukan penilaian resiko dan audit untuk membuat rencana pemulihan bencana teknologi informasi. Tim tersebut harus memahami proses bisnis, teknologi, jaringan dan layanan. Analisa dilakukan dengan mempertimbangkan skenario terburuk yaitu dari kehilangan atau kerusakan total fasilitas. Analisa juga dilakukan dengan mempertimbangkan aspek geografis, rancangan sistem IT saat ini dan layanan yang tersedia. Setiap analisa harus menggambarkan dampak finansial dari pernggantian perangkat, alokasi sumberdaya tambahan dan kontrak pemasangan layanan tambahan.
    c. Menentukan prioritas terhadap jaringan dan aplikasi. Prioritas pada masing-masing proses bisnis dan komponen IT yang digunakan dapat dikategorikan sebagai berikut:
        - Mission Critical

Merupakan kegagalan sistem IT yang akan menyebabkan gangguan yang sangat besar terhadap usaha, menyebabkan kerugian hukum dan finansial atau dapat mengancam keselamatan seseorang.

- Important

  Merupakan kegagalan sistem IT yang dapat menyebabkan gangguan yang bersifat moderat pada bisnis, menyebabkan kerugian kecil pada hukum dan finansial atau menyebabkan masalah akses ke sistem lain.

- Minor

  Merupakan kegagalan sistem IT yang hanya menyebabkan sebuah gangguan kecil pada bisnis.

d. Merancang resiliency (kemampuan bertahan) dan strategi recovery. Dengan merancang resiliency dalam infrastruktur jaringan, layanan dan sumberdaya dapat disebar kedalam area geografis yang lebar, untuk membentuk fault tolerant pada site yang diproritaskan dan lokasi dimana layanan utama berada. Strategi recovery harus ditujukan pada manusia, fasilitas, layanan jaringan, perangkat komunikasi, aplikasi, client dan server, kontrak support dan maintenance, layanan tambahan vendor, lead-time layanan Telco dan lingkungan. Strategi recovery harus menyertakan estimasi down time layanan, rencana aksi dan prosedur pemulihan. Rencana tersebut juga menentukan ambang batas, seperti level minimum layanan agar usaha dapat tetap beroperasi, sistem yang harus berfungsi penuh dan lain-lain.

e. Menyiapkan sebuah inventory yang terbaru dan dokumentasi rencana. Sangatlah penting memiliki inventori yang selalu diperbaharui dan memiliki daftar lengkap semua lokasi, perangkat, vendor, pengguna layanan dan contact name. Inventory dan dokumentasi adalah bagian dari perencanaan dan pembangunan pemulihan bencana. Dokumentasi setidaknya mengandung aspek-aspek sebagai berikut : Inventory lengkap, termasuk prioritas sumberdaya. Tinjauan ulang penilaian struktur proses, audit dan

laporan-laporan. Analisa resiko dan gap berdasarkan hasil penilaian resiko dan audit. Rencana yang diterapkan untuk menghilangkan resiko dan gap.

Dalam hal terjadinya insiden pengamanan informasi pada PT. BPR Karya Bakti Sejahtera seperti adanya kejadian kritis, penyalahgunaan atau kejahatan pada penyelenggaraan teknologi informasi sebagaimana tertera didalam Peraturan Otoritas Jasa Keuangan nomor 75/POJK.03/2016 yang menimbulkan kerugian keuangan secara signifikan atau menggangu kelancaran operasional secara fatal, maka PT. BPR Karya Bakti Sejahtera akan melaporkan kejadian tersebut kepada Otoritas Jasa Keuangan.

Pelaporan insiden tersebut akan dilakukan oleh Pejabat Eksekuti Audit Intern, kemudian akan didokumentasikan dan dilakukan pemantauan kepada pihak-pihak terkait dalam menindaklanjuti dan menyelesaikan insiden pengamanan informasi tersebut sampai insiden tersebut bisa tertangani dan terselesaikan.

BAB 12
AUDIT INTERN TEKNOLOGI INFORMASI

Penggunaan sarana Teknologi Informasi di samping meningkatkan kemampuan BPR dalam melaksanakan kegiatan operasional, juga mengandung risiko yang dapat mengakibatkan kerugian dalam BPR. Oleh karena itu sistem pengendalian intern yang efektif perlu agar dapat menjaga dan menjamin segala asset dan kerugian.

Hal-hal yang perlu dilakukan jika terjadi audit intern yaitu :

a. Kebijakan umum audit
b. Perencanaan audit
c. Pelaksanaan audit
d. Pelaporan
e. Tindak lanjut audit
f. Pengembangan dan pengujian sistem elektronik

Wewenang pelaksanaan Audit Intern PT. BPR Karya Bakti Sejahtera diberikan kepada Pejabat Eksekutif Audit Intern. Dimana proses audit setiap tahun wajib dilaksanakan minimal 1 (satu kali). Dalam setiap temuan pada audit internal dilakukan tindak lanjut guna meningkatkan efisiensi serta efektivitas dalam tata kelola teknologi informasi.

Laporan audit intern terhadap penyelenggaraan teknologi informasi ditandatangani oleh Direktur Utama dan ditembuskan kepada Direktur yang Membawahkan Fungsi Kepatuhan.

Pihak penyedia jasa teknologi informasi dapat membantu pihak penyelenggara teknologi informasi jika nantinya memerlukan informasi bila terjadi pemeriksaan BI / OJK, ataupun pihak eksternal yang ditunjuk untuk melakukan audit teknologi informasi.

BAB 13
KERJASAMA DENGAN PENYEDIA JASA TEKNOLOGI INFORMASI

Kerjasama dengan penyedia jasa teknologi informasi yang dilakukan oleh PT. BPR Karya Bakti Sejahtera dengan PT Intisoft Mitra Sejahtera merupakan penyedia jasa teknologi informasi yang sampai saat ini masih berjalan di PT. BPR Karya Bakti Sejahtera. Bentuk kerjasama PT. BPR Karya Bakti Sejahtera dengan PT. Intisoft Mitra Sejahtera dalam bentuk perjanjian kerjasama yang telah disepakati oleh kedua belah pihak dengan mengimplementasikan komitmen berupa :

a. Lisensi atas aplikasi Corsys-BPR selama PT BPR Karya Bakti Sejahtera masih menggunakannya untuk kegiatan operasional.
b. Pemeliharaan terhadap aplikasi Corsys-BPR dengan cara melaksanakan perbaikan, pembaruan, pengembangan dan modifikasi.
c. Dukungan teknik dalam proses penginstallan dan pelatihan sesusai jadwal yang disepakati.

Segala bentuk aturan, jangka waktu, biaya serta manfaat dalam penggunaan aplikasi Corsys-BPR tercantum dalam bentuk perjanjian kerjasama antara PT. BPR Karya Bakti Sejahtera dengan PT. Intisoft Mitra Sejahtera.

Diajukan	Disetujui		Diketahui
Dody Sugiantoro	Eko Nuryanto	Lauw Sumiwati	Jacky Hardi
SPV IT	Direktur Utama	Direktur Operasional & Kepatuhan	Komisaris

LAMPIRAN

1. ASSET IT

No	Nama Asset	Unit	Posisi

2. Backup Data Corsys
   - Pastikan semua data selesai di otorisasi
     - Pilih Menu Utility -> Laporan -> Laporan Sebelum Proses Akhir Hari
     - Pilih Customer, Teller, Deposito, Retail, Pinjaman, Akunting
     - Untuk Akunting tidak boleh ada otoritas yang belum diotoritas
     - Untuk Teller harus sudah balance (0 saldo)
   - Disable transaksi
     - Pilih Menu Utility -> Utility -> Update Flag Proses
     - Klik tombol Disable Transaksi Entry Corsys
   - Backup file database Operasional
     - Kembali ke Desktop Server pilih icon backup_OPR_KBS.bat
     - Ketik BACKUP_OPR_TGLBULANTAHUN_BEFORE_EOD kemudian Enter
     - Tunggu Proses Backup Operasional Before Day selesai
     - Kembali ke Corsys pilih Menu Data Center -> Proses Akhir Hari
     - Pilih Proses EOD Teller -> Lalu OK
     - Pilih Proses EOD Deposito -> Lalu OK
     - Pilih Proses EOD Pinjaman -> Lalu OK
     - Pilih Proses EOD Retail -> Lalu OK
     - Kembali ke Menu Data Center -> Proses Data Center -> Proses Data Center -> Lalu OK
     - Kembali ke Menu Data Center -> Proses Awal Hari
     - Pilih Proses BOD Retail -> Lalu OK
     - Pilih Proses BOD Teller -> Lalu OK
     - Pilih Proses BOD Pinjaman -> Lalu OK
     - Pilih Proses BOD Deposito -> Lalu OK
     - Kembali ke Dekstop Server pilih icon backup_OPR_KBS.bat
     - Ketik BACKUP_OPR_TGLBULANTAHUN_AFTER_BOD kemudian Enter
     - Tunggu Proses Backup Operasional After Day selesai
   - Backup file database Akunting
     - Kembali ke desktop pilih icon backup_akunting_KBS.bat
     - Ketik BACKUP_ACC_TGLBULANTAHUN_BEFORE_EOD kemudian Enter
     - Tunggu Proses Backup Akunting selesai
     - Kembali ke Menu Akunting -> Proses -> Proses Akhir Hari / EOD -> Lalu OK
     - Menu Akunting -> Proses -> Proses Awal Hari / BOD -> Lalu OK
     - Kembali ke Destop Server pilih icon backup_akunting_KBS.bat

- Ketik BACKUP_ACC_TGLBULANTAHUN_BOD kemudian Enter
- Tunggu Proses Backup Akunting After Day

- Enable transaksi
  - Menu Utiliy -> Update flag_proses -> Enable Transaksi
  - Menu Akunting -> Proses -> Proses Posting Harian -> Lalu Posting
  - Kembali ke Dekstop Server pilih icon backup_akunting_KBS.bat
  - Ketik BACKUP_ACC_TGLBULANTAHUN_BEFORE_EOD kemudian Enter
  - Kembali ke Menu Akunting -> Proses -> Proses EOD/Akhir Hari
  - Kembali ke Menu Akunting -> Proses -> Proses BOD/Awal Hari
  - Kembali ke Dekstop Server pilih icon backup_akunting_KBS.bat
  - Ketik BACKUP_ACC_TGLBULANTAHUN_BOD kemudian Enter
  - Menu Utility -> Utility -> Update Flag Proses
  - Pilih tombol Enable Transaksi Enttry Corsys

3. IP ADDRESS DAN BANDWITH

No	Nama Device	Divisi	IP Address	Bandwidth
1	Mikrotik RB 1100	OPS	192.168.10.0	Unlimited
2	Customer Service	OPS	192.168.10.5	1 Mbps
3	Teller	OPS	192.168.10.6	1 Mbps
4	HRD	OPS	192.168.10.7	1 Mbps
5	Admin Kredit 1	OPS	192.168.10.8	2 Mbps
6	Admin Kredit 2	OPS	192.168.10.9	2 Mbps
7	IT	OPS	192.168.10.10	2 Mbps
8	SPV Operasional	OPS	192.168.10.11	3 Mbps
9	Audit	Audit	192.168.10.17	1 Mbps
10	Surveyor 1	Bisnis	192.168.10.16	2 Mbps
11	Surveyor 2	Bisnis	192.168.10.18	2 Mbps
12	Surveyor 3	Bisnis	192.168.10.19	2 Mbps
13	Colletion	Bisnis	192.168.10.20	2 Mbps
14	CA	Bisnis	192.168.10.21	1 Mbps
15	Laptop Pak Jacky	Komisaris	192.168.10.94	10 Mbps
16	Sinology	OPS	192.168.10.99	30 Mbps
17	Server Corsys	OPS	192.168.10.101	30 Mbps
18	DVC	OPS	192.168.10.110	7 Mbps
19	IP CAM 1	OPS	192.168.10.111	10 Kbps

20	DHCP POOL	OPS	192.168.10.200	10 Kbps
21	Redmi 10 Pro	OPS	192.168.10.203	1 Mbps
22	Redmi Note 5A	OPS	192.168.10.204	1 Mbps
23	Laptop Pak Eko	Direksi	192.168.10.205	10 Mbps
24	Laptop Bu Mimi	Direksi	192.168.10.206	10 Mbps
25	Laptop Pak Andri	Bisnis	192.168.10.207	10 Mbps
26	Laptop Pak Doni	OPS	192.168.10.208	3 Mbps
27	Tablet Pak Andry	Bisnis	192.168.10.209	1 Mbps
27	Laptop Dani	OPS	192.168.10.210	1 Mbps
28	Laptop Tele	Bisnis	192.168.10.212	1 Mbps
29	Laptop Dody	OPS	192.168.10.213	2 Mbps
30	Iphone Pak HTJ	Komisaris	192.168.10.245	3 Mbps
31	Android Pak HTJ	Komisaris	192.168.10.246	3 Mbps
32	Iphone Pak Jacky	Komisaris	192.168.10.247	3 Mbps
33	Android Pak Jacky	Komisaris	192.168.10.248	3 Mbps
34	KAP 1	Audit	192.168.10.249	

4. Jadwal Pemeliharaan Komputer

No	Lantai	Waktu
1	Lantai 1 : 1. PC CS 2. PC Teller 3. PC Admin 1 4. PC Admin 2 5. PC SPV OPS 6. Printer CS 7. Printer Admin 1 8. Printer Admin 2 9. Photocoppy	Sabtu di minggu ke 2
2	Lantai 2 : 1. Laptop SPV Collection 2. Laptop Direktur Utama 3. Laptop Direktur Operasional	Sabtu di minggu ke 3

	4. PC HRD 5. PC Audit 6. PC Analis 7. PC IT 8. PC Collection 9. Printer Lantai 2 10. Printer Direktur Operasional	
3	Lantai 3 : 1. Laptop Direksi Bisnis 2. Laptop SPV Bisnis 3. PC Surveyor 1 4. PC Surveyor 2 5. PC Surveyor 3 6. Printer Lantai 3 7. Infocus 8. Server 9. Synologi	Sabtu di minggu ke 4