PT. BALAIRUNG CITRAJAYA SUMBAR

KEBIJAKAN TEKNOLOGI INFORMASI

DAFTAR ISI

I. Latar Belakang 3
II. Dasar, Tujuan dan Manfaat 3
III. Tujuan & Manfaat 4
IV. Kebijakan Umum 4
V. Kebijakan Tata Kelola Teknologi Informasi 5
Lampiran 1

I. Kebijakan Perencanaan Jangka Pendek dan Jangka Panjang TI (Master Plan TI). 17
II. Kebijakan Penggunaan dan Pengelolaan Komputer dan Perangkat Keras TI..... 18
III. Kebijakan Penggunaan , Pembuatan dan Pengelolaan Aplikasi Perangkat Lunak . 20
IV. Kebijakan Penggunaan dan Pengelolaan Infrastruktur Jaringan LAN/WAN(Local Area Network / Wide Area Network)..... 22
V. Kebijakan Penggunaan dan Pengelolaan Infrastruktur Jaringan Internet 23
VI. Kebijakan Penggunaan dan Pengelolaan E-mail Perusahaan 24
VII. Kebijakan Penggunaan dan Pengelolaan Pemakaian Siskomdat/Simpelweb 25
VIII. Kebijakan Penggunaan dan Pengelolaan Web Intranet..... 25
IX. Kebijakan Risiko Teknologi Informasi (IT Risk)..... 26
X. Kebijakan Pengelolaan Server..... 26
XI. Kebijakan Keamanan Sistem Informasi danTI (IT Security)..... 27
XII Kebijakan Audit Sistem Informasi dan Teknologi Informasi..... 38
XIII. Kebijakan Keterbukaan Informasi melalui Media TI dan Pengelolaan website Perusahaan 38
XIV. Kebijakan Pencadangan Data (Backup Data)..... 39
XV. Kebijakan Penggunaan Media Sosial..... 39

KEBIJAKAN TATA KELOLA TEKNOLOGI INFORMASI
PT. Balairung Citrajaya Sumbar

I. Latar Belakang

Teknologi Informasi (TI) telah menjadi bagian penting dalam organisasi, terutama bagi organisasi yang bisnisnya berorientasi kepada profit. Saat ini infrastruktur bisnis tidak dapat dipisahkan dari TI. Infrastruktur TI tidak hanya mendukung strategi bisnis yang telah ada tetapi juga dapat digunakan untuk mengasah strategi baru. Infrastruktur TI atau disebut juga portofolio TI memungkinkan membantu organisasi untuk menghadapi persaingan dan juga meningkatkan produktifitas. Penggunaan Teknologi Informasi (TI) juga sangat penting dalam mendukung proses bisnis untuk mencapai Visi dan Misi Perusahaan.

Visi perusahaan adalah :

"Menjadi perusahaan milik daerah yang dikelola secara profesional dan terus tumbuh, serta berbasis pada sistem informasi yang handal'"

Misi perusahaan adalah:

1. Menempatkan perusahaan berdomisili di Jakarta sebagai plaza Sumatra Barat (Minangkabau) di bidang kebudayaan dan pariwisata yang bernilai ekonomi.
2. Menempatkan perusahaan berdomisili di Jakarta sebagai plaza Sumatra Barat (Minangkabau) di bidang kebudayaan dan pariwisata yang bernilai ekonomi.
3. Menjadi perusahaan yang profesional dengan menempatkan konsep GCG dan berbasis sistem informasi tekonologi.
4. Menjadi perusahaan yang tumbuh di atas rata-rata industrinya.
5. Merencanakan, mengembangkan, dan melaksanakan usaha dalam bidang perhotelan yang disesuaikan dengan keinginan pemilik perusahaan dan kebutuhan dari para konsumen.
6. Menyusun, mengolah, dan mengoptimalkan produk serta servis yang berkualitas, kompetitif, dan memiliki nilai jual yang tinggi.
7. Membina dan mengembangkan standar dan prosedur operasional yang konsisten dan berkelanjutan dalam rangka menjamin terciptanya kepuasan.
8. Selalu memberikan solusi yang terbaik dalam menjalankan usaha perhotelan

Penerapan Sistem Informasi dan Teknologi Informasi bukanlah tanpa risiko mengingat nilai investasi TI dalam menunjang proses bisnis perusahaan cukup besar. Untuk itu diperlukan suatu pengelolaan Sistem TI yang efektif dan efisien dalam bentuk kerangka kebijakan dan tata kelola TI yang baik (IT GCG).

Salah satu kunci keberhasilan dalam implementasi TI adalah adanya strategi dan kebijakan TI yang baik. Dengan adanya tata kelola dan kebijakan TI memungkinkan organisasi untuk memperoleh manfaat dalam mendukung proses bisnis untuk mencapai Visi dan Misi perusahaan. Kebijakan tata kelola TI ini merupakan dasar bagi penyusunan kebijakan dan pengambilan keputusan yang berkaitan dengan Teknologi Informasi PT. BALAIRUNG CITRAJAYA SUMBAR.

II. Dasar

Dasar dan acuan penyusunan Kebijakan dan Tata Kelola TI PT. BALAIRUNG CITRAJAYA SUMBAR ini adalah :

1. Peraturan Menteri Badan Usaha Milik Negara Nomor : PER- 02/MBU/2013 tentang Panduan Penyusunan Pengelolaan Teknologi Informasi Badan Usaha Milik Negara.
2. Peraturan Menkominfo nomor 41/PER/MEN.KOMINFO/11/2007 tanggal 19 November 2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional.
3. Peraturan Gubernur Sumatera Barat Nomor 37 Tahun 2023 Tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik
4. Surat Keputusan Direksi Nomor 236/BCS/Kep.Dir/IX/2024 tentang Kebijakan Tata Kelola Teknologi Informasi.

III. Tujuan dan Manfaat

Tujuan dan manfaat dari Kebijakan dan Tata Kelola TI adalah :

1. Agar Teknologi Informasi dapat dimanfaatkan secara optimal, terukur , terarah dan memenuhi prinsip-prinsip *Good Corporate Governance* (GCG).
2. Mendukung proses bisnis perusahaan untuk mencapai Tujuan, Visi dan Misi Perusahaan.
3. Memberikan nilai tambah bagi bisnis dan penanganan risiko pada implementasi TI.
4. Perusahaan dapat melakukan Pengelolaan Sumber Daya TI secara efektif dan efisien.
5. Mengoptimalkan keselarasan antara TI dengan bisnis perusahaan.

IV. Kebijakan Umum

Proses perencanaan, implementasi dan pengembangan Sistem Teknologi Informasi yang dilaksanakan di PT. BALAIRUNG CITRAJAYA SUMBAR harus memenuhi prinsip-prinsip sebagai berikut :

1. Tranparansi, yaitu apa yang sedang dan akan dilakukan dan yang dihasilkan oleh proses Teknologi Informasi harus di dokumentasikan secara transparan tanpa

harus mengorbankan aspek kerahasiaan.

2. Akuntabilitas, yaitu seluruh personil yang memiliki tugas terkait dengan proses teknologi informasi dapat mempertanggunjawabkan tindakan dan keputusan menurut garis kewenangan yang ditetapkan oleh perusahaan.
3. Responsibilitas, seluruh proses teknologi informasi mempunyai pembagian dan pemisahan tugas dan kewenangan yang jelas sehingga dapat saling mengontrol satu sama lain.
4. Independensi, bahwa seluruh personil yang terkait dengan proses sistem teknologi informasi bebas dari segala benturan kepentingan (*conflict of interest*) dan tetap mengutamakan kepentingan perusahaan.
5. *Fairness*, proses teknologi informasi harus memberikan layanan yang dapat memenuhi kebetuhan *stakeholder* secara adil.
6. Sistem teknologi Informasi yang dirancang, yang sedang dan akan dilaksanakan harus selaras dengan Visi dan Misi Perusahaan.
7. Penerapan sistem TI harus sesuai dengan aturan perusahaan dan aturan yang berlaku di Indonesia.
8. Sistem TI harus mampu melakukan digitalisasi proses bisnis perusahaan secara efektif dan efisien.
9. Sistem TI harus dapat mengefisienkan proses administrasi dan dapat mendukung sistem kantor elektronis dengan menggunakan sedikit kertas (*less paper*).
10. Kebijakan TI atau IT GCG harus dimonitor dan dievaluasi secara berkala.

V. Kebijakan Tata Kelola Teknologi Informasi PT. BALAIRUNG CITRAJAYA SUMBAR

Struktur kebijakan tata kelola TI perusahaan mengatur garis-garis haluan tata kelola TI, sedangkan untuk peraturan detail dan teknis dituangkan dalam prosedur, *manual book* atau instruksi kerja yang disesuaikan dengan kebutuhan organisasi/sesuai dengan *framework* Tata Kelola TI untuk proses pengelolaan TI meliputi 2 domain proses pengendalian kebijakan yaitu kebijakan strategis dan kebijakan operasional yang dapat dirinci sebagai berikut :

1. Kebijakan Srategis

a. Penetapan peran TI Perusahaan

- Defenisi : Kebijakan penetapan peran TI adalah pernyataan kebijakan yang ditetapkan untuk menentukan peran TI dalam perusahaan.
- Tujuan : Untuk menempatkan fungsi TI sesuai dengan peran yang telah ditentukan. Hal ini akan berkaitan dengan tugas, wewenang dan tanggung jawab TI dalam perusahaan.
- Teknologi Informasi berperan diantara sebagai pendukung
- (*support*) dan *factory* dan diharapkan juga sebagai *enabler* bisnis perusahaan untuk meningkatkan nilai (*value*) dan mencapai tujuan

strategis perusahaan.

- Visi Teknologi Informasi adalah menjadi partner strategis perusahaan melalui implementasi Teknologi Informasi yang selaras dengan proses bisnis dan kebutuhan bisnis.
- Misi TI adalah :
    1. Penyiapan dan peningkatan kualitas sumber daya manusia dalam penguasaan teknologi informasi.
    2. Memberikan layanan berbasis TI kepada perusahaan.
    3. Mengelola sumber daya TI perusahaan secara efektif dan efisien.
    4. Menata sistem informasi dan teknologi informasi PT. BALAIRUNG CITRAJAYA SUMBAR yang baik dan berorientasi pada *good corporate governance* (GCG).
    5. Penyiapan infrastruktur telekomunikasi dan teknologi informasi yang mendukung sistem informasi perusahaan.
- Tugas pokok dan fungsi (tupoksi) TI adalah :

  <u>Tugas Pokok</u>

    1. Merencanakan/merancang, mengimplementasikan , mengelola, merawat dan mengembangkan Sistem Teknologi Informasi yang selaras dengan bisnis dan kebutuhan perusahaan.
    2. Menciptakan solusi berbasis TI bagi perusahaan.
    3. Memastikan ketepatan ukuran TI perusahaan.
    4. Memastikan operasional layanan TI berjalan dengan baik

  <u>Fungsi</u>

    1. Perumusan dan penetapan Rencana Jangka Panjang TI / Master Plan TI Perusahaan.
    2. Perumusan dan penetapan Kebijakan dan Tata Kelola TI Perusahaan
    3. Pengelolaan sistem teknologi TI berdasarkan tata kelola TI (IT GCG).
    4. Penyebaran pengetahuan (*sharing knowledge*) di bidang Teknologi Informasi.

b. Perencanaan TI

- Defenisi : Kebijakan perencanaan TI adalah kebijakan yang mengatur tata kelola perencanaan TI dalam suatu perusahaan sesuai dengan peran TI dalam perusahaan.
- Tujuan : Hal ini dilakukan agar perencanaan TI selaras dengan perencanaan dan tujuan bisnis perusahaan.
- Teknologi Informasi perlu dinyatakan secara jelas untuk menjamin keselarasan bisnis dengan TI, sesuai dengan peran TI dalam perusahaan. Perencanaan TI (Masterplan TI) untuk kurun waktu 3- 5 tahun, meliputi :

- Konteks Bisnis
- Arsitektur Bisnis
- IT *Visioning (visi,* misi TI)
- Arsitektur Informasi
- Arsitektur Aplikasi
- Arsitektur Teknologi
- Rencana Program TI
- Roadmap Transisi Pengembangan & Implementasi TI
- IT Governance (termasuk didalamnya antara lain Prinsip prinsip TI,Organisasi TI, Pengelolaan *Governance Enforcement,* PengelolaanAkuisisi dan Implementasi Solusi TI**,** Pengelolaan Layanan TI,Pengelolaan Keamanan TI, Pengelolaan Risiko TI**,** *TransformationReadiness Assessment)*

- Aspek perencanaan TI dapat dilihat pada Lampiran Nomor I

c. Kerangka kerja proses dan organisasi TI

- Defenisi :Kebijakan kerangka kerja proses dan organisasi TI adalah kebijakan yang mengatur tata kelola proses TI perusahaan serta kebutuhan organisasi pendukungnya.
- Tujuan : dari kebijakan ini adalah agar proses utama TI perusahaan dapat dijalankan dan selaras dengan peran TI perusahaan, serta tersedianya organisasi pendukung tersebut.
- Perusahaan membentuk unit tersendiri dalam bentuk Sub Bagian Teknologi Informasi yang bertanggung jawab dalam hal pengelolaan, pemanfaatan dan pengembangan Sistem Teknologi Informasi Perusahaan yang didukung oleh personil yang berkompeten di bidangnya.Struktur Organisasi, uraian tugas, tanggung jawab, wewenang dan uraian deskripsi setiap personil tersebut dinyatakan dalam dokumen Uraian Pekerjaan PT. BALAIRUNG CITRAJAYA SUMBAR yang menjadi satu kesatuan yang tidak terpisahkan dengan dokumen Kebijakan TI ini. Organisasi TI di perusahaan disesuaikan dengan kebutuhan bisnis perusahaan.

d. Pengelolaan investasi TI

- Defenisi : kebijakan tentang pengelolaan investasi TI adalah kebijakan yang mengatur tata kelola investasi TI perusahaan dimana pada kebijakan ini harus dipastikan bahwa setiap investasi TI harus terkait dengan inisiatif bisnis dan tujuan perusahaan.
- Tujuan : hal ini bertujuan agar setiap investasi TI selaras dengan strategi bisnis perusahaan.
- Pengelolaan pendanaan investasi/pembiayaan TI Perusahaan merupakan bagian dari proses pengembangan, operasi dan pemeliharaan Sistem Informasi yang harus dilaksanakan dalam kerangka Master Plan TI. Roadmap atau rencana investasi yang dituangkan dalam master plan TI

dan Rencana Kerja Anggaran Perusahaan (RKAP) bidang TI. Dilakukan pencatatan biaya TI dan dilakukan review terhadap biaya TI tersebut.

e. Pengelolaan sumber daya TI

- Defenisi : Kebijakan pengelolaan sumber daya TI adalah kebijakan yang mengatur tatanan pengelolaan seluruh sumber daya TI yang berupa SDM, data/informasi, aplikasi dan infrastruktur.
- Tujuan : Kebijakan ini bertujuan agar seluruh proses pengelolaan sumber daya TI dapat dikelola sesuai dengan aturan-aturan yang dipersyaratkan sehingga dapat menghasilkan produk TI yang dapat dipercaya, efektif dan efisien.
- Standar dan prosedur yang mengatur tata cara penyediaan dan pengelolaan sumber daya TI sebagaimana berikut :
    - Sumber Daya Manusia

      Kebijakan SDM TI merupakan bagian dari kebijakan pengelolaan SDM PT. BALAIRUNG CITRAJAYA SUMBAR secara umum meliputi rekruitasi & pengelolaan kompetensi, pendefenisian peran dan tugas suatu posisi termasuk kinerja dan supervisi posisi yang didefenisikan, pelatihan SDM, perubahan dan pemberhentian tugas dan penilaian dan evaluasi performansi karyawan. Setiap implementasi TI harus didukung oleh pengelola dan pengguna yang berkompetensi. Kompetensi di dapat dari pelatihan dan pendidikan di bidang TI dimulai dari identifikasi pelatihan yang dibutuhkan (*training need analysis*) , pelaksanaan sampai dengan evaluasinya. Pelatihan SDM ini mengacu kepada aturan dan prosedur pengembangan SDM yang digunakan perusahaan.
    - Data/Informasi

      Kebijakan pengelolaan sumber daya data dan informasi meliputi proses-proses akuisisi data yang dapat menjamin kelengkapan (*completness*). Akurasi (*accuracy*), validitas (*validity*) dan autorisasi (*authorization*) data yang biasanya didefenisikan dalam suatu *manual/applications*. Aspek ini terkait erat dengan Lampiran Nomor III, VI, VII, VIII, dan XI. Penyimpanan data disimpan dalam media penyimpan data di dalam Laptop atau PC pemilik data, selain itu harus memiliki *backup* data tersebut di media lainnya seperti flashdisk, CD dan disimpan di menu *backup* file pada web intranet melalui *account* ybs. Pertukaran dan pembuangan/penghapusan data dilakukan atas seijin dari pemilik data. Aspek ini terkait erat dengan Lampiran Nomor XIV.
    - *Software*/Aplikasi

      Kebijakan *Software*/Aplikasi mengacu kepada lampiran Nomor III.

- Infrastruktur
  Kebijakan infrastruktur mengacu kepada lampiran Nomor IV dan V.
- Tata kelola pengadaan sumber daya TI
  Kebijakan tata kelola pengadaan sumber daya TI merupakan kebijakan pengadaan secara umum yang di gunakan oleh PT. BALAIRUNG CITRAJAYA SUMBAR.

f. Pengelolaan Risiko TI
   - Defenisi : Kebijakan pengelolaan Risiko TI adalah kebijakan yang mengatur pengelolaan risiko akibat diimplementasikannya TI dalam pencapaian sasaran bisnis perusahaan
   - Tujuan : Kebijakan ini bertujuan agar risiko-risiko akibat diimplementasi-kannya TI atau tidak beroperasinya TI sebagai pendukung bisnis dapat diidentifikasikan dan dilakukan mitigasi yang tepat.
   - Kebijakan risiko TI mengacu kepada Lampiran Nomor IX

g. Pengelolaan Proyek (*project management*)
   - Defenisi :Merupakan Sebuah program dan kerangka manajemen proyek untuk pengelolaan semua proyek TI yang dibangun .
   - Tujuan :Kerangka kerja ini memastikan prioritas yang benar dan koordinasi dari semua proyek TI. Pendekatan ini mengurangi risiko biaya tak terduga dan pembatalan proyek, meningkatkan komunikasi dan keterlibatan dari pengguna akhir, memastikan nilai dan kualitas penyerahan proyek, dan memaksimalkan kontribusi terhadap program investasi IT.
   - Kerangka manajemen proyek merupakan sebuah program dan kerangka manajemen proyek untuk pengelolaan semua proyekTI yang dibangun .Kerangka kerja ini memastikan prioritas yang benar dan koordinasi dari semua proyek. Kerangka kerja ini mencakup rencana induk proyek, penugasan dan penggunaan sumber daya, mendefinisikan lingkup kerja dan penyerahan hasil kerja , persetujuan oleh pengguna, pendekatan bertahap untuk penyerahan hasil kerja, *quality of assurance*, rencana pengujian, dan pengujian dan kajian pasca implementasi setelah instalasi untuk memastikan manajemen risiko proyek dan penghantaran nilai kebisnis.

h. Penanganan kebutuhan dan identifikasi solusi (*Identify automated solution*)
   - Defenisi : Pengelolaan proses *Identify automated solution* adalah suatu proses menerjemahkan kebutuhan fungsional dan kontrol bisnis ke desain yang efektif dan efisien.
   - Tujuan : Adalah memenuhi tujuan bisnis untuk memastikan pendekatan yang efektif dan efisien dalam memenuhi kebutuhan pengguna.
   - Aspek ini terkait erat dengan Lampiran Nomor III.

2. Kebijakan Operasional

a. Pengelolaan layanan TI (IT Service Management)

- Defenisi : kebijakan pengelolaan layanan TI adalah kebijakan yang mengatur tata kelola layanan TI.
- Tujuan : Agar proses layanan TI dapat teridentifikasi dan didefenisikan dengan baik untuk mencapai kinerja TI yang diharapkan dan kelangsungan layanan TI perusahaan.
- Kebijakan pengelolaan layanan TI meliputi antara lain proses- proses sebagai berikut :

Tahapan *Service Strategy*

- Pengelolaan *Service Portofolio* (*Service Portfolio Management*)
  Proses pengelolaan portofolio layanan yang bertujuan memberikan arahan strategis dan pengelolaan investasi pada pengelolaan layanan TI, sehingga portofolio layanan yang optimal tetap dapat dipelihara. Pengelolaan investasi pada pengelolaan layanan TI ini terkait erat dengan aspek Investasi TI sebagaimana yang tercantum pada Kebijakan Strategis di atas.
- Pengelolaan Keuangan Layanan TI
  (*Financial Management*) Proses pengelolaan keuangan layanan TI yang meliputi pengelolaan anggaran, akunting dan penagihan biaya dari penyediaan layanan TI merupakan kebijakan pengelolaan anggaran, akunting dan penagihan biaya dari penyediaan layanan TI yang digunakan oleh PT. BALAIRUNG CITRAJAYA SUMBAR.
- Pengelolaan Permintaan layanan TI
  (*Demand Management*) merupakan aktifitas untuk memahami dan mempengaruhi kebutuhan pelanggan untuk layanan dan penyediaan kapasitas layanan TI dalam rangka memenuhi kebutuhan tersebut.

Tahapan *Service Design*

- Pengelolaan Katalog Layanan TI
  Pengelolaan Katalog Layanan TI adalah menyediakan sumber tunggal informasi yang pada semua layanan yang telah disepakati dan memastikan ketersediaannya secara luas bagi siapa saya yang disetujui untuk mengaksesnya. Unit kerja yang dibentuk perusahaan yang mengelola Sistem TI perusahaan bersama-sama dan saling berkoordinasi dengan unit pemilik informasi menyediakan sumber tunggal informasi pada setiap layanan TI yang disediakan melalui mekanisme akses sebagaimana yang telah disebutkan di atas.
- Pengelolaan tingkat layanan TI
  Proses pengelolaan tingkat layanan TI adalah proses yang mengelola perjanjian tingkat layanan TI dengan pengguna, serta pelaporan hasil

layanan TI selama dijaminkan.

Pengelolaan tingkat layanan dapat dikaitkan dengan pola *charge back* (jika diterapkan) untuk menyelaraskan kualitas layanan yang diberikan dengan upaya layanan TI yang dilakukan pengelola TI.

- Pengelolaan Kapasitas (*Capacity Management*)

  Proses pengelolaan kapasitas infrastruktur layanan TI adalah proses yang mengelola penggunaan sumber daya infrastruktur TI dan proses pemenuhan kebutuhan infrastruktur untuk layanan TI yang dijaminkan agar tetap memiliki kinerja dan tingkat ketersediaan yang baik. Aspek pengelolaan kapasitas ini terkait erat dengan Lampiran Nomor IV.
- Pengelolaan ketersediaan layanan TI (*Availability Management*)

  Proses pengelolaan ketersediaan layanan TI adalah proses yang mengelola ketersediaan layanan TI baik software/aplikasi, infrastruktur dan jaringan agar tetap dapat beroperasi sesuai dengan tingkat layanan yang dijaminkan. Aspek ini sangat erat terkait dengan pengelolaan server dan jaringan pada Lampiran Nomor IV dan X.
- Pengelolaan kesinambungan layanan TI (*Service Continuity Management*)

  Proses pengelolaan kesinambungan layanan TI adalah proses yang mengelola kesinambungan layanan TI agar tetap beroperasi sesuai dengan tingkat layanan yang dijaminkan. Salah satu upayanya antara lain dengan adanya *Disaster Recovery Plan* (DRP) untuk layanan kritikal. Aspek ini terkait erat dengan Lampiran Nomor IX, X dan XI

Tahapan *Service Transition*

- Pengelolaan perubahan (*Change Management*)

  Proses pengelolaan perubahan seluruh aspek layanan TI yang berupa identifikasi permintaan perubahan, identifikasi dampak akibat perubahan layanan TI, pelaksanaan perubahan layanan TI dan pelaporan perubahan layanan TI. Setiap perubahan yang terkait dengan implementasi Sistem TI haruslah dilakukan secara sistematis, bertahap, dan konsisten.
- Pengelolaan konfigurasi (*Service Assest and Configuration Management*)

  Proses pengelolaan konfigurasi adalah proses yang mengelola pencatatan konfigurasi sistem layanan TI baik berupa aplikasi maupun infrastruktur serta tata cara perubahan konfigurasi yang diperlukan. Setiap konfigurasi sistem TI dicatat dan didokumentasikan oleh pengelolaa TI

dan setiap perubahan di catat pada *log book*, sehingga jika terjadi pergantian personil riwayat konfigurasi tetap tersimpan dan diketahui oleh personil penggantinya. Konfigurasi dasar setiap sistem dilakukan secara terpusat oleh pengelola TI, memonitor dan mencatat setia aset TI dan perubahannya. Setiap ada perubahan yang dilakukan oleh *user* maka pengguna tersebut wajib melaporkan kepada pengelola TI.

- *Release and Deployment Management*
  Proses pengelolaan *release* atau versi aplikasi adalah proses yang berupa identifikasi pencatatan versi aplikasi yang beroperasi, penyimpanan sumber (*source)* aplikasi yang dioperasikan dan proses validasi bahwa versi aplikasi yang dioperasikan sama dengan *source* versi aplikasi yang disetujui untuk dioperasikan.
- *Service Validation and testing*
  Proses yang bertanggung jawab untuk validasi dan pengujian dari perubahan baru layanan TI. Layanan validasi dan pengujian memastikan bahwa layanan TI sesuai dengan rancangan dan akan memenuhi kebutuhan dari perusahaan.
- Manajemen Pengetahuan (*Knowledge Management*) Proses yang bertanggung jawab untuk mengumpulkan, menganalisis, menyimpan dan berbagi pengetahuan dan informasi dalam organisasi. Tujuan utama dari manajemen pengetahuan adalah untuk meningkatkan efisiensi dengan mengurangi kebutuhaNuntuk menemukan kembali pengetahuan. Aplikasi Web Intranet dan E-mail harus digunakan secara intensif oleh seluruh karyawan dalam rangka saling berbagi pengetahuan. Aspek ini terkait erat dengan lampiran Nomor VI dan VIII.

Tahapan *Service Operation*

- *Service Desk*
  Pengelolaan fungsi layanan untuk penerimaan laporan insiden, gangguan, keluhan dan permintaan layanan TI yang pada umumnya berupa *call center* atau *helpdesk*. Pengelola TI menyediakan *helpdesk* yang akan melayani pengguna TI dari masalah gangguan layanan dan pertanyaan seputar masalah TI.
- *Event Management*
  Proses yang memonitor semua peristiwa yang terjadi melalui infrastruktur TI untuk memungkinkan sistem beroperasi secara normal dan juga untuk mendeteksi dan meng-eskalasi kondisi gangguan dari layanan TI.
- Pengelolaan Insiden Layanan TI (*Incident Management*) Proses pengelolaan insiden layanan TI yang berupa penerimaan laporan

insiden, penanganan insiden, eskalasi dan pelaporan insiden layanan TI. Pengelola layanan TI melalui help desk menerima laporan insiden layanan TI. Setiap insiden tercatatdalam *log book* dan saling dikomunikasi diantara personil yang bertanggung jawab.

- Pengelolaan Permasalahan layanan TI (*Problem management*)
  Proses pengelolaan permasalahan layanan TI yang berupa identifikasi masalah dari laporan insiden, penyelesaian masalah, eskalasi permasalahan dan pelaporan permasalahan layanan TI. Setelah menerima laporan insiden, pihak *help desk* akan meneruskan ke pihak dan personil yang terkait dan memonitor proses eskalasi sampai dengan penanganan insiden tersebut. Setiap permasalahan layanan tercatat dalam *log book*.
- Pengelolaan Permintaan Layanan TI (*Request Fulfilment*) Aspek ini berhubungan dengan Pengelolaan permintaan layanan TI dari pengguna kepada pengelola TI. Setiap permintaan layanan dikelola dengan baik melalui surat resmi dari pengguna layanan kepada pengelola TI, kemudian permintaan tadi disesuaikan dan diselaraskan dengan kemampuan TI dan kebutuhan perusahaan.
- Pengelolaan Akses (*Access Management*)
  Proses untuk mengelola dan memberikan pengguna yang berwenang hak untuk menggunakan layanan TI, sementara di lain pihak membatasi akses kepengguna yang tidak berwenang. Aspek ini terkait erat dengan Lampiran Nomor VI, VII, VIII dan XI.

<u>Tahapan Continual Service Improvement</u>

- *Continual Service Improvement*
  Peningkatan pelayanan secara terus-menerus menggunakan 7 langkah perbaikan sebagai berikut :
  - Menentukan apa yang akan diukur
  - Menentukan apa yang dapat diukur
  - Pengumpulan data
  - Pemrosesan data
  - Analisa data
  - Menyajikan dan menggunakan informasi
  - Menerapkan aksi korektif.
- *Service Meauserement and Reporting*
  Mengkoordinasikan rancangan metrik ,pengumpulan data dari aktifitas pelaporan dari proses dan fungsi yang lain.

b. Pengelolaan sekuriti TI
   - Defenisi : Kebijakan pengelolaan sekuriti TI adalah kebijakan yang mengatur tata kelola sekuriti TI dalam perusahaan.

- Tujuan : Kebijakan ini bertujuan untuk menjaga kerahasiaan (*confidentality*), integritas (I*ntegrity*), dan ketersediaan (*Availability*) informasi perusahaan.
- Kebijakan sekuriti TI ini terkait erat dengan Lampiran Nomor XI.

c. Pengelolaan layanan pihak III
   - Defenisi : Kebijakan pengelolaan pihak III adalah kebijakan yang mengatur tata kelola layanan TI yang dilakukan pihak III (*outsourcing*).
   - Tujuan : Kebijakan pengelolaan pihak III bertujuan untuk menjamin bahwa layanan yang dijalankan pihak III (*supplier, vendor dan partners*) memenuhi kebutuhan bisnis perusahaan dan juga meminimalkan risiko bisnis jika pihak III tidak dapat memenuhi kewajibannya dalam memberikan layanan TI.
   - Dalam setiap perjanjian kerjasama diharuskan mencantumkan bahwa pihak III menjamin layanan yang dijalankan dan di serahkan ke pada perusahaan memenuhi kebutuhan bisnis perusahaan.

d. Pengelolaan operasional
   - Defenisi : Kebijakan pengelolaan operasional adalah kebijakan yang terkait dengan operasionalisasi layanan TI yang mendukung proses bisnis perusahaan baik di bidang software/aplikasi, infrastruktur jaringan maupun perangkat keras.
   - Tujuan : Kebijakan pengelolaan operasional menjamin terlaksananya operasional layanan TI yang baik , efektif dan efisien.
   - Kebijakan operasional TI ini terkait erat dengan Lampiran Nomor II, III, IV, V, VI, VII, VIII dan X.

e. Pengelolaan mutu
   - Defenisi : Kebijakan pengelolaan mutu adalah kebijakan yang terkait dengan operasionalisasi layanan TI dengan kualitas/mutu yang baik dalam mendukung proses bisnis perusahaan baik di bidang *software*/aplikasi, infrastruktur jaringan maupun perangkat keras.
   - Tujuan : agar layanan TI yang di-*deliver* dan yang digunakan perusahaan tetap terjaga dengan baik kualitasnya.
   - Setiap layanan TI yang diberikan dan yang digunakan dalam mendukung proses bisnis perusahaan harus berkualitas baik. *Quality of Service* layanan TI harus dikelola melalui fungsi-fungsi : *Service Level Management, Capacity Management, Avaibility Management, Service Continuity Management, IT Financial Management* dan *Workforce Management*.

f. Knowledge Transfer

- Defenisi : *Knowledge Transfer* adalah proses untuk mengirimkan *knowledge* seperti pengalaman, dan pelajaran dari berbagai sumber. *Knowledge transfer* melibatkan komunikasi antara manusia dan komunikasi individu. *Knowledge transfer* menyatakan secara tidak langsung bahwa individu didalam suatu organisasi memberitahu suatu informasi tertentu kepada individu lain di dalam organisasi itu atau dengan organisasi lain berdasarkan keadaan, kondisi, atau aturan tertentu. *Knowledge Transfer* tidak hanya dari internal organisasi juga dapat dilakukan dari pihak III kepada organisasi. Intinya *Knowledge transfer* adalah proses untuk memindahkan *knowledge* dari sumber ke penerima.
- Tujuan dari *Knowledge Transfer* adalah pada dasarnya *knowledge sharing* dan *knowledge transfer.*
- Sebenarnya memiliki tujuan yang sama, yaitu untuk memberikan manfaat bagi individu maupun organisasi. Berbagi pengetahuan dianggap sebagai proses penting dalam mendukung manajemen pengetahuan. Setiap layanan TI yang dibangun baik yang dibuat secara mandiri oleh perusahaan atau pun yang dibangun oleh pihak III harus mensyaratkan *Transfer Knowledge* dari layanan TI yang dibangun sehingga perusahaan mendapatkan pengetahuan dan dapat digunakan selain untuk menjalankan layanan TI dimaksud juga dapat mengembangkan layanan tersebut sesuai dengan kebutuhan perusahaan.

g. Pengelolaan Data Monitor dan Evaluasi Kinerja TI

- Defenisi : Kebijakan monitor dan evaluasi kinerja TI adalah kebijakan yang mengatur pengelolaan indikator kinerja TI hingga level korporat dan sistematika pelaporan kinerja serta tindak lanjut yang diperlukan jika terjadi deviasi.
- Tujuan : Kebijakan ini bertujuan untuk memastikan bahwa seluruh kinerja TI sesuai dengan arahan dan kebijakan berlaku.
- Kinerja TI merupakan kinerja yang diturunkan sampai ke level personil TI, didefenisikan, diukur dan dinilai melalui sistem *Integrated Competency Base Human Resources Management System* yang digunakan dan diterapkan oleh perusahaan dalam menilai kinerja karyawannya. Kinerja dan kegiatan TI dilaporkan secara berkala setiap Triwulan dan Setiap Tahunannya melalui Laporan Manajemen Perusahaan.

h. Monitor dan Evaluasi Pengendalian Internal

- Defenisi : Kebijakan monitor dan evaluasi pengendalian internal (*internal control*) adalah kebijakan yang diperlukan untuk mengevaluasi kegiatan sistem TI perusahaan.

- Tujuan : Untuk memberikan jaminan mengenai operasi TI yang efektif dan efisien dan kepatuhannya terhadap kebijakan dan aturan yang berlaku.
- Kebijakan ini terkait erat dengan Lampiran Nomor XII.

i. Pengelolaan *compliance external regulator*(Ketaatan terhadap kebijakan / standar di bidang TI)
   - Defenisi : Kebijakan pengelolaan *compliance external regulation* adalah kebijakan yang mengatur proses.
   - identifikasi kebutuhan *compliance* dan proses evaluasi untuk menjamin *compliance* terhadap aturan yang berlaku.
   - Tujuan : Kebijakan ini bertujuan untuk memastikan bahwa persyaratan aturan atau hukum yangberlaku telah dipenuhi.
   - Dalam penerapan sistem TI , perusahaan wajib mematuhi dan memenuhi aspek ketaatan terhadap kebijakan/standar di bidang TI.

LAMPIRAN

Penomoran setiap kebijakan di bawah ini menjadi Nomor Lampiran

I. Kebijakan Perencanaan Jangka Pendek dan Jangka Panjang TI (Master Plan TI)

1. Perencanaan Jangka Panjang/Rencana Jangka Panjang (RJP) maupun Jangka Pendek TI harus selaras dengan bisnis untuk mendukung Visi , Misi dan Tujuan Perusahaan.
2. Perencanaan Jangka Panjang/Rencana Jangka Panjang (RJP) maupun Jangka Pendek TI dalam implementasinya menyesuaikan dengan kondisi perusahaan saat itu dan perubahan-perubahan yang terjadi baik di dalam maupun di luar perusahaan.
3. RJP harus mampu menerjemahkan cita-cita dan keinginan baik dari manajemen , pengguna serta maupun perubahan-perubahan/ dinamika yang terjadi baik di dalam maupun di luar perusahaan.
4. Perencanaan Jangka Panjang/Master Plan/Blue Print TI dibuat setiap 5 tahun sekali yang disahkan oleh Direksi PT. BALAIRUNG CITRAJAYA SUMBAR.
5. Dalam menyusun RJP TI melibatkan partisipasi aktif dari seluruh unit kerja dan yang bertanggung jawab untuk menyusun RJP TI adalah unit kerja yang mengelola TI perusahaan atau bisa disebut dengan istilah pengelola TI atau Tim kerja yang dibentuk Direksi atau konsultan independen yang mempunyai kompetensi dalam pembuatan Master Plan TI .
6. Mekanisme penyusunan rencana strategis TI atau RJP TI adalah sebagai berikut :
   - Direksi menugaskan Pengelola TI atau Tim Kerja atau Konsultan (atau disebut dengan Tim Pembuat RJP TI).
   - Tim Pembuat RJP TI menggali aspirasi manajemen yaitu aspirasi mengenai apa yang peran TI yang diharapkan dalam mendukung bisnis perusahaan.
   - Selain itu juga Tim pembuat RJP TI menggali kebutuhan akan TI dari seluruh unit kerja.
   - Tim Pembuat RJP TI membuat *gap* analisis.
   - Tim Pembuat RJP TI merumuskan dan menyusun RJP TI dengan susunan sesuai dengan Peraturan Menteri Nomor PER-02/MBU/2013.
   - Tim Pembuat RJP TI mempresentasikan hasil penyusunan RJP TI ke depan Direksi
   - Pengesahan RJP TI oleh Direksi PT. BALAIRUNG CITRAJAYA SUMBAR.
7. RJP TI harus sejalan dengan Panduan Penyusunan Master Plan TI dari Kementrian yang menjadi satu kesatuan yang tidak terpisahkan dengan Kebijakan ini.
8. Pembuatan RJP TI dimulai dari Visi, Misi, Tujuan, arah bisnis perusahaan dan masukan dari Dewan Direksi / arahan dari Dewan Komisaris kemudian juga inventarisasi kebutuhan dari seluruh Bagian dan Unit Kerja di Lingkungan PT. BALAIRUNG CITRAJAYA SUMBAR.

9. Hal yang harus dimasukkan dalam RJP TI adalah memuat aspek-aspek sebagaimana mengacu kepada Peraturan Menteri Nomor PER- 02/MBU/2013 sebagai berikut :
    - Ringkasan Eksekutif
    - Lembar Pengesahan dari Direksi
    - Konteks Bisnis
    - Kajian Teknologi Informasi
    - Portofolio Proyek
    - *Roadmap*
    - Tata Kelola
10. RJP TI yang telah dibuat dan diimplementasikan terus dimonitor dan direview secara berkala dan disesuaikan dengan kebutuhan-kebutuhan atau perubahan-perubahan yang terjadi di dalam maupun di luar perusahaan. Sesuai dengan Pasal 3 Peraturan menteri Nomor PER-02/MBU/2013 , Direksi wajib melakukan monitoring dan evaluasi pelaksanaan RJP TI.
11. Perencanaan Jangka Pendek TI tertuang dalam RKAP perusahaan yang dibuat setahun sekali.
12. RKAP TI merupakan turunan dari RJP TI.

II. Kebijakan Penggunaan dan Pengelolaan Komputer dan Perangkat Keras TI

1. Perangkat keras TI berupa komputer, perangkat jaringan dan periferal yang digunakan harus mendukung pekerjaan dan proses bisnis perusahaan.
2. Seluruh perangkat keras yang dipunyai perusahaan harus dirawat dan dipelihara dengan baik.
3. Sebagai bentuk preventif maintenance perangkat keras adalah dengan melakukan perawatan secara rutin dan berkala.
4. Dalam perawatan perlu menghindari kondisi yang dapat menyebabkan kesalahan dan kerusakan yang tidak dikehendaki. Beberapa penyebab yang harus dihindari karena akan mempengaruhi komputer dan periferal adalah:
    - Debu atau kotoran lain seperti asap, bahan kimia, serat karpet ,sisa-sisa makanan dan minuman serta partikel halus lainnya merupakan benda yang harus dihindarkan dan selalu dibersihkan dari ruang komputer. Debu yang terletak di dalam komputer atau peripheral computer dapat menyebabkan kerusakan misalnya menyebabkan hubungan singkat antar komponen. Sebagai pencegahan kerusakan yang diakibatkan oleh debu perlu dilakukan hal-hal berikut :
        a. Jangan membawa makanan dan minuman ke dalam ruang komputer
        b. Jangan merokok di dalam ruang komputer
        c. Bersihkan debu-debu yang melekat di meja, kursi, lantai, serta tampat-tempat lain
        d. Bersihkan juga debu-debu yang melekat pada casing komputer,

keyboard, mouse,monitor dan printer

e. Gunakan penyedot debu dalam membersihkan debu, jangan menggunakan kemucing (sulak)

- Panas, setiap peralatan elektronik akan menghasilkan panas. Kompon enelektronik di dalam komputer terutama di bagian *motherboard* dan monitor . Panas yang berlebih pada prosesor dan memori akan menyebabkan fungsi system menjadi terganggu dan mengurangi usia komponen. Pencegahan kerusakan akibat panas dapat dilakukan dengan cara :
  a. Hindari sinar matahari langsung
  b. Berikan ruang sirkulasi udara yang cukup dalam meletakkan komputer dan peripheral lainnya
  c. Bila memungkinkan menggunakan pendingin ruangan
- Medan Elektromagnetis, disebabkan oleh kabel listrik, transformator, magnet speaker dan sebagainya. Medan elektromagnetis akan mengacaukan fungsi komputer, merusak data dalam media penyimpan magnetis misalnya hardisk dan merusak tampilan pada layar monitor. Sebagai pencegahan pengaruh elektromagnetis terhadap fungsi kerja komputer dan periferalnya adalah :
  a. Jauhkan telepon yang menggunakan bel magnetik
  b. Jauhkan speaker aktif dari komputer, monitor dan eksternal hardisk
  c. Jangan meletakkan media penyimpanan magnetis di dekat monitor, printer, speaker aktif serta periferal lain yang menghasilkan elektromagnetik.
  d. Jauhkan trafo penstabil tegangan dari komputer, periferal dan penyimpan data magnetis
- Elektrostatis, merupakan bahan yang bermuatan elektrostatis dan dapat menghasilkan tegangan elektrostatis, jika tegangan ini sangat besar maka akan merusak komponen elektronik yang ada dalam komputer dan periferal. Pencegahan yang dapat dilakukan agar tidak terjadi kerusakan akibat tegangan elektrostatis adalah : Peralatan harus mempunyai *grounding* yang baik.
- Gangguan Daya Listrik yang apling sering terjadi adalah fluktiasi tegangan listrik serta *noise* (derau). Fluktuasi yang terlalu tinggi dapat mengakibatkan komputer atau periferal menjadi macet (*hang*) atau dapat menyebabkan media penyimpanan rusak. Pencegahan yang perlu dilakukan adalah:
  a. Kondisi stop kontak listrik harus selalu baik, stop kontak yang sudah kendor harus diganti
  b. Jika memungkinkan menggunakan stabilisator tegangan (stavolt) baik secara terpusat atau sendiri- sendiri di setiap komputer
  c. Jika memungkinkan menggunakan UPS

5. Teknis tata cara perawatan hardware dapat dilihat pada panduan in house training perawatan hardware yang menjadi satu kesatuan yang tidak dipisahkan dengan panduan ini.
6. Pemeliharaan perangkat keras secara umum dilakukan secara berkala tidak hanya oleh pengelola TI perusahaan tapi melibatkan partisipasi aktif dari pengguna perangkat untuk selalu merawat dan menjaga perangkat kerasnya masing-masing.
7. Untuk menjaga ketersediaan (*Availability*) dari perangkat keras digunakan proteksi perangkat seperti menggunakan *stabilizer voltage*, UPS dan bangunan yang menggunakan anti petir untuk menghindari rusaknya perangkat elektronis karena induksi langsung atau pun langsung dari petir.
8. Pengelola TI melakukan identifikasi dan assesment risiko yang terkait dengan ancaman dan keamanan dalam penggunaan perangkat keras.
9. Kebijakan yang mengatur tentang perolehan dan pengadaan perangkat TI (infrastruktur, fasilitas, *hardware, software* dan jasa lainnya) mengikuti prosedur pengadaan yang berlaku diterapkan oleh perusahaan.
10. Setiap instalasi dan perubahan perangkat TI harus diketahui dan dicatat oleh Pengelola TI.

III. Kebijakan Penggunaan , Pembuatan dan Pengelolaan Aplikasi Perangkat Lunak

1. Perangkat lunak yang digunakan baik Sistem Operasi atau program aplikasi harus mendukung pekerjaan dan proses bisnis perusahaan
2. Perusahaan memegang prinsip kepatuhan pada Hak Atas kekayaan Intelektual (HAKI) akan lisensi *software*. Alternatif pemenuhan kepatuhan akan lisensi dapat menggunakan aplikasi pen source.
3. Seluruh perangkat lunak yang digunakan harus legal dan karyawan dilarang menggunakan, mendistribusikan dan menyebarluaskan perangkat lunak ilegal.
4. Seluruh perangkat lunak yang digunakan harus bebas dari virus, *malware* dan *trojan.*
5. Seluruh aplikasi yang diinstal di komputer harus sepengetahuan Sub Bagian Teknologi Informasi dan setiap penambahan aplikasi juga harus melalui sepengetahuan Sub Bagian Teknologi Informasi.
6. Pembuatan aplikasi perangkat lunak baik yang dibuat secara mandiri oleh karyawan maupun oleh Pihak III harus sesuai dengan kebutuhan perusahaan , mendukung pekerjaan dan selaras dengan proses bisnis perusahaan.Pembangunan maupun pengembangan aplikasi berasal dari kebutuhan perusahaan atau pengguna, kebutuhan ini dikelola dan juga merupakan bagian dari proses menerjemahkan kebutuhan fungsional dan kontrol bisnis menjadi sebuah desain yang efektif dan efisien.
7. Dalam membangun suatu aplikasi mengacu kepada metodologi

pembangunan aplikasi yang secara umum sudah digunakan yaitu *System Development Lyfe Cycle* (SDLC). SDLC adalah keseluruhan proses dalam membangun sistem melalui beberapa langkah. Ada beberapa model SDLC. Model yang cukup populer dan banyak digunakan adalah *waterfall*. Beberapa model lain SDLC misalnya *fountain, spiral, rapid, prototyping, incremental, build & fix, dan synchronize & stabilize.* Dengan siklus SDLC, proses membangun sistem dibagi menjadi beberapa langkah dan pada sistem yang besar, masing-masing langkah dikerjakan oleh tim yang berbeda. Dalam sebuah siklus SDLC, terdapat enam langkah. Jumlah langkah SDLC pada referensi lain mungkin berbeda, namun secara umum adalah sama. Langkah tersebut adalah :

a. Analisis sistem, yaitu membuat analisis aliran kerja manajemen yang sedang berjalan
b. Spesifikasi kebutuhan sistem, yaitu melakukan perincian mengenai apa saja yang dibutuhkan dalam pengembangan sistem dan membuat perencanaan yang berkaitan dengan proyek sistem
c. Perancangan sistem, yaitu membuat desain aliran kerja manajemen dan desain pemrograman yang diperlukan untuk pengembangan sistem informasi
d. Pengembangan sistem, yaitu tahap pengembangan sistem informasi dengan menulis program yang diperlukan
e. Pengujian sistem, yaitu melakukan pengujian terhadap sistem yang telah dibuat
f. Implementasi dan pemeliharaan sistem, yaitu menerapkan dan memelihara sistem yang telah dibuat

8. Pembuatan aplikasi perangkat lunak di lingkungan PT. BALAIRUNG CITRAJAYA SUMBAR harus mempunyai prinsip terintegrasi, terpadu, menghindari duplikasi input data untuk mencegah terciptanya pulau-pulau informasi (*information island*) dan jika memungkinkan juga mendukung pemrosesan data secara *real time*dan *online.*
9. Aplikasi perangkat lunak yang dibangun di lingkungan PT. BALAIRUNG CITRAJAYA SUMBAR mempunyai *platform Web/Visual/Desktop Based* dengan menggunakan database berbasis SQL (*Structured Query Language*) yang dapat diakses baik dari jaringan Intranet atau Internet dengan menggunakan level akses keamanan.
10. Khusus untuk aplikasi berbasis web yang dibangun di lingkungan PT. BALAIRUNG CITRAJAYA SUMBAR harus terpasang di server yang dikelola oleh Sub Bagian Teknologi Informasi dan mempunyai domain resmi perusahaan yaitu ptpn5.co.id atau ptpn5.com.
11. Dalam pembuatan aplikasi perangkat lunak sedapat mungkin dibuat secara mandiri oleh personil perusahaan yang mempunyai keahlian di bidang pemrograman perangkat lunak dan jika skala pekerjaan bersifat lintas sektoral

maka pekerjaan pembuatan aplikasi tersebut dibuat dalam bentuk Tim Kerja atau melalui Surat Penugasan

12. Jika aplikasi dibuat oleh pihak III maka pihak III yang ditunjuk bekerja secara profesional , memenuhi kebutuhan perusahaan dan sesuai dengan perjanjian kerja.Selain itu juga pihak III menjaga kerahasiaan dan keamanan data sebagaimana yang tercantum pada Lampiran Nomor XI mengenai Keamanan Sistem Informasi dan TI (*IT Security*) mendukung *source* aplikasi yang dibangun menjadi milik perusahaan dan pihak III yang membuat aplikasi wajib melakukan *Transfer Knowledge* kepada personil pengelola TI perusahaan.
13. Pembuat aplikasi melakukan tindakan yang dibutuhkan agar pemakai dan manajemen dapat menggunakan aplikasi dengan benar dan sesuai dengan peraturan yang berlaku.
14. Memastikan agar system yang dibangun memakai standar bahasa pemrograman yang telah ditentukan perusahaan dan memastikan agar software yang dipakai untuk pembangunan system memiliki lisensi dan bukan illegal *software.*
15. Konfigurasi dan implementasi atas aplikasi/*software* dilakukan oleh personil pengelola TI yang berkompeten. Upgrade sistem dilakukan sesuai dengan kebutuhan untuk meningkatkan kualitas *software* yang digunakan. Review atas *software* dilakukan dalam rangka penyempurnaan , perbaikan aplikasi dan *continous improvement*. Strategi dan rencana pemeliharaan aplikasi dilakukan secara berkala.

IV. Kebijakan Penggunaan dan Pengelolaan Infrastruktur Jaringan LAN/WAN(Local Area Network / Wide Area Network)

1. Sistem Jaringan LAN/WAN yang digunakan harus mendukung pekerjaan dan proses bisnis dan kebutuhan perusahaan.
2. Manajemen kapasitas infrastruktur jaringan dan perencanaan kapasitas mengikuti dan memenuhi kebutuhan perusahaan, seperti banyaknya aplikasi yang berjalan di atas infrastruktur jaringan, banyaknya pengguna dan faktor-faktor lainnya yang mempengaruhi perencanaan kapasitas jaringan.
3. Avaibility jaringan LAN/WAN berhubungan dengan *Service Level Agreement* (SLA) yang diberikan oleh penyedia koneksi jaringan dan wajib memenuhi tingkat layanan yang dipersyaratkan perusahaan .
4. Untuk standarisasi , system Jaringan LAN/WAN perusahaan menggunakan protocol TCP/IP (*Transmission Control Protocol* / Internet Protocol).
5. Sistem Jaringan LAN/WAN perusahaan dikelola oleh Sub Bagian Teknologi Informasi bidang SIstem Jaringan dan Komunikasi Data.
6. Pengelolaan Jaringan LAN/WAN harus terus selalu meningkatkan kualitas jaringan, keamanan, efisiensi, efektifitas dan ekonomis dalam pemanfaatannya.
7. Implementasi infrastruktur jaringan LAN/WAN diselaraskan dengan

implementasi pada aspek aplikasi.

8. Kebutuhan koneksi komputer dan perangkat peripheral ke Jaringan LAN/WAN dari Bagian-Bagian maupun unit kerja disampaikan melalui Memo tertulis kepada Bagian yang membawahi Sub Bagian TI.
9. Untuk efisiensi penggunaan *peripheral* seperti penggunaan printer perlu diintensifkan penggunaan *sharing* printer melalui jaringan LAN/WAN.
10. Penggunaan jaringan nirkabel LAN (Wireless WAN) harus menggunakan system keamanan dengan menggunakan *account* berupa *username* dan *password*.
11. Yang berhak menggunakan Wireless LAN adalah karyawan yang telah memiliki *account* untuk mengakses jaringan Wireless LAN.
12. Tata cara penggunaan Jaringan WAN secara lengkap dapat dilihat pada panduan penggunaan Jaringan WAN yang menjadi bagian yang tidak terpisahkan dari kebijakan ini.

V. Kebijakan Penggunaan dan Pengelolaan Infrastruktur Jaringan Internet

1. Pemakaian internet harus mendukung pekerjaan dan proses bisnis perusahaan, pemakaian internet yang sehat dan baik adalah bertujuan untuk meningkatkan motivasi dan mendukung produktifitas kerja karyawan.
2. Yang dapat mengakses internet adalah karyawan yang telah diberi hak akses ke nomor IP komputer maupun yang mendapat *username* dan *password* wifi.
3. Penggunaan akses internet diatur sesuai dengan kebutuhan Bagian dan unit kerja.
4. Penambahan *user* ke internet sebagaimana yang disebutkan pada point sebelumnya dimungkinkan melalui mekanisme sebagai berikut :
   - Bagian/unit kerja yang memerlukan akses tambahan ke internet mengirim surat permohonan penambahan koneksi ke Sub Bagian TI dengan tembusan kepada Direksi
   - Isi surat permohonan memuat : nama-nama *user* yang akan terkoneksi ke internet , alasan kebutuhan koneksi, intensitas koneksi ke internet beserta daftar website yang sering dikunjungi yang berkaitan dengan pekerjaan
5. Pengelolaan koneksi internet dilakukan oleh personil TI.
6. Pengelola dan penyedia layanan internet harus terus meningkatkan keandalan koneksi, kenyamanan dan keamanan berkoneksi serta efisiensi bandwith.
7. Karyawan yang memiliki hak akses ke internet dilarang membuka halaman web yang memiliki konten negatif terutama bermuatan SARA dan berbau pornografi.
8. Karyawan dilarang mengunduh (*download*) file dari internet yang tidak berhubungan dengan pekerjaan dan mendukung produktifitas kerja.
9. Pengelolaan koneksi internet menutup akses ke situs-situs yang mengandung muatan pornografi, SARA maupun situs-situs yang mengandung *malware, phising*, dll.

VI. Kebijakan Penggunaan dan Pengelolaan E-mail Perusahaan

1. Email perusahaan yang digunakan harus mendukung pekerjaan dan proses bisnis perusahaan.
2. Yang berhak memiliki *account* e-mail perusahaan adalah karyawan PT. BALAIRUNG CITRAJAYA SUMBAR yang masih aktif bekerja.
3. Untuk mendapatkan e-mail perusahaan , karyawan melalui Bagian/Unit kerjanya masing-masing menjajukan kepada Sub Bagian Teknologi Informasi dengan perihal pengajuan *account* e-mail perusahaan dan berisi nama karyawan.
4. Setiap karyawan yang telah memiliki account e-mail dilarang memberikan *account* e-mailnya kepada orang lain.
5. Pengelola e-mail server perusahaan adalah personil dari TI.
6. Pengelola e-mail server berkewajiban melakukan maintenance E-Mail Server , meng-*update patch system security* serta upgrade system jika diperlukan.
7. Untuk keperluan komunikasi resmi setiap karyawan harus menggunakan email resmi perusahaan.
8. E-Mail Perusahaan hanya digunakan untuk komunikasi antara karyawan perusahaan PT. BALAIRUNG CITRAJAYA SUMBAR dengan karyawan Perusahaan lain yang berhubungan dengan pekerjaan.
9. Alamat E-mail resmi perusahaan yaitu :corporatebcs@balairung-hotel.co.id dikelola oleh Bagian Sekretaris Perusahaan.
10. Setiap Bagian dan unit kerja yang memiliki e-mail resmi Bagian/Unit kerja mengelola e-mailnya dengan baik dan dipergunakan untuk keperluan komunikasi eksternal.
11. Dalam menggunakan e-mail resmi perusahaan setiap *user* harus memperhatikan hal-hal beikut ini :
    - Dilarang dengan sengaja mengirim dan menyebarkan SPAM e- mail, content yang bermuatan negatif terutama yang bermuatan SARA dan pornografi, penyebaran file yang mengandung virus.
    - Dalam mengirim e-mail perlu diperhatikan etika sebagai berikut:
        a. Gunakan salam pembuka seperti Selamat Pagi/*Dear*/Yth. Bapak/Ibu
        b. Pergunakan kalimat dengan jelas dan singkat
        c. Jangan menggunakan huruf besar di seluruh kalimat karena penggunaan huruf besar di seluruh kalimat akan menimbulkan persepsi bahwa anda sedang marah
        d. Jangan menggunakan tanda baca yang berlebihan
        e. Jika anda ingin mengirim lampiran (*attachment*) e- mail berupa file dengan ukuran yang besar (Lebih besar dari 2 Mega Byte) , kita mengirimkan e-mail permohonan ijin terlebih dahulu ke tujuan apakah kita dapat mengirim file attachment dengan ukuran sekian MB
        f. Jangan mem-*forward* dan me-*reply* e-mail tanpa terlebih dahulu di edit (

body email jangan *reply/forward* semua)

g. Menggunakan subyek yang relevan dengan isi e-mail

12. E-mail Perusahaan tidak diperkenankan mengikuti mailing list yang memiliki konten negatif dan tidak mendukung produktifitas kerja.
13. E-Mail perusahan tidak diperkenankan untuk registrasi di jejaring sosial seperti Facebook, Twiter, ataupun ke website tertentu guna meminimalisir peyebaran E-Mail SPAM.
14. Cara penggunaan e-mail resmi perusahaan dapat dilihat pada Panduan Penggunaan E-mail dan Web Intranet Perusahaan yang menjadi satu kesatuan yang tidak terpisahkan dengan kebijakan ini.

VII. Kebijakan Penggunaan dan Pengelolaan Pemakaian Siskomdat/Simpelweb

1. Siskomdat (Sistem Komunikasi Data)/Simpelweb (Sistem Pengiriman Surat dan laporan Berbasis Web) merupakan sistem pengiriman Surat dari Unit Kerja Ke Kantor Pusat dan begitu sebaliknya. Sistem ini menggantikan sistem pengiriman berita berbasis Ratel (Radio Telekomunikasi). Siskomdat/Simpelweb wajib digunakan seluruh Bagian/unit kerja dalam mendukung proses pengiriman berita di lingkungan internal.
2. Siskomdat/Simpelweb yang digunakan harus mendukung pekerjaan dan proses bisnis perusahaan.
3. Pengelola aplikasi dan server Siskomdat/Simpelweb adalah personil TI.
4. Yang berhak mengakses aplikasi Siskomdat/Simpelweb adalah personil Bagian/Unit Kerja yang telah ditunjuk.
5. Cara penggunaan aplikasi Siskomdat/Simpelweb dapat dilihat pada Panduan Penggunaan Aplikasi Siskomdat/Simpelweb yang menjadi satu kesatuan yang tidak terpisahkan dengan kebijakan ini.

VIII. Kebijakan Penggunaan dan Pengelolaan Web Intranet

1. Penggunaan Web Intranet harus mendukung pekerjaan dan proses bisnis perusahaan.
2. Yang berhak mengakses Web Intranet perusahaan adalah karyawan PT. BALAIRUNG CITRAJAYA SUMBAR yang telah memiliki *account* berupa *user*name dan password web intranet.
3. Pengelola aplikasi dan server Web adalah personil TI.
4. Pengelola aplikasi dan server harus menjaga ketersediaan (availability) dan keamanan aplikasi serta mengembangkan dan menyempurnakan aplikasi sesuai dengan kebutuhan perusahaan.
5. Karyawan yang telah memiliki *account* wajib mengakses web intranet dan menggunakannnya untuk mendukung produktifitas kerja

6. Setiap *user* web intranet ikut berkontribusi aktif dalam pengisian content, *sharing knowledge* dan berbagi dalam penyebaran informasi seputar kegiatan perusahaan.
7. Cara penggunaan Web Intranet perusahaan dapat dilihat pada Panduan Penggunaan E-mail dan Web Intranet Perusahaan yang menjadi satu kesatuan yang tidak terpisahkan dengan kebijakan ini.
8. Setiap *user* pada aplikasi Web Intranet dilarang menyimpan dan menyebarkan file-file yang bermuatan negatif dan yang tidak berhubungan dengan pekerjaan.

IX. Kebijakan Risiko Teknologi Informasi (IT Risk)

1. Proses manajemen risiko TI atau IT Risk merupakan bagian yang tidak terpisahkan dari manajemen umum. IT Risk harus menjadi bagian dari budaya organisasi, praktek terbaik organisasi dan proses bisnis organisasi.
2. Risk merupakan kombinasi dari komponen kejadian yang menyangkut ancaman (*threat*), *vulnerability* dan *impact. Vulnerability* merupakan kelemahan dari system sedangkan impact merupakan penilaian atas pengaruh ancaman yang dilakukan terhadap baik asset maupun tujuan dari organisasi dengan memanfaatkan kelemahan dari sistem.
3. Identifikasi Risiko/Daftar Risiko dari TI dapat dilihat pada Risk Assessment dan panduan dan kebijakan Manajemen Risiko PT. BALAIRUNG CITRAJAYA SUMBAR yang menjadi satu kesatuan yang tidak terpisahkan dengan kebijakan ini.
4. Monitoring atas rencana aksi atas risiko TI diatur pada Panduan Manajemen Risiko perusahaan yang menjadi bagian tak terpisahkan dari kebijakan ini.
5. Untuk menghindari kegagalan sistem TI, khususnya untuk sistem yang sifatnya kritikal maka harus diterapkan *contingency planning* berupa penerapan *Disaster Recovery Planning* atau suatu kegiatan yang menfokuskan pada semua aksi yang perlu dilakukan sebelum, ketika, dan setelah terjadinya bencana dimana dalam konteks ini adalah bencana yang mengakibatkan kegagalan sistem TI.
6. Untuk menghindari hilang atau rusaknya file-file penting pendukung pekerjaan, setiap karyawan harus mem-*backup* file nya tersebut melalui menu *Backup File* yang ada di Web Intranet.
7. Agar data secara *logic* dapat tersimpan secara rapi di media penyimpanan seperti hardisk , setiap pengguna komputer melakukan proses defragmentasi minimal 1 bulan sekali
8. Untuk menghindari kerusakan data atau system diakibatkan oleh virus komputer di setiap komputer harus terinstal program Antivirus yang selalu update.
9. Secara berkala yaitu seminggu 2 kali setiap pengguna komputer harus men-scan komputernya dengan program antivirus.
10. Setiap pengguna komputer harus berhati-hati terhadap media penyimpanan seperti USB Flash Disk ataupun hardisk eksternal yang terkoneksi ke komputer

dan sebelum mengakses data apapun di media penyimpanan tadi pengguna komputer harus men-scan media penyimpanan tersebut dengan program antivirus

11. Untuk menghindari kerusakan dan kehilangan data diakibatkan kegagalan listrik maka setiap *personal computer* (PC) dapat menggunakan perangkat UPS.

X. Kebijakan Pengelolaan Server

1. Server yang digunakan harus mendukung pekerjaan dan proses bisnis perusahaan.
2. Penggunaan server dan perangkat pendukungnya harus disesuaikan dengan kebutuhan dan kondisi perusahaan.
3. Server – server di tempatkan pada ruangan khusus (ruangan server) yang memiliki system kelistrikan yang baik , system *backup* catu daya/ UPS, CCTV dan memiliki pendingin ruangan (AC). Akses control / masuk ke ruangan server dibatasi dan hanya petugas yang berhak saja yang bisa masuk ke ruangan server.
4. Server yang digunakan memiliki fasilitas backup sehingga jika terjadi kegagalan aplikasi maupun kerusakan pada server, system dan aplikasi dapat berjalan dan tidak terganggu operasionalnya.
5. Pengelola server tetap melakukan maintenance ,*update/patch* jika diperlukan, memperhatikan aspek keamanan pada server yang dikelola serta melakukan pengembangan sebagai bentuk *continuous improvement* pada pengelolaan server di lingkungan PT. BALAIRUNG CITRAJAYA SUMBAR.
6. Pengelolaan lingkungan fisik server. Jika dimungkinkan Server ditempatkan pada lingkungan geografis yang relatif aman dari bencana dan pada bangunan dimana server tersebut berada terus dimonitor dan dijaga oleh pihak keamanan (pengaturan keamanan aset TI) sehingga aman dari kemungkinan kecurian, kebakaran, air dan ledakan

XI. Kebijakan Keamanan Sistem Informasi danTI (IT Security)

Sistem Manajemen Keamanan Informasi mengacu kepada kerangka kerja ISO 27001 yang mencakup beberapa klausa sebagai berikut :

a. Kebijakan keamanan informasi
b. Organisasi keamanan informasi
c. SDM Menyangkut keamanan informasi
d. Manajemen asset
e. Akses control
f. Kriptopgrafi
g. Keamanan fisik dan lingkungan
h. Keamanan operasi

i. Keamanan komunikasi
j. Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
k. Hubungan dengan pemasok
l. Pengelolaan insiden keamanan informasi
m. Manajemen kelangsungan usaha (business continuity management).
n. Kepatuhan

Klausa tersebut di atas diuraikan pada point-poin sebagai berikut:

1. Tujuan dari Keamanan system informasi dan TI adalah agar system informasi yang dibangun atau yang sedang berjalan terjamin integritasnya dan keamanannya.
2. Keamanan system informasi merupakan urusan dan tanggung jawab seluruh karyawan.
3. Langkah keamanan system informasi harus sesuai dengan peraturan dan undang-undang yang berlaku.
4. Organisasi keamanan informasi terkait dengan tanggung jawab secara umum yang berkaitan dengan pemakaian dan keamanan system informasi dapat dibedakan atas kategori sebagai berikut :
   - Tanggung jawab karyawan
   - Tanggung jawab manajer

   Secara spesifik, personil yang memiliki kaitan dengan sistem komputerisasi/sistem informasi adalah sebagai berikut :
   - Personil yang ditunjuk sebagai pemilik sistem
   - Persinil lain yang dikategorikan sebagai pemakai.
   - Pengembang sistem (pimpinan proyek, sistem analis, programmer) jika ada
   - Spesialis database.
   - Spesialis jaringan komunikasi
   - Spesialis PABX jika ada
   - Spesialis data processing (operator) jika ada
   - Auditor (EDP) jika ada
   - Administrator sistem keamanan. jika ada

Personil administrasi Dan dapat diuraikan sebagai berikut :

Karyawan

Yang dimaksud karyawan adalah semua orang yang bekerja di dalam perusahaan termasuk karyawan kontrak, karyawan sementara, dan karyawan magang.

Tanggung jawab.

Setiap karyawan harus :

1. Mengetahui secara sadar untuk bertindak sesuai dengan peraturan

keamanan yang berlaku. Pelajari aturan-aturan keamanan informasi yang sudah ada. Buku panduan (yang disusun oleh sistem Administrator) harus diberikan oleh bagian personalia pada saat karyawan memulai bertugas. Panduan ini merupakan salah satu bagian dari buku panduan peraturan perusahaan.

2. Melaporkan kepada atasannya, apabila mengetahui atau melihat kejanggalan atau kekurangan dalam hal keamanan.
3. Memastikan agar semua informasi yang sensitif mengenai perusahaan tidak akan disebarluaskan yang akan mengakibatkan kerugian bagi perusahaan. Kembalikan seluruh hak milik perusahaan yang berkaitan dengan data pada saat memutuskan hubungan kerja.
4. Setelah menerima password, mengganti langsung dan secara teratur sesuai dengan peraturan yang telah ditentukan.

Manajer

Yang dimkasud manajer adalah seseorang yang secara fungsional membawahi dan bertanggung jawab atas karyawan yang bekerja di perusahaan.

Tanggung jawab :

1. Memastikan agar semua bawahannya mengetahui tanggung jawab mereka dan pertauran keamanan sistem informasi yang berlaku serta memonitor agar mereka tetap mematuhinya.
2. Memastikan agar staf bagiannya memiliki sumber daya dan kahlian yang memadai untuk melaksanakan tanggung jawab mereka atas keamanan informasi.
3. Memastikan agar karyawan bawahannya mendapat akses ke sistem sesuai dengan fungsi yang mereka emban.
4. Mengatur pemisahan tugas/pekerjaan karyawan di bagiannya sesuai dengan fungsi mereka yang berkaitan dengan sistem informasi sesuai dengan otoritas yang diberikan.
5. Memastikan agar setiap personel mengetahui bagaimana cara pengamanan keamanan berfungsi yang telah diintegrasikan dalam prosedur kerja harian.
6. Bertindak cepat dan tepat waktu sesuai kemmapuannya apabila terjadi kejadian yang mengganggu kelancaran pekerjaan operasional sehari-hari berkaitan dengan kemanan sistem informasi. Ia harus memastikan agar user mengetahui apa yang harus diperbuat saat layanan komputer yang sangat dibutuhkan, tidak bekerja seperti yang seharusnya.
7. Memastikan agar perusahaan tidak tergantung pada satu orang saja untuk setiap pekerjaan utama.

Tanggung Jawab Secara Spesifik yang Berkaitan dengan Keamanan Sistem

Informasi

Pemilik sistem

Pemilik sistem adalah mereka yang bertanggung jawab atas kebenaran desain fungsional dari sistem komputer di perusahaan dan yang memiliki wewenang untuk menentukan penggunaannya.

Tanggung jawab. Pemilik harus :

1. Mengetahui nilai dan risiko dari sistem komputer yang digunakan, mengklasifikasi sistem tersebut berdasarkan risikonya sesuai dengan kepekaannya dan mengevaluasinya secara berkala.
2. Bertanggung jawab untuk kemanan sistemnya yang memadai. Ia harus merumuskan kebutuhan akan keamanan sistem informasi yang dikehendaki secara umum berdasarkan kepekaan risiko keamanan sistem. Secara rutin ia harus mengevaluasi kepekaan risiko keamanan sistem dan merevisinya apabila dibutuhkan.
3. Mengotorisasi pengaksesan dan penggunaan sistemnya serta memastikan bahwa penggunaan otorisasi diimplementasikan secara benar.

Pemakai

Pemakai adalah semua karywan perushaan yang memakai sistem komputer.

Tanggung jawab. Pemakai harus:

1. Menggunakan sistem informasi sesuai dengan tanggung jawabnya untuk melaksanakan tugasnya.
2. Bertanggung jawab atas semua transaksi/tindakan yang dilakukan terhadap sistem dengan menggunkan User-ID- nya.
   Semua tindakannya bersama User-ID- nya akan terekam didalam audit trail.
3. Mengetahui semua intruksi untuk menggunakan sistem beserta aturan keamanan dan mematuhinya.
4. Melaporkan kepada atasannya apabila terjadi kejanggalan pada saat pengoperasian sistemnya misalnya:
   - Pelanggaran hak akses
   - Kegagalan sistem
   - Transaksi elektronik yang tidak terkontrol dengan baik atau sering mendapat gangguan sehingga pelaksanaanya dan/ atau pemrosesan gagal.
5. Setelah menerima password, mengganti langsung dan secara teratur sesuai dengan peraturan yang telah ditentukan.
6. Menyadari akibat dari sharing password (berbagi password) yang dapat mengakibatkan kerugian kepada perusahaan. Apabila hal ini terjadi, ia harus siap bertanggung jawab dan menerima konsekuensinya mulai dari

surat peringatan sampai pemutusan hubungan kerja. Semua transaksi yang dilakukan dengan password ini akan terekam di log file, sehingga editor dapat dengan mudah mengetahui pelakunya apabila terjadi diskrepansi.

7. Mengembalikan seluruh hak milik perusahaan yang berkaitan dengan data pada saat memutuskan hubungan kerja.
8. Membuat backup sendiri dari PC-nya, apabila menganggap datanya penting untuk dirinya, misalnya lembar kertas kerja dan lain-lain, sedangkan laporan yang penting akan disimpan di server.
9. Menyadari bahwa komputer dikantor hanya boleh digunakan untuk keperluan kantor atau yang berkaitan dengan pekerjaanya dan bukan untuk kebutuhan pribadi
10. Sign-Off dari sistem apabila ia akan menginggalkan tempat kerja untuk jangka waktu yang cukup lama. Mematikan computer sesuai dengan prosedur apabila ia akan pulang.
11. Memahami risiko apabila ia meninggalkan sistem tanpa penjangaan yang memadai (misalnya screen saver dengan password) untuk jangka waktu yang lama sehingga dapat

    digunakan secara sengaja atau tidak disengaja oleh pihak ketiga. Apabila fasilitas ini belum dimiliki, secara proaktif ia harus menginformasikan personil TI.
12. Menyadari dan berjanji tidak akan menginstall apa pun juga pada komputer yang dipakai. Hanya personil TI yang diperbolehkan menginstall software yang telah ditentukan oleh perusahaan dan yang berlisensi.

    Dalam praktiknya tidak jarang pemakai melanggar peraturan dengan menginstall sendiri software yang ia miliki (entah dari mana ia memilikinya, apakah ia men-download-nya sendiri atau mengcopy dari rekan/temannya).

Pengembang Sistem

Pengembang sistem adalah staf TI yang memiliki keahlian dalam bidang designing, programming, troubleshooting sistem, dan memilki tanggung jawab untuk memelihara, mengembangka, dan memelihara sistem computer atas nama pemilik sistem.

Tanggung Jawab. Pengembang Sistem harus:

1. Memastikan bahwa sistem yang akan dibangun telah ditentukan dan dipilih oleh pemiliknya bedasarkan kepekaan risiko sistem informasi dan kebutuhan pengontrolan dalam bentuk screening.
2. Menspesifikasikan kebutuhan atas penggunaan, pemonitoran, dan keamanan Sistem Informasi dengan cara berkonsultasi dengan pemilik sistem dan pihak lain yang terkait dengan fungsinya. Ia harus merumuskan

dan menyusun keamanan yang dibutuhkan.

3. Mengizinkan pemilik sistem, auditor, dan pihak fungsional lain yang terkait dengan tim pengembangan, untuk mengevaluasi hasil sementara atau akhir pengembangannya.
4. Melalukan tindakkan yang dibutuhkan agar pemakai dan manajemen dapat menggunakan Sistem Informasi dengan betul dan sesuai dengan peraturan.
5. Memastikan agar sistem yang dibangun memakai standar bahasa pemrograman perusahaan dan memastikan agar software yang dipakai untuk pembangunan sistem memiliki lisensi dan bukan illegal software.
6. Memastikan agar sistem secara otomatis sign-off atau log-off apabila pemakai meninggalkan tempatnya lebih lama daripada waktu yang ditentukan.
7. Berjanji untuk tidak mengungkapkan data produksi yang sensitif kepada pihak lain apabila ia telah mendapat wewenangnya. Data ini bias atau boleh didapat apabila ia akan melakukan pengujian data dengan data yang sebenarnya.
8. Mengetahui semua sistem yang ia kembangkan tidak akan ia perjualbelikan di luar perusahaan, baik selama ia masih sebagai karyawan perusahaan maupun sudah tidak sebagai karyawan lagi. Semua sistem yang dikembangkan di dalam organisasi adalah milik organisasi.
9. Berjanji tidak akan melakukan bypass aturan koneksi jaringan yang telah ditetapkan.
10. Mengembalikan kembali account yang memiliki hak sebagai administrator. Account ini dibutuhkan pada saat-saat tertentu misalnya pada saat menginstall software atau meng-configure sistem.

Spesialis Database

Spesialis database memiliki keahlian yang luas dalam bidang manajemen database dan memiliki tanggung jawab untuk memilih, mengembangkan, dan memelihara sistem database atas nama pemilik sistem.

Tanggung Jawab. Spesialis database harus:

1. Memastikan bahwa siste database yang akan digunakan sesuai dengan kebutuhan sistem yang akan dibagun dan telah dikonsultasikan dengna dan dikonfirmasikan oleh pimpinan pengembang sistem.
2. Memastikan agar database memiliki perlindungan sedemikian rupa sehingga orang yang tak berwenang tidak dapat menyusup database.
3. Memastikan agar pemakai yang berwenang menggunakan database sesuai dengan kewenangannya yang telah dianjurkan oleh manager terkait dan pimpinan proyek yang telah disetujui oleh pemilik sistem.
4. Berjanji untuk tidak mengungkapkan isi database kepada pihak lain.
5. Memindahkan database ke production environment apabila sistem baru

telah ditetapkan “SELESAI” oleh pemilik sistem.

Spesialis jaringan Komunikasi

Spesialis jaringan komunikasi adalah staf yang memiliki keahlian mengenai jaringan komunikasi misalnya LAN, WAN, VSAT, Radio IP beserta penunjangnya baik yang berupa hardware maupun yang berupa software dan memiliki tanggung jawab untuk memilih dan memelihara jaringan sistem komunikasi atas nama pemilik sistem.

Tanggung Jawab.

Spesialis jaringan komunikasi harus:

1. Memastikan bahwa jaringan sistem komunikasi yang akan digunakan sesuai dengan kebutuhan sistem yang akan dibangun dan telah dikonsultasikan dengan dan dikonfirmasikan oleh pimpinan pengembang sistem.
2. Memastikan agar jaringan sistem komunikasi selalu tersedia, karena ketersediaan jaringan sistem komunikasi merupakan salah satu persyaratan utama dari keamanan sistem informasi.
3. Memastikan agar jaringan sistem komunikasi memiliki perlindungan yang memadai sehingga tidak dapat disusupi oleh pihak lain.
4. Memastikan agar karyawan yang memiliki wewenang untuk menggunakan jaringan ini sesuai dengan kebutuhan organisasi. Jalur yang tidak ada hubungan dengan kegitatan yang digeluti oleh perusahaan harus dinonaktifkan.
5. Memastikan software yang digunakan untuk menunjang jaringan komunikasi sesuai dengan kebutuhan sistem dan organisasi serta memiliki lisensi.

Spesialis PABX

Spesialis PABX adalah staf yang meiliki keahlian megenai sistem telepon dan memiliki tanggung jawab untuk memilih PABX sesuai dengan kebutuhan perusahaan dan memeliharanya.

Tanggung Jawab. Spesialis PABX harus:

1. Memastikan bahwa PABX yang akan digunakan sesuai dengan kebutuhan organisasi dan telah dikonsultasikan dengan manajemen.
2. Memastikan agar sistem PABX selalu tersedia.
3. Memastikan agar karyawan dapat menggunakan sistem telepon sesuai dengan kewenangnya yang telah ditetapkan oleh manager bagian terkait.
4. Memastikan informasi pemakaian telepon terekam di log file sehingga mudah untuk penangihan biaya antar departemen.
5. Apabila organisasi menggunakan sistem perekaman percakapan, maka ia harus memastikan semua percakapan unit kerja tertentu dengan pelanggan

terekam dengan baik yang dapat digunakan sebagai alat bukti apabila terjadi perselisihan.

6. Menyimpan media yang berisikan rekaman percakapan

Organisasi Data Processing

Tanggung jawab.

Organisasi *Data Processing* harus:

1. Menjaga dan melaksanakan pemrosesan sistem sesuai dengan syarat yang diberikan oleh pemilik sistem untuk penggunaan, pemonitoran, dan keamanan. Ia harus dapat mengambil langkah yang diperlukan untuk memastikan agar penggantian dan perubahan terhadap sistem dilaksanakan sesuai dengan peraturan yang berlaku.
2. Memindahkan sistem ke *production environment* setelah disetujui oleh pemilik sistem.
3. Memastikan agar wewenang yang diberikan kepada pemakai dapat dimonitor dengan baik.
4. Mencatat semua percobaan atau penggunaan sistem secara tidak wajar dan melaporkan kepada pemakainya, auditor, dan pemilik sistem.
5. *Log off* apabila ia meninggalkan *server console*.

Auditor

Auditor TI adalah staf yang memiliki keahlian untuk menilai dan memberikan rekomendasi secara objektif mengenai kontrol, keamanan, dan pengoperasian sistem.

Tanggung jawab. Auditor harus:

1. Memberikan penilaian dan rekomendasi control dan langkah pengamanan yang menyangkut pengembangan sistem, manajemen, proses, dan pendayagunaan sistem komputer.
2. Melaporkan penemuannya kepada yang bersangkutan dan manajemen.
3. Melakukan audit terhadap sistem (pengamanan dan kontrol) paling sedikit satu kali per tahun, tergantung ruang lingkup dan besar dari perusahaan.
4. Memastikan agar semua kontrak berkaitan dengan sistem informasi harus sudah disetujui oleh unit kerja hukum.

Administrator Sistem Keamanan

Administrator Sistem Keamanan adalah staf yang memiliki keahlian untuk mengimplementasi dan memelihara keamanan terhadap sistem informasi yang telah dirumuskan bersama pemilik sistem dan kepala unit kerja terkait.

Tanggung Jawab:

1. Merumuskan struktur keamanan sistem informasi dan mengkomunikasikan kepada organisasi.
2. Mengimplementasi dan me-*maintain* struktur keamanan sistem informasi (*system information security structur*).
3. Melakukan administrasi dan memberikan otorisasi pengaksesan sistem kepada pemakai yang telah disetujui oleh pemilik sistem dan kepala bagian terkait.
4. Memastikan agar hanya *software* yang berlisesnsi yang diperbolehkan untuk dipasang di komputer perusahaan. Ia harus mengetahui dan sadar konsekuensinya untuk perusahaan apabila software ilegal digunakan.
5. Menyimpan dengan baik password Administrator di dalam amplop yang tertutup dan menyerahkan kepada senior manager yang telah ditunjuk. Amplop ini hanya boleh dibuka pada saat darurat oleh orang lain yang diberi wewenang oleh manjemen. Apabila password telah digunakan oleh pihak ketiga, Administrator harus mengganti passwordnya dan menyimpan kembali di amplop.

Personel Administrasi

Yang dimaksud dengan Personel Administrasi adalah staf yang bertanggung jawab untuk urusan administrasi berkaitan dengan sistem informasi.

1. Akses control terkait dengan pengaksesan ke dalam system informasi harus berdasarkan kebutuhan fungsi, contohnya adalah hanya personil bagian terkait yang berhak untuk mengakses program aplikasi penggajian.
2. Hanya karyawan perusahaan yang diperbolehkan untuk diproses di system informasi perusahaan.
3. Apabila ada pekerjaan yang dilakukan oleh pihak ketiga maka perusahaan harus dilindungi oleh keamanan atas informasi perusahaan.
   Di dalam kontrak pekerjaan harus di defenisikan agar
   pihak III mematuhi peratuhan dan keamanan system informasi perusahaan.
4. Untuk menjaga kestabilan system informasi di lingkungan perusahaan, agar diadakan pemisahan secara fungsional antara pengembang system, pengoperasian system harian dan pemakai akhir
5. Implementasi system baru atau permintaan perubahan terhadap system yang sudah ada harus melalui pengontrolan yang ketat .
6. Setiap pemakai bertanggung jawab penuh atas semua aktifitas yang dilakukan dengan memakai kode identitasnya (*User*-ID)
7. Pemakai adalah semua karyawan perusahaan yang memakai system informasi, setiap pemakai harus :
   - Menggunakan system informasi sesuai dengan tanggung jawabnya untuk melaksanakan tugasnya

- Bertanggung jawab atas semua aktifitas yang dilakukan di dalam system dengan menggunakan *User*-ID/account nya
- Melaporkan kepada atasan apabila terjadi kejanggalan pada saat pengoperasian system.
- Mengembalikan seluruh hak milik perusahaan yang berkaitan dengan data perusahaan.
- Menyadari bahwa komputer milik perusahaan hanya boleh digunakan untuk keperluan perusahaan atau yang berkaitan dengan pekerjaannya dan bukun untuk kepentingan pribadi.
- Sign off atau logout dari system apabila akan meninggalkan tempat kerja dalam waktu lama dan mematikan komputer jika akan pulang.

8. Setiap pengembang aplikasi baik yang dilakukan pihak internal perusahaan atau pihak III harus memenuhi :
    - Memastikan bahwa system yang akan dibangun telah ditentukan dan dipilih oleh pemilik aplikasi berdasarkan kepekaan risiko system informasi.
    - Menspesifikasikan kebutuhan atas penggunaan, pemonitoran dan keamanan system informasi dengan cara berkonsultasi dengan pemilik system dan pihak lain yang terkait dengan fungsinya. Pembuat aplikasi harus merumuskan dan menyusun system keamanan yang dibutuhkan.
    - Mengijinkan pemilik system, auditor dan pihak fungsional lain yang terkait dengan tim pengembangan untuk mengevaluasi hasil sementara atau akhir pengembangan.
    - Memastikan agar system secara otomatis *sign off* atau *logout* apabila pemakai meninggalkan tempatnya lebih lama daripada waktu yang telah ditentukan
    - Berjanji untuk tidak mengungkapkan data perusahaan yang sensitif kepada pihak lain apabila ia telah mendapat wewenangnya. Data ini bisa di dapat atas seijin perusahaan untuk melakukan pengujian data.
    - Sistem yang akan dikembangkan tidak akan diperjualbelikan di luar perusahaan.
    - Tidak melakukan *bypass* aturan koneksi jaringan yang telah ditetapkan.
    - Mengembalikan kembali *account* yang memiliki hak sebagai administrator.
    - Aplikasi yang dibangun harus memiliki keamanan yang tinggi dan memiliki level akses dan *logfile*
9. Setiap karyawan yang telah memiliki*username* dan password untuk mengakses aplikasi harus menyimpan kerahasiaan informasi passwordnya masing-masing dan dilarang memberikan accountnya tersebut kepada orang lain (*sharing password*). Setelah menerima password langsung mengganti dan secara teratur.

10. Secara berkala password harus diganti untuk menghindari penggunaan password dari orang-orang yang tidak berhak
11. Sistem informasi yang dibangun pihak III datanya tidak boleh disebarluaskan.
12. Password yang dibuat haruslah password yang tidak mudah di tebak dan aman, dalam membuat dan menggunakan password yang baik dapat memperhatikan aspek berikut
    - Membuat password yang tidak berhubungan dengan diri sendiri seperti memuat : tanggal lahir, nama anda, nama keluarga anda dan lain sebagainya. Panjang password minimal adalah 6 karakter
    - Memiliki kombinasi huruf dan angka
    - Memuat karakter di luar huruf dan angka
    - Tidak menulis password di secarik kertas
    - Jika menggunakan akses public dalam mengakses system informasi perusahaan misalnya dari warung internet, hotel dan lain sebagainya, mematikan fungsi *cache* pada *browser* sehingga password yang kita isikan tidak tersimpan pada *cachelocal* komputer tersebut.
13. Server di tempatkan di ruangan khusus yang memiliki system keamanan yang baik. Sembarang orang tidak bisa masuk selain petugas atau administrator server yang ditunjuk.
14. Monitoring kinerja keamanan dilakukan secara berkala oleh pengelola TI, dievaluasi dan dilakukan tindakan korektif jika terjadi gangguan keamanan kepada sistem TI perusahaan untuk mengetahui kelemahan keamanan atau kejadian lainnya.
15. Setiap PC atau laptop harus terpasang minimal 1 *software anti virus* dan pengguna melakukan update antivirus secara berkala.
16. Kemanan fisik dan lingkungan terkait dengan :
    - Ruang server harus mempunyai pintu dengan keamanan akses yang memadai dan dilengkapi dengan CCTV serta alat pemadam kebakaran, ruang server adalah ruangan yang aksesnya sangat terbatas karena tidak semua orang bisa masuk ke ruangan server tersebut, hanya pengelola ruangan server seperti Administrator , personil TI dan orang-orang yang diberi ijin oleh pengelola ruangan server.
    - Komputer dan laptop pengguna harus tersimpan di ruangan yang mempunyai keamanan yang baik.
17. Kriptografi adalah suatu ilmu sekaligus seni untuk menjaga kerahasiaan pesan atau secara singkat berarti cara menjaga privasi saat berkomunikasi. Untuk tujuan tersebut dilakukan enkripsi dan dekripsi terhadap pesan atau dokumen penting yang sifatnya rahasia. Enkripsi merupakan proses mengubah data menjadi bentuk yang sulit/tidak dapat dimengerti. Sedangkan dekripsimerupakan proses pengembalian data yang telah dienkripsi menjadi

bentuk yang sebenarnya dan dapat dimengerti kembali. Penerapan kriptografi di terapkan dalam pembangunan sistem informasi khusus terkait username / password pengguna tersimpan dalam database dalam bentuk data yang sudah terenkripsi.

XII. Kebijakan Audit Sistem Informasi dan Teknologi Informasi

1. Tujuan dari Kebijakan Audit Sistem Informasi dan Teknologi Informasi dapat dikelompokkan ke dalam dua aspek, yaitu
    - *Conformance* (kesesuaian) ,pada kelompok tujuan audit system informasi difokuskan untuk memperoleh kesimpulan atas aspek kesesuaian, yaitu : *confidentiality* (kerahasiaan), *integrity* (integritas), *Availability* (Ketersediaan) dan *Compliance* (Kepatuhan)
    - *Performance* (Kinerja),pada kelompok tujuan ini audit system informasi difokuskan untuk menarik kesimpulan atas aspek kinerja, yaitu : *Effectiveness* (Efektifitas), *Eficiency* (Efisiensi) dan *Reliability* (Kehandalan).
2. Yang melakukan audit system informasi dan teknologi informasi adalah pihak Auditor Internal Perusahaan ataupun Auditor Eksternal yang mempunyai kompetensi dan pengalaman di Bidang Audit Sistem dan Teknologi Informasi.
3. Auditor harus menggunakan kerangka kerja yang berlaku umum atau *best practices* seperti COBIT, ITIL , ISO 17799 dan lain sebagainya.
4. Hasil yang diharapkan dari kegiatan audit system informasi adalah :
    - Dokumentasi obyektif, perencanaan, prosedur dan laporan audit
    - *Review* secara bekala untuk memeriksa peningkatan kemampuan system.

XIII. Kebijakan Keterbukaan Informasi melalui Media TI dan Pengelolaan website Perusahaan

1. Untuk keterbukaan informasi kepada publik maupun *stakeholders* perusahaan mempunyai media TI berupa website resmi perusahaan yang dapat diakses melalui alamat www.ptpn5.com. Selain website resmi tersebut informasi perusahaan dapat juga diakses secara melalui portal Lembaga Pendidikan Perkebunan (LPP) dan Portal
2. Pengelola atau administrator website resmi perusahaan adalah personil unit TI sedangkan yang meng-*update content* website tersebut adalah personil Bagian Sekretaris Perusahaan.
3. Petugas dan pengelola content website yang telah di tunjuk perusahaan harus secara aktif dan rutin mengupdate informasi perusahaan baik di website resmi perusahaan, di portal LPP dan portal .
4. Setiap insan perusahaan , publik dan *stakeholders* dapat menyampaikan informasi kepada perusahaan melalui Media TI yaitu ke e-mail resmi perusahaan

yaitu: corporatebcs@balairung-hotel.co.id atau melalui website resmi perusahaan.

XIV. Kebijakan Pencadangan Data (Backup Data)

1. *Backup* adalah proses membuat data cadangan dengan cara menyalin atau membuat arsip data komputer sehingga data tersebut dapat digunakan kembali apabila terjadi kerusakan atau kehilangan. *Backup* memiliki dua tujuan. Tujuan utama adalah untuk mengembalikan data apabila data tersebut hilang, baik karena terhapus atau karena rusak *(corrupt)*. Tujuan kedua adalah untuk mengembalikan data ke titik tertentu pada masa lalu. Karena fungsinya, proses backup mengharuskan pengguna menggandakan data
2. Data yang dibackup merupakan data-data elektronis yang mendukung dan relevan dengan pekerjaan.
3. Setiap karyawan wajib melakukan kegiatan backup data secara berkala minimal setiap hari atau setiap terjadinya perubahan data.
4. Data yang dibackup tersebut di simpan di media penyimpanan internal seperti Hardisk pada komputer/laptop juga di simpan pada media eksternal komputer/laptop seprti pada hardisk eksternal, usb flash drive, CD/DVD atau di media eksternal lainnya.
5. Selain dibackup seperti yang tersebut pada poin sebelumnya data-data tersebut dibackup melalui menu Backup File pada Web Intranet atau melalui aplikasi online lainnya seperti dropbox, drive google, e-mail dan lain sebagainya.
6. Khusus untuk data-data yang tersimpan pada database server ataupun database aplikasi lainnya personil yang ditunjuk sebagai administrator wajib membackup secara rutin data-data pada database tersebut baik secara manual maupun otomatis.

XV. Kebijakan Penggunaan Media Sosial

1. Media sosial adalah sebuah media daring (online), dengan para penggunanya bisa dengan mudah berpartisipasi, berbagi, dan menciptakan isi meliputi blog, jejaring sosial, wiki, forum dan dunia virtual. Blog, jejaring sosial dan wiki merupakan bentuk media sosial yang paling umum digunakan oleh masyarakat di seluruh dunia.
2. Media sosial resmi perusahaan di kelola oleh Bagian Sekretaris Perusahaan u.p Hubungan Masyarakat.
3. Setiap karyawan yang mempunyai Blog pribadi, situs web dan profil media sosial mencantumkan pernyataan sangkalan dengan jelas bahwa pandangan yang dikemukakan oleh penulis adalah pandangan pribadi penulis dan tidak mewakili pandangan Perusahaan.
4. Setiap karyawan secara bijak menggunakan identitas perusahaan seperti logo ,

foto kantor dan lain-lain pada Blog pribadi, situs web dan profil media sosial dan tidak menyampaikan serta tidak berbagi ujaran kebencian dan segala bentuk materi yang mengandung unsur SARA dan pornografi.

5. Setiap karyawan dalam bermedia sosial harus mentaati kode etik Perusahaan (*Code of Conduct*) dan peraturan hukum yang berlaku.
6. Dalam bermedia sosial setiap karyawan wajib menjaga etika berkomunikasi seperti : tidak menyampaikan dan tidak membagi konten yang memiliki unsur Hoax, SARA dan Pornografi , tidak menyampaikan dan tidak berbagi ujaran kebencian dan segala hal yang bertentangan dengan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan yang berlaku lainnya.