BAB III

PEMBAHASAN

3.1. Aspek Kegiatan Perusahaan

PT.PLN (Persero) merupakan unsur pelaksana dari bagian tugas pokok dan fungsi departemen pertambangan dan energi. Adapun tugas dan fungsi PT.PLN (Persero) adalah sebagai berikut:

1. Tugas pokok PT. PLN (Persero)

Tugas pokok PT. PLN (Persero) adalah melaksanakan sebagaian tugas dan fungsi departemen pertambangan dan energi yang meliputi pembangkitan, transmisi, pendistribusian, serta pengusahaan tenaga listrik sesuai dengan kebijaksanaan yang ditetapkan oleh menteri serta berdasarkan peraturan perundang-undangan yang berlaku.

2. Tugas dari PT. PLN (Persero)

PT.PLN (Persero) mempunyai beberapa fungsi dalam melaksanakan tugasnya yaitu :

a. Perumusan kebijaksanaan teknis, pemberian pembimbingan dan pembinaan sesuai dengan kebijaksanaan yang telah ditetapkan menteri berdasarkan peraturan perundang-undangan yang berlaku, meliputi:
    1. Penyediaan tenaga listrik meliputi pembangunan sarana kelistrikan, pembangkitan transmisi serta distribusi.
    2. Pengusahaan tenaga listrik.

3. Pemanfaatan dan pengembangan tenaga listrik.
4. Pendidikan dan pengembangan tenaga listrik.

b. Pelaksanaannya sesuai dengan tugas dan berdasarkan peraturan perundang-undangan yang berlaku.

Usaha-usaha ketenaga listrikan yang dilakukan oleh PT.PLN (Persero) dalam mencapai tujuannya meliputi usaha bidang:

1. Produksi, transmisi dan distribusi tenaga listrik.
2 Perencanaan dan pembangunan tenaga listrik.
3 Pengusahaan jasa-jasa dibidang tenaga listrik.

Adapun kegiatan usaha yang dilaksanakan yang berhubungan dengan penyediaan tenaga listrik antara lain sebagai berikut:

a. Pembangunan Jaringan

Merupakan pembangunan hantaran udara yang meliputi :

1 Tenaga Rendah (TR)
2 Tegangan Menengah (TM)
3 Tegangan dibawah tanah (kabel TR dan TM)

b. Pembangunan gardu-gardu distribusi.

Merupakan pembangunan gardu yang didistrribusikan KWH atau menyalurkan tenaga atau aliran listrik kepada langganan melalui jaringan tegangan rendah (TR) termasuk perlengkapan KWH.

c. Pembangunan Tiang.

Meliputi tiang tegangan rendah dan tegangan menengah.

d. Pemeliharaan gardu, jaringan, sambungan rumah dan pemeliharaan gedung yang secara khusus meliputi :

   1. Pemeliharaan gangguan gardu tembok
   2. Pemeliharaan gangguan gardu tiang
   3. Pemeliharaan gardu kios.
   4. pemeliharaan ganguan saluran udara tegangan menengah
   5. Pemeliharaan gangguan saluran udara tegangan rendah dan penerangan jalan umum (PJU).
   6. Pemeliharaan gangguan sambungan rumah.

e. Penyambungan baru.

   Berarti mengadakan kegiatan pemasangan atau penyambungan listrrik rumah-rumah konsumen baru.

f. Tambah daya.

   Merupakan perubahan beban daya baik penambahan atau penurunan daya.

g. Perubahan tarif.

   Merupakan perubahan jenis tarif dari pelanggan umum kelompok lainnya atau sebaliknya, misalnya dari rumah tinggal ke tarif industri atau usaha.

h. Pelayanan Kepada Pelanggan.

   1 Pelayanan kepada pelanggan
   2 Permintaan sambungan baru dan perubahan daya
   3 Pergantian ganti nama dan tariff
   4 Permintaan penerangan sementara

5 Permiantaan perbaikan atau pembongkaran sambungan rumah

i. Pembacaan meter.

j. Melakukan pencatatan standar meter atas pemakaian tenaga listrik.

k. Pembuatan rekening atas pemakaian tenaga listrrik.

l. Penerimaan pelunasan atau pembayaran rekening listrik.

m. Pengawasan tunggakan rekening listrik dan lanjut

3.2. Kegiatan dalam kerja praktek dan hasil kerja praktek

Pada bab ini penulis menguraikan dan membahas tentang cara kerja computer dan tentang penelitian system cara penanganan computer pada PT.PLN (Persero) Unit Distribusi Jawa barat dan Banten.

3.2.1. Pengamanan Data masukan/input

Data merupakan aset perusahaan yang sangat penting dan bernilai tinggi, karenanya harus dijaga keamanannya, sehingga bahaya yang dapat terjadi pada data dapat diperkecil atau dihilangkan.

3.2.1.1. Hal-hal yang dapat membahayakan data :

- Hilang, sebagian atau seluruh data hilang.
- Rusak, kerusakan data dapat terjadi karena kesalahan operasi, salah penanganan atau kegagalan hardware.
- Interferensi, pencurian, perubahan atau copy oleh orang yang tidak berwenang atau penyalahgunaan data.

3.2.1.2.Usaha-usaha pengamanan yang harus dilakukan

a. Masukan / Input

1.Umum

Dalam hal ini meliputu:

- Data mentah : biasanya dalam bentuk source-document.
- Data yang sudah siap untuk dimasukan ke dalam komputer :
    1. biasanya dalam bentuk media magnetik (tape, disket, CD) atau langsung dari peralatan on-line (terminal, PC).
    2. Resiko hilang, rusak atau interferensi data dapat diperkecil dengan menerapkan prosedur dan supervisi yang baik.
    3. Semua pekerjaan harus dilakukan sesuai wewenang dan tanggung jawab yang didefinisikan dengan jelas.

2.Terminal

- Hal-hal yang boleh dilakukan pada terminal harus didefinisikan dengan jelas.
- Terminal ID, dapat digunakan untuk :
    a. Mengidentifikasi tingkat data yang dapat diakses melalui terminal tertentu.
    b. Mencegah penggunaan terminal-terminal tertentu diluar jam kerja.

- User-ID

1. Setiap *user–id* diberikan tingkat hak akses sesuai dengan tanggung jawab user yang bersangkutan, misalnya tingkat hak akses seorang operator berbeda dengan hak akses seorang pemogram.
2. Permintaan *user-id* baru dan perubahan otorisasi harus mendapat persetujuan atasan yang berwenang.

- Password

1. *Password* dapat diganti /diubah oleh user/pengguna.
2. Harus diganti minimum 1 (satu) bulan sekali.
3. *Password* yang efektif adalah kombinasi dari minimum 6 (enam) charakter yang mempunyai arti tertentu bagi penggunanya.
4. Dapat dipergunakan lebih dari 1 (satu) tingkat password; misalnya satu password untuk *sign-on* dan yang lainnya untuk akses file data dengan tingkat pengamanan tertentu.
5. Password yang diberikan pertama kali oleh sistem, harus segera diganti.
6. Sistem akan mengunci user-id setelah beberapa kali, biasanya oleh administrator dibuat sebanyak 3 (tiga) kali memasukan *password* yang salah ; sistem juga akan mencatat waktu, *user-id* terminal pada saat kejadian untuk keperluan penyelidikan.

- Semua personil yang sudah keluar harus dihapus *ID, password* dan otoritasinya.

- Apabila melakukan pengiriman data yang bersifat rahasia, harus digunakan teknik enkripsi atau teknik laninnya sesuai kemajuan teknologi.
- Teminal yang tidak aktif selama waktu tertentu harus diputuskan dari sistem sampai password dimasukan kembali.
- Terminal harus dikunci bila tidak dipergunakan (untuk terminal yang dilengkapi dengan kunci pengaman).

3.2.1.3. Kerahasiaan

Data, terutama yang bersifat *Confidential*, harus dilindungi dari *interferensi* dengan memastikan bahwa hanya orang yang diberi otoritas khusus yang dapat melakukan akses pada data tersebut dan selalu tersimpan dengan baik pada saat tidak dipergunakan.

Tindakan pengamanan harus termasuk :

- Membatasi penanganannya hanya pada staf yang dapat dipercaya.
- Menggunakan kode sebagai pengganti nama untuk mempersulit identifikasi.
- Data rahasia yang tidak diperlukan lagi harus segera dimusnahkan sesuai prosedur yang ada.

Menyimpan data yang penting didalam lemari besi.

3.2.2. Proses Komputer

3.2.2.1. Umum

Sedapat mungkin proses produksi dilakukan sesuai jadwal yang ditentukan. Penyimpanan dari jadwal harus dipertimbangkan dengan hati-hati, terutama mengingat adanya ketergantungan proses yang satu dengan proses lainnya dan adanya batas waktu penyelesaian yang sudah ditentukan.

3.2.2.2. Perangkat keras/Hardware

Pemeliharaan hardware harus dilakukan dengan baik dan dalam periode tertentu yang berkesinambungan, sehingga kerusakan data karena kegagalan hardware dapat dihindari atau dikurangi.

3.2.2.2. Penanganan Media

Data dapat hilang atau rusak karena penanganan yang salah pada media. Kerugian minimum karena hal ini adalah membuat kembali data tersebut; kerugian yang lebih parah dapat terjadi karena terganggunya seluruh operasi perusahaan.

Prosedur tentang cara penanganan media harus mengkombinasikan rekomendasi dari pabrik pembuatnya dengan kebutuhan operasional setempat.

Prosedur ini antara lain mencakup :

- Selalu menjaga kebersihan media.
- Menghindari media dari sinar matahari langsung.
- Menghindari media dari kelembaban, medan magnet dan temperatur tinggi.
- Selalu memasang kembali cover pada saat media tidak dipakai.
- Media harus diberi label yang lengkap dan jelas untuk menghindari tertukarnya data.
- Tidak merokok, makan atau minum pada saat menangani media.
- Media harus segera dikembalikan ke tempat penyimpanan bila sudah selesai digunakan.

3.2.2.3. Kecurangan

Tindakan pencegahan harus dilakukan untuk menghindari pemakaian fasilitas untuk melakukan hal-hal sebagi berikut :

- Manipulasi data
- Menjalankan pekerjaan diluar wewenang
- Membuat copy file tanpa wewenang

Tindakan pencegahan ini mencakup :

- Membuat copy dari master, program dan file-file back-up dan menyimpannya ditempat yang aman, terpisah dari instalasi dari komputer. Akses terhadap copy ini harus dikontrol secara ketat.

- Melakukan pengawasan terhadap stationery untuk memastikan jumlah yang tepat yang telah digunakan dan jumlah copy yang dibuat. Hal ini menjadi sangat penting, misalnya dalam hal pemakaian bill-form.
- Hasil output penting yang tidak digunakan harus dihancurkan sebelum dibuang.
- Mengkaji/meneliti system log untuk memastikan bahwa hanya pekerjaan resmi yang dilakukan dan pada waktu yang tepat. Setiap penyimpanan dari kebiasaan harus diteliti.

Melakukan supervisi dengan baik dan memastikan bahwa paling sedikit ada 2 (dua) orang diruang komputer pada satu saat, susunan tim harus ditukar dari waktu ke waktu untuk menghindari kolusi.

3.2.3. Keluaran / Output

Dalam hal ini, yang dimaksudkan dengan keluaran / Output adalah hasil pengolahan komputer yang berupa cetakan / kertas.

3.2.3.1. Umum

Resiko kehilangan, kerusakan dan interferensi dapat diperkecil dengan membatasi akses kepada personil yang berwenang, melakukan supervisi yang baik dan pelatihan.

3.2.3.2. Pengolahan output

Pelatihan harus diberikan pada penggunaan peralatan pengolahan output, yaitu decollator (pemisah kertas) dan detacher (pemotong kertas), karena seringkali terjadi kerusakan output pada pekerjaan ini.

Peralatan ini perlu dipelihara dengan baik untuk menjamin mutu hasil kerjanya.

3.2.3.3. Serah terima output

- Serah terima output dicatat dengan jelas, disertai bukti serah terima yang ditandatangani.
- Output yang menunggu pengambilan tidak boleh dibiarkan tanpa dijaga.
- Output yang bersifat rahasia harus diberikan hanya kepada personil yang berwenang, dan dikemas sedemikian rupa untuk menghindari pembacaan oleh orang yang tidak berwenang.
- Output harus ditandai dengan jelas untuk menjaga kesalahan penyerahan.
- Output dari sistem on-line hanya boleh disimpan di komputer/server milik PLN (dalam hal kerjasama dengan pihak lain, misalnya Bank) dan dibuat aturan-aturan dalam dalam pelaksanaannya (misal : download, dsb)

3.3. Pengamanan Sistem (System Security)

Yang dimaksud dengan Sistem disini adalah Perangkat Lunak Sistem / System Software (operating system, dan sofware penunjangnya) dan program-program aplikasi.

Langkah-langkah pengamanan, dimaksudkan pada tahap sistem desain oleh sistem analis dan pembuat program / programmer. Harus diyakini bahwa pengaman yang dimasudkan sudah cukup memadai sebelum sistem layak untuk dioperasikan.

3.3.1. Perencanaan Pengamanan.

Sebuah sistem harus :

- Sudah diuji coba bahwa sistem berfungsi sesuai spesifikasinya.
- Sudah diperiksa dengan teliti untuk memastikan bahwa hanya input yang benar akan diterima dan output yang benar akan dihasilkan.
- Dimonitor kinerjanya untuk meyakinkan bahwa sistem tetap berfungsi secara efisien.

Langkah-langkah Pengamanan harus :

- Sederhana
- Langkah-langkah pengamanan yang kompleks sering menyebabkan kesalahpahaman dan meningkatkan resiko terjadinya kesalahan.
- Terpadu ; dimaksudkan sebagai bagian dari sistem.
- Didokumentasikan dengan baik ; menyediakan audit trail dan sarana pemeriksaan.

- Memungkinkan kesalahan ditemukan sedini mungkin.
- Memberi kemudahan untuk melakukan koreksi dalam kondisi terkontrol.
- Tidak berlebihan, sehingga tidak memperlambat produksi.
- Informatif; tidak hanya mendektesi bahwa ada sesuatu yang salah, tetapi juga memberi tahu apa yang salah dan bagaimana memperbaikinya.

3.3.2. Langkah-langkah pengamanan umum

Langkah-langkah pengamanan yang relavan terhadap pengamanan data, relevan juga terhadap pengamanan sistem termasuk sistem software/perangkat lunak dan sistem jaringan (LAN/WAN/Internet).

3.3.3. Pengamanan sistem software

a. penggunaan versi yang tepat

- Prosedur-prosedur harus disusun untuk memastikan bahwa versi system software yang dipergunakan.
- Perubahan yang dilakukan terhadap sistem software harus diberitahukan dan disadari oleh staf yang berkaitan dengan system software.
- Rencana Implementasi harus mencakup rencana contigency yang mengatur langkah-langkah yang harus dilakukan dalam hal terjadi kesalahan.

- Versi sistem software yang obsolete harus dikeluarkan dari sistem ; tetapi back-upnya tetap disimpan untuk keperluan contingency.
- Back-up dari seluruh sistem software harus selalu tersedia dan copynya disimpan di lokasi yang terpisah dari instalasi komputer utama.

a. Kerusakan sistem sofware yang tidak sengaja

- Prosedur-prosedur harus memastikan bahwa sistem sofware tidak rusak karena kesalahan sistem atau operator.
- resiko ini dapat dikuranggi dengan:
  1. memperketat uji coba sebelum sistem software dapat diterima dan dioperasikan
  2. melakukan pelatihan yang seksama
  3. melakuakan back updan membuat dokumentasi

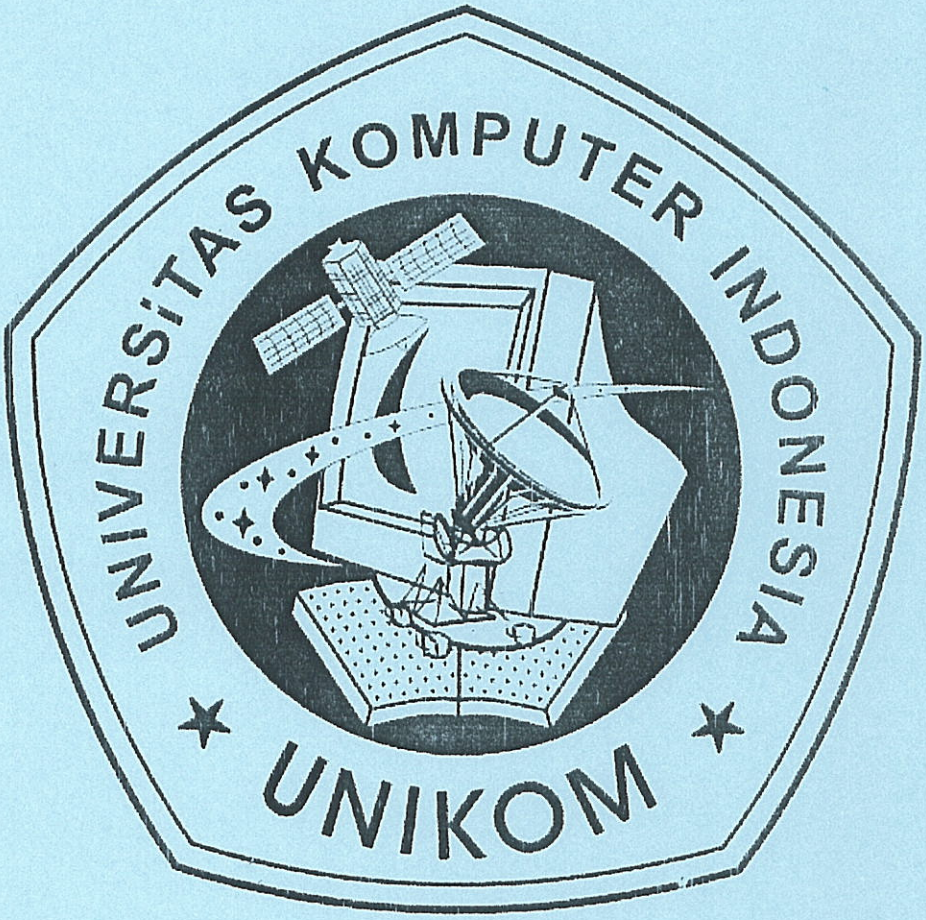
b. Perubahan terhadap sistem software.

Perubahan terhadap sistem software hanya dapat dilakukan setelah disetujui dan ditanda tangani oleh orang yang berwenang.

3.3.4. Pemeliharaan program-program aplikasi.

- Perubahan-perubahan terhadap program aplikasi yang opersional dilakukan sesuai prosedur yang ada yang menunjukan tingkat kewenangan yang diperlukan.

- Versi baru dari program aplikasi tidak dapat dioperasikan sebelum ada persetujuan dari orang yang mempunyai wewenang.
- Semua perubahan harus didokumentasikan dengan baik.
- Perbaikan harus dilakukan terhadap copy program, bukan terhadap program aslinya. Semua program aplikasi harus di back-up dan disimpan dengan baik.


UNIVERSITAS KOMPUTER INDONESIA
UNIKOM