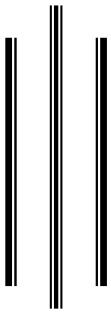
TUGAS MATA KULIAH
PROTEKSI DAN TEKNIK KEAMANAN SISTEM INFORMASI
STUDI KASUS: PT. KONTRAKTOR SIPIL JAYA



DISUSUN OLEH:

ANTO DWIHARJA(7203010014)
DARMAWAN (720301009X)
SIGIT SUPRIYADI (7203010375)

PROGRAM MAGISTER TEKNOLOGI INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS INDONESIA
2004

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Pengantar

Keamanan komputer merupakan salah satu bagian penting dalam pengembangan sistem, karena informasi merupakan aset yang sangat penting bagi setiap institusi ataupun perusahaan. Begitu pentingya informasi sehingga informasi kadang hanya diperuntukkan bagi orang-orang tertentu. Oleh karena itu, keamanan sistem informasi harus terjamin dalam batas-batas yang dapat diterima. Sayangnya, keamanan informasi oleh banyak perusahaan masih dianggap sebagai masalah teknis yang cukup ditangani oleh bagian teknologi informasi (TI) saja, sehingga menghasilkan solusi teknologi tanpa melibatkan proses bisnis. Artinya, perangkat lunak dengan sistem keamanan tercanggih pun sering kali belum mencukupi. Tentunya suatu perusahaan belum tentu membutuhkan atau mampu menerapkan semua cara pengamanan sistem. Sia-sia apabila kita menerapkan sistem TI dengan teknologi pengamanan mutakhir dan biaya sangat mahal kalau ternyata kebutuhan kita tidak serumit itu dan fungsinya pun tidak optimum. Sebaliknya, tidak ada gunanya membeli sistem murah namun tidak dapat memberikan tingkat keamanan sistem yang diharapkan.

1.2 Tujuan Penulisan Makalah

Makalah ini bertujuan untuk membahas kesebelas domain dalam keamanan sistem informasi pada sebuah perusahaan jasa konstruksi yang berdomisili di Jakarta yaitu PT. Kontraktor Sipil Jaya. Kesebelas domain keamanan tersebut adalah: praktek manajemen keamanan, metodologi dan sistem kontrol akses, arsitektur dan model keamanan, keamanan fisik, keamanan jaringan dan telekomunikasi, kriptografi, pemulihan bencana dan kelangsungan bisnis, hukum-investigasi-dan etika, pengembangan sistem dan aplikasi,

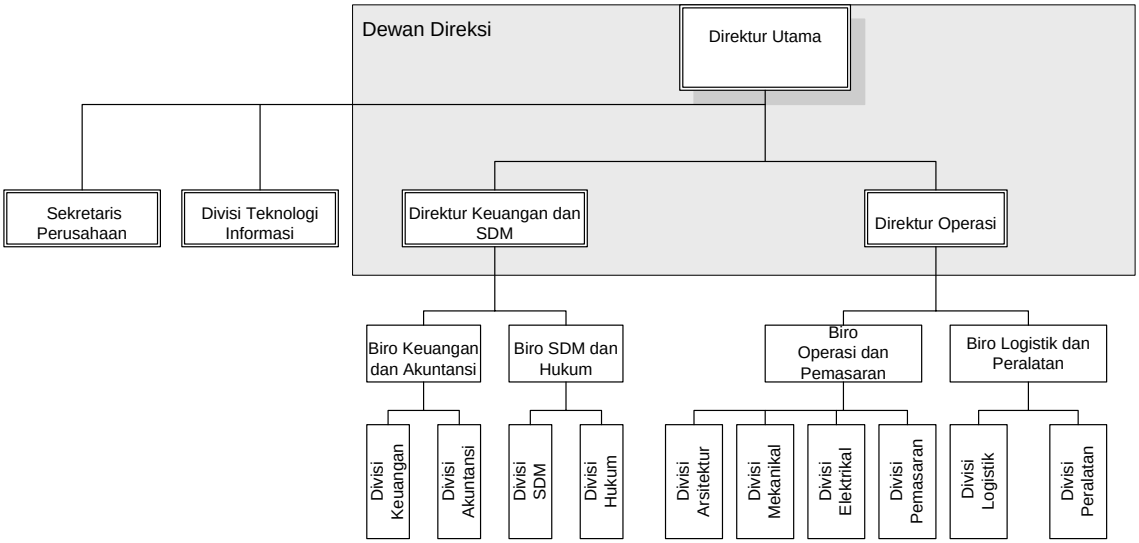
keamanan operasi, dan audit dan jaminan.

1.3 Profil Perusahaan

PT. Kontraktor Sipil Jaya merupakan sebuah perusahaan jasa konstruksi yang berdiri pada tahun 1994 dan berlokasi di Jakarta. Wilayah kerja perusahaan sampai saat ini sudah mencakup wilayah Jabotabek, namun perusahaan belum merasa perlu memiliki kantor perwakilan.

Pada mulanya perusahaan ini merupakan badan usaha berbentuk CV dengan modal disetor Rp. 10.000.0000,-. Seiring dengan perkembangan usaha, maka pada tahun 2000 perusahaan merubah bentuk badan usahanya menjadi PT., sehingga namanya menjadi PT. Kontraktor Sipil Jaya. Pada saat yang sama, manajemen yang baru terbentuk melakukan suntikan modal sebesar Rp. 100.000.000,- (seratus ratus juta rupiah). PT. Kontraktor Sipil Jaya merupakan perusahaan jasa konstruksi dengan kualifikasi M2, yaitu perusahaan yang mampu melaksanakan pekerjaan 1 milyar sampai dengan 3 milyar. Perusahaan ini menangani berbagai proyek konstruksi bangunan dari berbagai skala dan tipe, seperti rumah tinggal, rumah toko, kantor, sekolah, tempat ibadah, gedung olahraga, gedung pameran, tempat perbelanjaan, maupun villa; pekerjaan mekanikal seperti instalasi tata udara dan tata suara, konstruksi lift dan elevator; dan pekerjaan elektrikal seperti instalasi listrik, dan penangkal petir. Saat ini, PT. Kontraktor Sipil Jaya telah menghasilkan kenaikan keuntungan setiap tahunnya. Hal ini membuat PT. Kontraktor Sipil Jaya mampu menambah investasi berbagai peralatan dan meningkatkan secara dramatis kualitas dari sumber daya manusia. Konsumen PT. Kontraktor Sipil Jaya adalah seluruh lapisan masyarakat baik individu maupun perusahaan yang membutuhkan jasa konstruksi. PT. Kontraktor Sipil Jaya dalam kegiatan usahanya juga berhubungan dengan perusahaan yang menyewakan mesin-mesin atau alat-alat berat dan toko-toko yang menjual bahan-bahan bangunan.

Struktur organisasi PT. Kontraktor Sipil Jaya diperlihatkan pada Gambar 1.1. Sedangkan rincian lebih lengkap mengenai personil perusahaan diperlihatkan pada Tabel 1.1. Jam kerja PT. Kontraktor Sipil Jaya adalah mulai dari hari Senin sampai dengan hari Jumat dengan satu *shift* kerja per hari. Sedangkan untuk satpam dikenakan dua *shift* kerja per hari. Apabila seorang pegawai sakit atau berhalangan hadir maka tugasnya akan dilimpahkan kepada rekan kerjanya dalam satu bagian.



Gambar 1.1 Struktur organisasi PT. Kontraktor Sipil Jaya

No.	Nama	Jabatan
1.	A01	Direktur Utama
2.	A02	Direktur Keuangan dan SDM
3.	A03	Direktur Operasi
4.	A04	Sekretaris Perusahaan
5.	A05	Staf Sekretaris Perusahaan
6.	A06	Kepala Divisi TI
7.	A07	Staf Divisi TI
8.	A08	Manajer Keuangan & Akuntansi
9.	A09	Manajer SDM & Hukum
10.	A010	Manajer Operasi & Pemasaran
11.	A011	Manajer Logistik & Peralatan
12.	A012	Staf Divisi Keuangan
13.	A013	Staf Divisi Akuntansi
14.	A014	Staf Divisi SDM
15.	A015	Staf Divisi Hukum
16.	A016	Staf Divisi Arsitektur

17.	A017	Staf Divisi Mekanikal
18.	A018	Staf Divisi Elektrikal
19.	A019	Staf Divisi Pemasaran
20.	A020	Staf Divisi Logistik
21.	A021	Staf Divisi Peralatan
22.	A022	Kepala Proyek
23.	A023	Kepala Proyek
24.	A024	Kepala Kontruksi
25.	A025	Kepala Kontruksi
26.	A026	Kepala Bagian Proyek
27.	A027	Kepala Bagian Proyek
28.	A028	Kepala Urusan Keuangan
29.	A029	Kepala Urusan Arsitektur
30.	A030	Kepala Urusan Mekanikal
31.	A031	Kepala Urusan Elektrikal
32.	A032	Kepala Urusan Logistik
33.	A033	Kepala Urusan Peralatan
34.	A034	Staf Urusan Keuangan
35.	A035	Staf Urusan Arsitektur
36.	A036	Staf Urusan Arsitektur
37.	A037	Staf Urusan Mekanikal
38.	A038	Staf Urusan Mekanikal
39.	A039	Staf Urusan Elektrikal
40.	A040	Staf Urusan Elektrikal
41.	A041	Staf Urusan Logistik
42.	A042	Staf Urusan Peralatan
43.	A043	Juru Gambar Arsitektur
44.	A044	Juru Gambar Mekanikal
45.	A045	Juru Gambar Elektrikal
46.	A046	Resepsionis
47.	A047	Pesuruh
48.	A048	Supir Perusahaan
49.	A049	Satpam
50.	A050	Satpam

Tabel 1.1 Personil PT. Kontraktor Sipil Jaya

Penjelasan singkat mengenai tugas masing-masing jabatan pada Tabel 1.1 adalah:

1. **Dewan Direksi** bertanggung jawab mengelola PT. Kontraktor Sipil Jaya antara lain dengan merumuskan strategi dan kebijakan, memelihara dan mengelola aset, serta memastikan perkembangan pencapaian hasil dan tujuan usaha. Komposisi direksi terdiri dari direktur utama, direktur keuangan dan sumber daya manusia, dan direktur operasi. Direktur memberikan petunjuk, membimbing dan mengawasi pejabat/biro dibawahnya.

2. **Direktur Utama** bertanggung jawab memimpin dan mengendalikan serta memberikan petunjuk kepada para direktur dalam rangka melaksanakan keputusan direksi.
3. **Direktur Keuangan dan SDM** bertugas dan berkewajiban membantu direktur utama dalam memimpin dan mengendalikan kegiatan pengelolaan keuangan, sumber daya manusia, dan aspek hukum perusahaan.
4. **Direktur Operasi** bertugas dan berkewajiban membantu direktur utama dalam memimpin dan mengendalikan kegiatan operasional dan pemasaran, serta pengelolaan logistik dan peralatan. Secara khusus, direktur operasi merupakan perwakilan perusahaan yang berhubungan dengan konsumen dalam hal pembuatan kontrak proyek.
5. **Sekretaris Perusahaan** berfungsi sebagai penghubung antara PT. Kontraktor Sipil Jaya dengan pihak eksternal perusahaan, melayani permintaan pimpinan, serta bertanggung jawab untuk menyediakan dan menyampaikan informasi publik kepada pihak-pihak yang memerlukan secara akurat dan tepat waktu. Sekretaris perusahaan dalam menjalankan tugasnya dibantu oleh seorang staf (staf sekretaris perusahaan).
6. **Kepala Divisi TI** bertugas menetapkan kebijakan dan strategi pengembangan serta pengelolaan SI/TI (perangkat keras dan perangkat lunak komputer), memelihara dan mengawasi penggunaan SI/TI. Kepala divisi TI dalam menerapkan kebijakan, memelihara, dan mengawasi penggunaan SI/TI dibantu oleh seorang staf (staf divisi TI).
7. **Manajer** adalah unsur pimpinan atau setingkat pimpinan dalam tingkatan manajemen yang tugasnya membantu direktur sesuai dengan bidang yang dipimpinnya. Manajer dalam melakukan tugasnnya dibantu oleh staf yang berada dibawahnya.
8. **Kepala Proyek** mempunyai tugas memimpin dan mengelola kegiatan proyek perusahaan.
9. **Kepala Konstruksi** mempunyai tugas memimpin dan mengelola kegiatan konstruksi bangunan dalam sebuah proyek.
10. **Kepala Bagian Proyek** mempunyai tugas membantu kepala proyek memimpin dan

mengelola proyek (misalnya disuatu lokasi) sesuai dengan penugasan yang ditetapkan oleh kepala proyek

11. **Kepala Urusan** mempunyai tugas mengelola urusan sesuai bidangnya masing-masing ditingkat proyek.
12. **Juru Gambar** mempunyai tugas membaca dan mengedit cetak biru gambar arsitektur bangunan, mekanikal, dan elektrikal.
13. **Resepsionis** mempunyai tugas menerima telepon yang masuk, menerima tamu, dan mengantarkan tamu.
14. **Pesuruh** mempunyai tugas membersihkan kantor dan peralatannya, membuat minuman, melayani permintaan pimpinan dan pegawai PT. Kontraktor Sipil Jaya.
15. **Supir Perusahaan** mempunyai tugas mengantar dan menjemput pimpinan perusahaan untuk keperluan pekerjaan.
16. **Satpam** bertugas menjaga keamanan di PT. Kontraktor Sipil Jaya dan mengelola parkir.

1.4 Sistem Informasi di PT. Kontraktor Sipil Jaya

Peranan SI/TI di PT. Kontraktor Sipil Jaya masih sebagai pendukung. Perangkat lunak yang digunakan adalah:

- aplikasi perkantoran untuk pembuatan dokumen, mengelola database, dan mengelola keuangan. Program yang digunakan adalah *Microsoft Office XP Professional Corporate Edition*.
- aplikasi perancangan gambar. Program yang digunakan adalah *AutoCAD 2000*.
- aplikasi manajemen proyek. Program yang digunakan adalah *Microsoft Project 2000*.

PT. Kontraktor Sipil Jaya belum memiliki *web site* perusahaan. Namun perusahaan sudah membuka jalur komunikasi dengan konsumen melalui *email*. Penggunaan Internet juga ditujukan untuk memperoleh *update* aplikasi. Perangkat keras yang digunakan akan dijelaskan

lebih lanjut pada bagian keamanan jaringan dan telekomunikasi.

BAB II

PRAKTEK MANAJEMEN KEAMANAN

Manajemen keamanan mencakup manajemen resiko, kebijakan keamanan, dan pendidikan keamanan. Manajemen resiko adalah proses mengidentifikasi aset-aset perusahaan, mengetahui resiko-resiko yang mengancam aset perusahaan, dan memperkirakan kerusakan dan kerugian yang dapat ditanggung perusahaan jika resiko tersebut menjadi kenyataan. Hasil dari analisa resiko membantu pihak manajemen untuk mengembangkan kebijakan-kebijakan keamanan yang mengarahkan tindakan-tindakan pengamanan dalam perusahaan dan menentukan pentingnya program keamanan perusahaan. Pendidikan keamanan memberikan informasi ini kepada setiap pegawai perusahaan sehingga semua orang mengetahui dan dapat melakukannya dengan lebih mudah dalam mencapai tujuan keamanan yang sama.

2.1 Manajemen Resiko

2.1.1 Identifikasi Aset

Aset dari sistem informasi PT. Kontraktor Sipil Jaya adalah sebagai berikut:

1. Gedung. Sampai saat ini PT. Kontraktor Sipil Jaya baru memiliki satu kantor yang berlokasi di Jakarta, walaupun jangkauan pelayanannya sudah mencakup wilayah Jabotabek. Perusahaan memiliki dua bangunan, yaitu kantor dan gudang. Dua bangunan tersebut dikelilingi tembok setinggi dua meter, dengan luas tanah 850m2, luas bangunan kantor 400m2, dan luas gudang 150m2. Memiliki satu pintu gerbang, satu pos jaga, dan tempat parkir kendaraan. Gedung kantor ini terdiri dari dua lantai, dua pintu (satu didepan dan satu disamping kanan belakang). Lantai bawah terdiri dari 6 ruangan, yaitu ruang lobi,

ruang biro operasi & pemasaran, ruang biro logistik & peralatan, ruang direktur operasi, WC, dan dapur. Lantai atas terdiri dari 8 ruangan, yaitu ruang tunggu atas, ruang biro keuangan & akuntansi, ruang biro SDM & hukum, ruang sekretaris, ruang direktur keuangan & SDM, ruang direktur utama, ruang divisi teknologi informasi, dan WC. Kedua lantai tersebut dihubungkan oleh sebuah tangga. Gudang perusahaan menempel langsung dengan bangunan kantor, untuk menyimpan peralatan. Gudang memiliki satu pintu masuk.

2. Satu *modem ADSL router* 1 *port*, satu *switch* 16 *port*, satu PC *desktop* untuk *server* jaringan yang berada di ruang divisi teknologi informasi.
3. *PC desktop* untuk *client* berjumlah 10 buah dengan rincian: satu untuk direktur utama, satu untuk sekretaris perusahaan, satu untuk direktur keuangan & SDM, satu untuk direktur operasi, dua untuk biro keuangan & akuntansi, satu untuk biro SDM & hukum, dua untuk biro operasi & pemasaran, satu untuk biro logistik dan peralatan.
4. *Notebook* untuk dibawa ke lapangan sebanyak satu buah.
5. *Printer Laser* berjumlah 5 buah, diletakkan dua dibawah dan tiga diatas.
6. *UPS* 1200 VA untuk *server* sebanyak satu buah diletakkan di ruang divisi teknologi informasi.
7. *UPS* 600 VA sebanyak 10 buah untuk masing-masing komputer *client*.
8. Pesawat telepon sebanyak 7 buah dengan rincian: satu untuk direktur utama, satu untuk sekretaris, satu untuk direktur keuangan & SDM, satu untuk direktur operasi, satu di ruang biro operasi dan pemasaran, satu di ruang biro SDM dan hukum, dan satu untuk resepsionis. Didekat pesawat telepon, disediakan nomor telepon penting seperti polisi, pemadam kebakaran, dan rumah sakit.
9. Mesin faksimili sebanyak satu buah di ruangan sekretaris.
10. *Local area network* (*LAN*) yang menghubungkan semua komputer *client* dengan *server*

jaringan.

11. Sistem operasi *server* yaitu *Windows 2000 Server*.
12. Sistem operasi *client* yaitu *Windows 2000 Cli*ent.
13. Aplikasi perkantoran, yaitu *Microsoft Office XP Professional Corporate Edition* yang diinstal di semua *host*.
14. Aplikasi manajemen proyek, yaitu *Microsoft Project 2000* yang hanya diinstal di komputer biro operasi (PC2).
15. Aplikasi perancangan gambar, yaitu *AutoCAD 2000* yang hanya diinstal di komputer biro operasi (PC2 dan PC3).
16. Data yang berisi data keuangan perusahaan, data konsumen, data personil perusahaan, data proyek, data peralatan, dan lain-lain.
17. Dokumen perusahaan seperti surat izin usaha, kontrak-kontrak kerja, dokumen proyek, dan lain-lain.
18. Dokumentasi jaringan komputer yang mencakup spesifikasi komputer dan peralatan lainnya, daftar aplikasi, dan setting modem.
19. Sambungan Internet dengan menggunakan *ADSL*.
20. Sambungan listrik
21. Sambungan telepon dua nomor
22. Sambungan jaringan komputer

Tata ruang beserta letak perangkat komputer diperlihatkan pada Lampiran A.

2.1.2 Analisa Resiko

Setelah mengetahui aset perusahaan, langkah selanjutnya dalam manajemen resiko adalah melakukan analisa resiko. Analisa resiko merupakan metode mengidentifikasi resiko dan menilai kerusakan yang mungkin disebabkan, sebagai alasan perlunya perlindungan keamanan. Analisa resiko memiliki tiga tujuan: mengidentifikasi resiko, menghitung dampak

dari ancaman, dan memberikan perbandingan biaya/manfaat antara dampak resiko dengan biaya. Pada makalah ini, analisa resiko akan dilakukan dengan pendekatan kuantitatif. Hasil analisa resiko diperlihatkan pada Tabel 2.1.

No.	Aset	Klasifikasi Aset	Resiko	Nilai Aset (Rp.)	Potensi Kerugian /SLE(Rp.)	Frekuensi Kejadian /ARO	Kerugian per tahun /ALE(Rp.)
1.	Data	informasi	terinfeksi virus/worm dicuri	20.000.000	5.000.000 16.000.000	1 0,4	5.000.000 6.400.000
2.	Dokumen perusahaan	informasi	dicuri	10.000.000	5.000.000	0,2	1.000.000
3.	Dokumentasi jaringan komputer	informasi	dicuri	500.000	500.000	0,01	50.000
4.	Sistem Operasi *Server* + 11 *Client*	perangkat lunak	terinfeksi virus/worm	7.000.000	6.300.000	1	6.300.000
5.	Aplikasi Perkantoran (11 paket)	perangkat lunak	terinfeksi virus/worm	55.000.000	27.500.000	0,1	2.750.000
6.	Aplikasi Manajemen Proyek (1 paket)	perangkat lunak	terinfeksi virus/worm	8.000.000	7.200.000	0,1	720.000
7.	Aplikasi Perancangan Gambar (2 paket)	perangkat lunak	terinfeksi virus/worm	3.000.000	2.700.000	0,1	270.000
8.	Gedung	fisik	kebakaran	3.000.000.000	1.500.000.000	0,02	30.000.000
9.	*Modem ADSL Router* (1 buah)	fisik	dicuri	2.500.000	2.500.000	0,5	1.250.000
10.	*Switch* (1 buah)	fisik	dicuri	6.000.000	6.000.000	0,5	3.000.000
11.	*Local Area Network*	fisik	dicuri	3.000.000	2.000.000	0,5	1.000.000
12.	*PC Desktop* untuk *server* (1 unit)	fisik	dicuri	25.000.000	25.000.000	0,5	12.500.000
13.	*PC Desktop* untuk *client* (10 unit)	fisik	dicuri	150.000.000	60.000.000	0,5	30.000.000
14.	*Notebook* (1 unit)	fisik	dicuri	25.000.000	25.000.000	0,8	20.000.000
15.	*Printer Laser* (5 unit)	fisik	dicuri	60.000.000	30.000.000	0,5	15.000.000
16.	Pesawat telepon (7 buah)	fisik	dicuri	4.200.000	2.100.000	0,5	1.050.000
17.	Faksimili (1 buah)	fisik	dicuri	3.000.000	3.000.000	0.5	1.500.000
18.	*UPS* 1200 VA (1 buah)	fisik	dicuri	16.000.000	16.000.000	0,5	8.000.000
19.	*UPS* 600VA (10 buah)	fisik	dicuri	10.000.000	4.000.000	0,5	2.000.000
20.	Jaringan komputer	layanan	putus	6.000.000	2.000.000	1	2.000.000
21.	Listrik	layanan	padam	36.000.000	7.200.000	1	7.200.000
22.	Telepon (dua nomor)	layanan	putus	50.000.000	10.000.000	1	10.000.000
23.	*ADSL*	layanan	putus	12.000.000	600.000	1	600.000
TOTAL							**167.590.000**

Tabel 2.1 Analisa resiko kuantitatif

Tabel 2.2 berikut memperlihatkan urutan aset berdasarkan besarnya ALE, resiko, dan agen pembawa resiko:

No.	Urutan Aset Berdasarkan ALE	Resiko	Agen Pembawa
1.	Gedung	kebakaran	api
2.	*PC desktop* untuk *client*	dicuri	pencuri
3.	*Notebook*	dicuri	pencuri
4.	*Printer Laser*	dicuri	pencuri
5.	*PC desktop* untuk *server*	dicuri	pencuri
6.	Data	terinfeksi virus/worm dicuri	virus/worm cracker, pegawai/pencuri
7.	Telepon	putus	sambaran petir
8.	*UPS* 1200 VA	dicuri	pencuri
9.	Listrik	padam	penyedia layanan
10.	Sistem operasi *server* + *client*	terinfeksi virus/worm	virus/worm
11.	*Switch*	dicuri	pencuri
12.	Aplikasi perkantoran	terinfeksi virus/worm	virus/worm
13.	Jaringan komputer	putus	attacker, administrator
14.	UPS 600VA	dicuri	pencuri
15.	Faksimili	dicuri	pencuri
16.	*Modem ADSL router*	dicuri	pencuri
17.	Pesawat telepon	dicuri	pencuri
18.	*LAN*	dicuri	pencuri
19.	Dokumen perusahaan	dicuri	pencuri
20.	Aplikasi manajemen proyek	terinfeksi virus/worm	virus/worm
21.	*ADSL*	putus	penyedia layanan
22.	Aplikasi perancangan gambar	terinfeksi virus/worm	virus/worm
23.	Dokumentasi jaringan komputer	dicuri	pencuri

Tabel 2.2 Urutan asset berdasarkan besar kerugian

Selanjutnya, urutan aset pada Tabel 2.2 dapat dikelompokkan lagi berdasarkan jenis resikonya seperti diperlihatkan pada Tabel 2.3 berikut:

No.	Aset	Resiko	ALE (Rp.)
1.	*PC desktop* untuk *client*	dicuri	30.000.000
2.	*Notebook*	dicuri	20.000.000
3.	*Printer Laser*	dicuri	15.000.000
4.	*PC desktop* untuk server	dicuri	12.500.000
5.	*UPS* 1200 VA	dicuri	8.000.000
6.	Data	dicuri	6.400.000
7.	*Switch*	dicuri	3.000.000
8.	*UPS* 600VA	dicuri	2.000.000
9.	Faksimili	dicuri	1.500.000
10.	*Modem ADSL Router*	dicuri	1.250.000

11.	Pesawat telepon	dicuri	1.050.000
12.	*LAN*	dicuri	1.000.000
13.	Dokumen perusahaan	dicuri	1.000.000
14.	Dokumentasi jaringan komputer	dicuri	50.000
Total			**102.750.000**
15.	Gedung	kebakaran	30.000.000
Total			**30.000.000**
16.	Sistem operasi *server + client*	terinfeksi virus/worm	6.300.000
17.	Data	terinfeksi virus/worm	5.000.000
18.	Aplikasi perkantoran	terinfeksi virus/worm	2.750.000
19.	Aplikasi manajemen proyek	terinfeksi virus/worm	720.000
20.	Aplikasi perancangan gambar	terinfeksi virus/worm	270.000
Total			**15.040.000**
21.	Listrik	padam	7.200.000
22.	Telepon	putus	10.000.000
23.	Jaringan komputer	putus	2.000.000
24.	*ADSL*	putus	600.000
Total			**19.800.000**
TOTAL KERUGIAN			**167.590.000**

Tabel 2.3 Klasifikasi aset berdasarkan resiko

2.1.3 Penanggulangan Resiko

Seperti dapat dilihat pada Tabel 2.3, kerugian yang dapat ditanggung perusahaan per tahun akibat resiko dicuri sebesar Rp 102.750.000,-. Hal ini tentu saja membutuhkan berbagai tindakan pengamanan yang sesuai, yang bisa berupa solusi teknis maupun solusi non teknis. Tindakan pengamanan teknis yang dapat dilakukan adalah:

1. Penambahan jumlah satpam dimana pada malam hari akan ditugaskan 2 orang satpam. Sedangkan untuk shift pagi dan siang ditugaskan masing-masing 1 orang satpam.
2. Perbaikan fasilitas keamanan fisik seperti penggunaaan gembok yang kuat di pintu gerbang, pintu depan dan pintu belakang kantor, penggunaan alarm di pintu depan dan belakang serta jendela lantai bawah, penambahan penerangan, pemasangan terali besi di semua jendela dan ventilasi, dan pemasangan CCTV didalam gedung.

3. Penyediaan satu pesawat telepon di pos jaga agar satpam dapat menghubungi polisi.
4. Mengasuransikan aset

Rincian biaya untuk penanggulangan pencurian disajikan pada Tabel 2.4 dibawah ini:

No.	Penganggulangan Resiko Pencurian	Jumlah	Biaya (Rp.)	Biaya Resiko per tahun (Rp.)
1.	Tenaga satpam	2 orang	18.000.000	
2.	Gembok	3 (1 gerbang dan 2 pintu)	300.000	
3.	Alarm	1 paket	20.000.000	
4.	Terali besi	20 (jendela dan ventilasi)	10.000.000	
5.	Lampu	5 lampu	100.000	
6.	CCTV	3 kamera	15.000.000	
7.	Pesawat telepon di pos jaga	1 pesawat	100.000	
8.	Asuransi kecurian	1 tahun	500.000	
Total			**64.000.000**	**102.750.000**

Tabel 2.4 Biaya penanggulangan pencurian Vs biaya resiko

Sedangkan untuk resiko kebakaran, kerugian akibat resiko ini per tahun adalah sebesar Rp 30.000.000,-. Tindakan pengamanan yang dapat dilakukan adalah:

1. Penambahan tiga buah tabung pemadam kebakaran, diletakkan di ruang divisi teknologi informasi, ruang biro keuangan dan akuntansi, dan ruang biro operasi dan pemasaran.
2. Penambahan alat pendeteksi asap yang akan mendeteksi adanya asap yang berlebihan di delapan titik, yaitu dapur, ruang tengah bawah, lobi, ruang tengah atas, ruang divisi teknologi informasi, dan tiga ruang direktur.
3. Penyediaan satu pesawat telepon di pos jaga agar satpam dapat menghubungi pemadam kebakaran.
4. Asuransi kebakaran

Rincian biaya untuk penanggulangan kebakaran disajikan pada Tabel 2.5 dibawah ini:

No.	Penanggulangan Resiko Kebakaran	Jumlah	Biaya (Rp.)	Biaya Resiko per tahun (Rp.)
1.	Tabung pemadam kebakaran	3 tabung	3.000.000	
2.	Alat pendeteksi asap	8 buah	4.000.000	
3.	Pesawat telepon di pos jaga	1 pesawat	100.000*	
4.	Asuransi kebakaran	1 tahun	500.000	
Total			**7.500.000**	**30.000.000**

***** tidak dihitung lagi

Tabel 2.5 Biaya penanggulangan kebakaran Vs biaya resiko

Untuk resiko infeksi virus dan ancaman cracker terhadap perangkat lunak, data elektronik, dan serangan DoS terhadap jaringan komputer, kerugian yang diakibatkan adalah sebesar Rp 17.040.000,- (15.040.000 + 2.000.0000). Oleh karena itu, tindakan pengamanan yang dapat dilakukan adalah :

1. Pemasangan program anti virus
2. Pemasangan program Internet security

Rincian biaya untuk penanggulangan virus dan attacker disajikan pada Tabel 2.6 dibawah ini:

No.	Penanggulangan Resiko Virus dan Attacker	Jumlah	Biaya (Rp.)	Biaya Resiko per tahun (Rp.)
1.	Symantec Antivirus Corporate Edition 9.0 For Workstations & Network Servers Gold Maint 2nd & 3rd Yr Ext for 12 Licenses	1	6.134.400	
2.	Norton Internet Security™ 2004 Professional Small Office Pack	1	7.200.000	
Total			**13.334.400**	**17.040.000**

Tabel 2.6 Biaya penanggulangan virus & attacker Vs biaya resiko

Resiko putusnya sambungan telepon karena sambaran petir dan layanan ADSL tidak bisa ditanggulangi. Untuk resiko terjadinya pemadaman listrik, kerugian yang dapat ditimbulkan per tahun adalah sebesar Rp 7.200.000,00. Tindakan pengamanan yang dapat dilakukan

adalah pembelian genset. Rincian biaya pembelian genset diperlihatkan pada Tabel 2.7.

No	Penanggulangan Resiko Pemadaman Listrik	Jumlah	Biaya (Rp.)	Biaya Resiko per tahun (Rp.)
1.	Genset 5000 watt	1	6.000.000	
Total			**6.000.000**	**7.200.000**

Tabel 2.7 Biaya penanggulangan pemadaman listrik Vs biaya resiko

Jadi, total biaya yang dikeluarkan untuk menghindari/mengurangi/menanggulangi resiko yang mengancam aset perusahaan per tahun adalah Rp. 90.834.400,- terhadap biaya resiko sebesar Rp. 167.590.000,-.

2.2 Kebijakan Keamanan

Selain solusi teknis yang dibahas diatas, perusahaan juga dapat melakukan solusi non teknis untuk menghadapi resiko keamanan. Solusi non teknis mencakup kebijakan, prosedur, standar, dan pedoman keamanan.

2.2.1 Kebijakan

Kebijakan keamanan adalah pernyataan umum yang dikeluarkan pihak manajemen sebagai visi keamanan yang berlaku di perusahaan. Saat ini, belum ada dokumentasi kebijakan keamanan yang dibuat perusahaan. Isi dokumen kebijakan keamanan mencakup judul kebijakan, tujuan, ruang lingkup, kebijakan, penegakan, definisi, dan histori revisi. Contoh dokumen kebijakan keamanan diperlihatkan pada Lampiran B. Beberapa kebijakan yang dapat dikembangkan adalah:

- kebijakan penggunaan komputer. Tujuan dari kebijakan ini adalah sebagai garis besar cara penggunaan komputer yang diperkenankan di PT. Kontraktor Sipil Jaya.
- kebijakan keamanan *server*. Tujuan dari kebijakan ini adalah untuk menetapkan standar konfigurasi dasar dari *server* jaringan yang dimiliki dan dioperasikan oleh PT. Kontraktor

Sipil Jaya. Pelaksanaan kebijakan *server* secara efektif akan meminimalkan akses yang tidak memiliki wewenang terhadap teknologi dan informasi milik. PT. Kontraktor Sipil Jaya.

- kebijakan enkripsi. Tujuan dari kebijakan ini adalah untuk memberikan panduan yang membatasi penggunaan enkripsi pada algoritma-algoritma yang terbukti efektif.
- kebijakan *email*. Tujuan dari kebijakan ini adalah untuk mencegah menurunnya citra PT. Kontraktor Sipil Jaya karena ketika *email* dikirim keluar dari PT. Kontraktor Sipil Jaya, masyarakat umum cenderung melihat pesan tersebut sebagai pernyataan resmi dari PT. Kontraktor Sipil Jaya.
- kebijakan audit. Tujuan dari kebijakan ini adalah untuk menyatakan persetujuan berkenaan dengan *scanning* keamanan jaringan yang ditawarkan oleh auditor eksternal kepada PT. Kontraktor Sipil Jaya.
- kebijakan *password*. Tujuan dari kebijakan ini adalah untuk menetapkan standar pembuatan *password* yang kuat, perlindungan *password*, dan frekuensi perubahannya.
- kebijakan keamanan *router*. Tujuan dari kebijakan ini adalah untuk menggambarkan konfigurasi keamanan minimal yang dibutuhkan untuk semua *router* dan *switch* yang terhubung ke jaringan di PT. Kontraktor Sipil Jaya.

Kebijakan-kebijakan perusahaan tidak hanya keamanan sistem komputer tapi juga menyinggung berbagai aspek diluar sistem komputer itu, seperti kebijakan perlindungan fisik atau fasilitas dimana sistem informasi berada, yang mencakup:

- Penetapan tanggung jawab satpam dan pegawai lainnya dalam melindungi fasilitas
- Apa yang dilakukan untuk mengamankan fasilitas seperti penguncian gedung pada hari libur, dimana menyimpan kunci secara aman dan siapa yang memegang kunci.

2.2.2 Prosedur

Prosedur adalah detil langkah demi langkah untuk melakukan tugas tertentu. Langkah-

langkah tersebut diterapkan oleh staf TI, *end user*, atau siapa saja yang ingin menginstal, mengkonfigurasi komputer atau peralatan jaringan. Prosedur merinci bagaimana kebijakan, standar, dan pedoman dilaksanakan. Saat ini belum ada dokumentasi prosedur yang ditemukan di PT. Kontraktor Sipil Jaya. Contoh isi dokumen prosedur diperlihatkan pada Lampiran B. Prosedur-prosedur penting yang seharusnya dibuat seperti: prosedur melakukan *scan* virus, prosedur *backup*, prosedur *format*, prosedur instalasi, prosedur pembuatan dan penggantian *password*, prosedur pembagian *file* dan data, prosedur penyimpanan file, prosedur *update* aplikasi, prosedur menghidupkan dan mematikan komputer, prosedur menghadapi kebakaran, banjir, huru hara, prosedur menghidupkan genset, dan lain-lain.

2.2.3 Standar

Standar keamanan perusahaan menetapkan produk perangkat keras dan perangkat lunak yang digunakan. Contoh isi dokumen standar keamanan diperlihatkan pada Lampiran B.

2.2.4 Pedoman

Pedoman adalah tindakan rekomendasi dan panduan operasional bagi pengguna, staf TI, dan pegawai lainnya bila tidak ada suatu standar yang berkaitan. Contoh isi dokumen pedoman keamanan diperlihatkan pada Lampiran B.

2.3 Pendidikan Keamanan

Agar kebijakan, prosedur, standar, dan pedoman keamanan dapat dilaksanakan secara efektif, maka perlu disebarkan kepada semua pegawai. Caranya dengan memberikan dokumen keamanan ini kepada semua pegawai pada saat penerimaan pegawai, mengadakan pelatihan dan pengawasan setiap hari bagaimana pegawai melaksanakan tindakan keamanan. Pelatihan juga dilakukan secara berulang setiap satu tahun agar pegawai tidak lupa terutama terhadap tindakan keamanan yang jarang dilakukan.

BAB III

KONTROL AKSES

Kontrol akses adalah fitur keamanan yang mengontrol bagaimana pengguna dan sistem berkomunikasi dan berinteraksi dengan sumber daya dan sistem yang lain. Kontrol akses bertujuan untuk melindungi sistem dan sumber daya dari akses yang tidak berwenang dan menentukan tingkat autorisasi setelah prosedur autentikasi berhasil dilaksanakan.

3.1 Identifikasi, Autentikasi, Autorisasi, dan Akuntabilitas

3.1.1 Identifikasi

Identifikasi menggambarkan suatu metode untuk memastikan bahwa subjek (pengguna, program, atau proses) merupakan entiti yang bersangkutan. Identifikasi yang digunakan pegawai PT. Kontraktor Sipil Jaya dalam penggunaan komputer adalah *username*, yang dibuat oleh administrator jaringan. Selain itu, secara fisik pegawai PT. Kontraktor Sipil Jaya juga diberi tanda pengenal dan memiliki nomor pegawai.

3.1.2 Autentikasi

Autentikasi adalah tindakan memverifikasi identitas. Teknik yang dipakai di PT. Kontraktor Sipil Jaya adalah dengan menggunakan *password* (sesuatu yang hanya diketahui pengguna). *Password* yang digunakan harus sesuai dengan standar *password* perusahaan, dan diganti secara teratur mengacu pada kebijakan penggunaan *password*. *Password* pengguna harus diganti setiap satu bulan.

3.1.3 Autorisasi

Autorisasi berarti pemberian izin bagi seseorang untuk mengakses atau melakukan sesuatu. Autorisasi dilakukan dengan melihat *access control matirx*. *Access control matrix*

adalah tabel berisi subjek dan objek yang menunjukkan tindakan apa yang dapat dilakukan subjek terhadap objek. *Access control matrix* untuk *file* diperlihatkan pada Lampiran C. Subjek adalah entiti aktif yang memerlukan informasi yang dapat berupa orang, proses, dan program. Sedangkan objek adalah entiti pasif yang mengandung informasi yang dapat berupa komputer, database, file, program, directory, atau field dalam database. Selain *access control matrix*, dibangun juga *access control lists* (*ACL*) yang menentukan akses terhadap perangkat keras, lihat Lampiran C. Walaupun pada *ACL* pengguna memiliki *full control* terhadap perangkat komputer, namun untuk proses instalasi program hanya boleh dilakukan oleh orang dari divisi TI. *Full control* berarti pegawai yang bersangkutan memiliki *account* pada komputer, walaupun mungkin jarang memakai komputer tersebut.

3.1.4 Akuntabilitas

Melakukan audit terhadap pengguna sistem informasi berguna untuk memeriksa apakah kebijakan keamanan sudah ditegakkan. Hal ini untuk menjamin bahwa para pengguna bertanggung jawab terhadap tindakan mereka. Audit dapat dilakukan oleh auditor eksternal atau internal (pengawasan harian). Hal-hal yang diaudit meliputi:

- *System-level events* (percobaan *logon*, *logon ID*, tanggal dan waktu *logon*, *lockouts*, peralatan yang dipakai, fungsi-fungsi yang dilakukan, dan lain-lain).
- *Application-level events* (pesan-pesan kesalahan aplikasi, *file* yang dibuka dan ditutup, modifikasi *file*, dan pelanggaran keamanan terhadap aplikasi).
- *User-level events* (percobaan identifikasi dan autentikasi, *file*-servis-dan sumber daya yang dipakai, perintah yang diberikan, dan pelanggaran keamanan).

BAB IV

ARSITEKTUR DAN MODEL KEAMANAN

Model keamanan merupakan suatu pernyataan yang menguraikan kebutuhan yang diperlukan untuk mendukung suatu kebijakan keamanan tertentu. Sedangkan arsitektur adalah kerangka dan struktur sebuah sistem.

4.1 Arsitektur Sistem

Jaringan komputer di PT. Kontraktor Sipil Jaya berupa sebuah *local area network* sederhana yang terdiri dari:

1. Satu *Modem ADSL Router* yang menghubungkan jaringan dengan Internet. Koneksi Internet hanya aktif selama jam kerja kantor.
2. Satu *server* jaringan yang diinstal perangkat lunak *Internet Security* dan *Anti Virus*. *Server* ini dimonitor oleh seorang staf TI.
3. Switch yang menghubungkan *server* dengan *workstation*. Setiap *workstation* juga diperlengkapi dengan perangkat lunak *Internet Security* dan *Anti Virus*.
4. Enam buah *workgroup/domain* masing-masing untuk sekretaris perusahaan, teknologi informasi, keuangan dan akuntansi, SDM dan hukum, operasional dan pemasaran, dan logistik dan peralatan.
5. *Database* yang masih terdistribusi, namun selalu dibuat cadangannya secara teratur oleh divisi TI melalui *server*.

4.2 Model Keamanan

Model keamanan yang diterapkan pada PT. Kontraktor Sipil Jaya adalah model *Bell-LaPadula*. Model ini menekankan pada aspek-aspek kerahasiaan dari kontrol akses. Model ini

menggunakan *access control matrix* dan tingkat keamanan untuk menentukan apakah subjek dapat mengakses objek. Izin yang dimiliki subjek dibandingkan dengan klasifikasi objek; jika izinnya lebih tinggi atau sama dengan klasifikasi objek, maka subjek dapat mengakses objek tanpa adanya pelanggaran kebijakan keamanan. Tabel 4.1 menunjukkan hubungan antara subjek dan objek menurut model Bell-LaPadula.

Subject's Clearance	***Right***	***Object's Classification***
Confidential	*Read*	*Confidential*
		Private
		Sensitive
		Public
Confidential	*Read-Write*	*Confidential*
Confidential	*Append*	*Confidential*
Private	*Read*	*Private*
		Sensitive
		Public
Private	*Cannot read*	*Confidential*
Private	*Read-Write*	*Private*
Private	*Append*	*Confidential*
		Private
Sensitive	*Read*	*Sensitive*
		Public
Sensitive	*Cannot read*	*Confidential*
		Private
Sensitive	*Read-Write*	*Sensitive*
Sensitive	*Append*	*Confidential*
		Private
		Sensitive
Public	*Read*	*Public*
Public	*Cannot read*	*Confidential*
		Private
		Sensitive

Public	*Read-Write*	*Public*
Public	*Append*	*Confidential*
		Private
		Sensitive
		Public

Tabel 4.1 Akses subjek terhadap objek

Tabel 4.2 dan 4.3 memperlihatkan izin dan klasifikasi terhadap subjek dan objek. Urutan sensitivitas dari yang tertinggi ke yang terendah adalah *confidential*, *private*, *sensitive*, dan *public*.

No.	Nama	Jabatan	Izin
1.	A01	Direktur Utama	*Confidential*
2.	A02	Direktur Keuangan dan SDM	*Confidential*
3.	A03	Direktur Operasi	*Confidential*
4.	A04	Sekretaris Perusahaan	*Confidential*
5.	A05	Staf Sekretaris Perusahaan	*Confidential*
6.	A06	Kepala Divisi TI	*Sensitive*
7.	A07	Staf Divisi TI	*Sensitive*
8.	A08	Manajer Keuangan & Akuntansi	*Confidential*
9.	A09	Manajer SDM & Hukum	*Confidential*
10.	A010	Manajer Operasi & Pemasaran	*Confidential*
11.	A011	Manajer Logistik & Peralatan	*Sensitive*
12.	A012	Staf Divisi Keuangan	*Confidential*
13.	A013	Staf Divisi Akuntansi	*Confidential*
14.	A014	Staf Divisi SDM	*Confidential*
15.	A015	Staf Divisi Hukum	*Confidential*
16.	A016	Staf Divisi Arsitektur	*Sensitive*
17.	A017	Staf Divisi Mekanikal	*Sensitive*
18.	A018	Staf Divisi Elektrikal	*Sensitive*
19.	A019	Staf Divisi Pemasaran	*Sensitive*
20.	A020	Staf Divisi Logistik	*Sensitive*
21.	A021	Staf Divisi Peralatan	*Sensitive*
22.	A022	Kepala Proyek	*Sensitive*
23.	A023	Kepala Proyek	*Sensitive*
24.	A024	Kepala Kontruksi	*Sensitive*
25.	A025	Kepala Kontruksi	*Sensitive*
26.	A026	Kepala Bagian Proyek	*Sensitive*
27.	A027	Kepala Bagian Proyek	*Sensitive*
28.	A028	Kepala Urusan Keuangan	*Sensitive*
29.	A029	Kepala Urusan Arsitektur	*Sensitive*
30.	A030	Kepala Urusan Mekanikal	*Sensitive*

31.	A031	Kepala Urusan Elektrikal	*Sensitive*
32.	A032	Kepala Urusan Logistik	*Sensitive*
33.	A033	Kepala Urusan Peralatan	*Sensitive*
34.	A034	Staf Urusan Keuangan	*Sensitive*
35.	A035	Staf Urusan Arsitektur	*Sensitive*
36.	A036	Staf Urusan Arsitektur	*Sensitive*
37.	A037	Staf Urusan Mekanikal	*Sensitive*
38.	A038	Staf Urusan Mekanikal	*Sensitive*
39.	A039	Staf Urusan Elektrikal	*Sensitive*
40.	A040	Staf Urusan Elektrikal	*Sensitive*
41.	A041	Staf Urusan Logistik	*Sensitive*
42.	A042	Staf Urusan Peralatan	*Sensitive*
43.	A043	Juru Gambar Arsitektur	*Sensitive*
44.	A044	Juru Gambar Mekanikal	*Sensitive*
45.	A045	Juru Gambar Elektrikal	*Sensitive*
46.	A046	Resepsionis	*Sensitive*
47.	A047	Pesuruh	*Sensitive*
48.	A048	Supir Perusahaan	*Sensitive*
49.	A049	Satpam	*Sensitive*
50.	A050	Satpam	*Sensitive*

Tabel 4.2 Izin Subjek

No.	Objek	Klasifikasi
1.	Neraca.xls	*Confidential*
2.	Laba Rugi.xls	*Confidential*
3.	Akuntansi.xls	*Confidential*
4.	Kontrak Proyek.doc	*Confidential*
5.	Surat Masuk dan Keluar.doc	*Confidential*
6.	Gaji Pegawai.xls	*Confidential*
7.	Inventaris Jaringan.xls	*Sensitive*
8.	HW dan SW setting.doc	*Sensitive*
9.	Logistik.xls	*Sensitive*
10.	Peralatan.db	*Sensitive*
11.	Gambar Konstruksi.dwg	*Sensitive*
12.	Keamanan.doc	*Sensitive*

Tabel 4.3 Klasifikasi Objek

BAB V

KEAMANAN FISIK

Keamanan fisik dan infrastrukturnya merupakan hal yang penting bagi perusahaan. Mekanisme keamanan fisik melindungi orang, data, perlengkapan, sistem dan fasilitas yang ada dalam perusahaan.

Keamanan fisik dapat dicapai melalui konstruksi fasilitas yang layak, perlindungan kerusakan air dan kebakaran, mekanisme anti pencuri dan adanya prosedur keamanan yang diberlakukan. Keamanan fisik berhubungan dengan bagaimana orang dapat masuk secara fisik kedalam lingkungan perusahaan, hal ini berbeda dengan keamanan komputer yang berhubungan dengan bagaimana orang dapat masuk kedalam lingkungan melalui port atau modem. Dengan pertimbangan diatas, PT. Kontraktor Sipil Jaya pun memerlukan adanya kontrol keamanan fisik yang bertujuan untuk melindungi aset perusahaan secara fisik.

Kontrol keamanan fisik yang dapat dilakukan di PT. Kontraktor Sipil Jaya, yang berada dibawah naungan keamanan fisik terdiri atas:

1. Kontrol administratif dapat terdiri dari :
    - Pemilihan/penggunaan fasilitas atau konstruksi yang baik. Beberapa tindakan pengamanan fasilitas sudah disinggung pada bagian praktek manajemen keamanan.
    - Manajemen fasilitas. Perkembangan gedung diwaktu mendatang harus melibatkan divisi TI dan seluruh direksi agar aspek keamanan sistem informasi juga turut masuk dalam perencanaan mendatang.
    - Kontrol personil. Kontrol personil pada PT. Kontraktor Sipil Jaya melibatkan secara khusus Biro SDM.

- Pelatihan keamanan mencakup pelatihan menghadapi kebakaran, atau tindakan yang harus dilakukan jika terjadi gangguan secara fisik lainnya seperti banjir, pencuri, dan lain-lain.

2. Kontrol Teknis

   Seperti pada bagian praktek manajemen keamanan, disebutkan bahwa penambahan keamanan fisik dilakukan dengan memasang alarm pencuri, detektor asap, pemasangan *CCTV* didalam gedung, pemasangan genset, kontrol akses gedung oleh satpam.

3. Kontrol Fisik

   Kontrol fisik dilakukan dengan penambahan cahaya, pemakaian gembok yang lebih kuat untuk pagar dan kedua pintu masuk gedung, dan penambahan pencahayaan. Pada bab praktek manajemen keamanan sudah dicantumkan biaya penanggulangan versus biaya kerugian jika resiko terjadi. Penguncian gedung dilakukan oleh satpam, namun satpam hanya memegang kunci pintu luar. Untuk kunci-kunci ruangan digantung didekat meja resepsionis. Sedangkan kunci lemari meja disimpan oleh pemiliknya masing-masing ditempat yang tersembunyi atau dapat dibawa pulang. Semua kunci serep disimpan di ruangan direktur utama.

5.1 Manajemen Fasilitas

Fasilitas fisik mencakup bangunan atau gedung yang berisikan karyawan, perlengkapan, data, dan komponen jaringan. Manajemen fasilitas ini semestinya dibuat terlebih dahulu sebelum bangunan atau gedung didirikan, yang diperuntukkan untuk pemilihan lokasi, material dan sistem pendukung.

Ketika pemilihan lokasi, beberapa hal yang kritis terhadap pengambilan keputusan yaitu:

1. Visibiliti yang terdiri atas :
    - Dari segi tanda bangunan, perusahaan memiliki papan nama perusahaan yang cukup besar sehingga orang dengan mudah melihatnya.
    - Dari segi tipe tetangga, tetangga cukup mendukung dan tidak pernah terjadi perselisihan. Gedung PT. Kontraktor Sipil Jaya bersebelahan dengan bengkel kendaraan dan toko bangunan, serta dibagian belakang merupakan rumah penduduk.
    - Dari segi populasi area bahwa populasi di area tersebut cukup padat namun tidak mengganggu aktivitas perusahaan.
2. Area lingkungan sekitar dan entitas luar
    - Area lingkungan perusahaan dinilai cukup aman dan jarang terjadi tindakan kriminalitas.
    - Jarak lokasi dengan pos polisi, rumah sakit dan stasiun pemadam kebakaran, tidaklah terlalu jauh hanya radius kurang lebih 1 km sehingga relatif lebih aman.
3. Kemudahan Akses
    - Dari segi akses jalan, cukup mudah karena lokasi gedung berada di samping jalan raya sehingga mudah dijangkau.
    - Dari segi kepadatan lalu lintas, lalu lintas tidaklah terlalu macet karena lebar jalan cukup besar.
    - Dari segi jarak ke lapangan udara cukup jauh sekitar 25 km, sedangkan jarak dari stasiun kereta cukup dekat sekitar 1 km sehingga mudah dijangkau.
4. Bencana alam

    Bencana alam yang cukup mengganggu adalah banjir yang semakin tinggi dan meluas di kota Jakarta. Walaupun banjir belum sampai masuk ke halaman perusahaan, namun jalan-jalan disekitar lokasi perusahaan sudah mulai tergenang.

5.2 Konstruksi

Material konstruksi fisik dan komposisi struktur bangunan perlu dievaluasi karakteristik proteksinya, utilitas dan biaya serta keuntungan yang diberikan. Material bangunan yang berbeda menyediakan level yang berbeda pula terhadap perlindungan api kebakaran dan ketahanan yang berhubungan dengan tingkat api. Dengan demikian untuk keamanan fasilitas fisik, beberapa hal dibawah ini perlu dikaji dan dievaluasi untuk perencanaan perbaikan di masa mendatang, yaitu :

1. Pintu
    - Dari segi material, pintu gedung terbuat dari kayu dimana bahan ini memang tidak kuat terhadap api sehingga bisa diganti dengan pintu dari bahan logam.
    - Seperti sudah disinggung sebelumnya, PT. Kontraktor Sipil Jaya akan memasang alarm pencuri pada pintu masuk gedung, dan penggantian gembok dengan kualitas yang lebih baik di pintu gerbang dan pintu masuk gedung.
2. Langit-langit
    - Bahan material langit-langit yang digunakan saat ini adalah kayu, namun antara lantai 1 dan 2 dan juga atap bangunan paling atas merupakan beton yang cukup tebal.
3. Jendela
    - Gedung mempunyai beberapa jendela yang akan dipasang alarm pencuri (lihat bab praktek manajemen keamanan).
4. Lantai
    - Bahan material lantai yang digunakan saat ini adalah terbuat dari marmer dan cukup tahan terhadap api.
5. Pemanas dan Pendingin Udara
    - Perusahaan tidak memiliki pemanas ruangan, yang ada adalah *AC* hampir di semua ruangan kecuali WC dan dapur.

6. Pendeteksi Kebakaran

- Disebutkan juga pada bab praktek manajemen keamanan, PT. Kontraktor Sipil Jaya akan memasang detektor asap hampir disemua ruangan.

5.3 Ruangan Komputer

Pada perusahaan, ruangan komputer adalah ruangan divisi TI yang berisi *server* jaringan, *modem*, *switch*, dan *tape* untuk *backup* data yang disimpan dalam brankas tahan api. Ruangan ini hanya bisa dimasuki oleh orang divisi TI, dan kunci ruangan juga tidak diberikan ke satpam. Artinya jika ada orang selain divisi TI masuk ke ruangan, orang tersebut akan langsung berhadapan dengan kepala dan staf divisi TI yang ada didalam. Ruangan ini tidak terlalu besar dan hanya mempunyai satu pintu masuk untuk akses ke dalam ruangan. Tidak ada jalan lain untuk masuk ke ruangan komputer ini. Pengamanannya yaitu pada pintu ruangan dikunci dan belum ada mekanisme lain atau teknologi lain untuk masuk ke dalam ruangan tersebut seperti dengan menggunakan *finger print*, *magnetic cards* dan sebagainya dikarenakan harga alat tersebut cukup mahal.

5.4 Security Must

Seperti telah diatur oleh undang-undang, ada kebutuhan keamanan tertentu yang harus dimiliki oleh sebuah gedung. Kebutuhan keamanan tersebut yang ada di gedung PT. Kontraktor Sipil Jaya adalah detektor asap, tanda keluar gedung yang jelas dan mengeluarkan cahaya diwaktu gelap, dua pintu untuk masuk dan keluar gedung.

5.5 Security Should

Ada beberapa prosedur perlindungan yang sudah dimasukkan dan diterapkan dalam perusahanan seperti *backup* data kritis, konfigurasi komponen-komponen yang sudah

merupakan bagian dari sistem operasi dan perangkat keras, memperhatikan aktivitas karyawan yang mencurigakan, mensegmentasi area network secara logis dan fisik dan mempunyai penjaga keamanan yaitu satpam yang berputar mengelilingi gedung (tidak hanya disatu lokasi). Hal-hal tersebut diatas merupakan prosedur perlindungan yang dapat diterapkan dengan harga yang relatif murah jika dibandingkan dengan biaya yang harus dibayar jika resiko keamanan terjadi. Hal yang diingat adalah jika mekanisme perlindungan keamanan membutuhkan biaya yang rendah tetapi keuntungannya berupa material maka mekanisme seperti ini seharusnya diimplementasi. Kunci dan gembok merupakan contoh alat proteksi yang murah, namun dapat melindungi fasilitas dan isinya dari pencuri dan pengrusakan.

5.6 Backup

Backup data sangat diperlukan khususnya jika jaringan *down*, data hilang atau korup hingga *user* dan manajemen berteriak. Tidak semua data perlu di*backup*, jadi ini penting untuk mengidentifikasi data yang kritis, penting dan dengan kata lain perlu dibuat prioritas mengenai apa yang perlu di *backup*. Saat ini *backup* data dilakukan oleh divisi TI melalui *server* jaringan.

BAB VI

KEAMANAN JARINGAN DAN TELEKOMUNIKASI

Telekomunikasi adalah transmisi data secara elektrik antar sistem baik secara analog, digital atau nirkabel. Telekomunikasi mengacu pada sistem telepon, dan penyedia layanan. Sedangkan jaringan berhubungan dengan komunikasi antar komputer, sumber daya bersama, dan penyediaan administrasi terpusat.

6.1 Peralatan Jaringan dan Telekomunikasi

Berikut ini merupakan spesifikasi komponen jaringan di PT. Kontraktor Sipil Jaya:

1. *Modem ADSL Router*, merek Prolink dengan jumlah port 1 buah.
2. *Server* jaringan, *PC Desktop* dengan prosesor *Pentium* 4 2,8 GHz, memori 1 GB, *hardisk* 80 GB, sistem operasi *Windows 2000 Server*, *CD-RW Asus* 52x24x52x, *Ethernet Card*, aplikasi *Symantec Antivirus Corporate Edition 9.0*, *Norton Internet Security 2004*, dan *Microsoft Office XP Profesional Corporate Edition*. Catatan: tidak ada *server database*.
3. Sepuluh *PC Desktop client* + 1 *Notebook*
    - Satu di ruangan direktur utama, satu di ruangan sekretaris, satu di ruangan direktur keuangan & akuntansi, satu di ruangan direktur operasi, dua untuk biro keuangan & akuntansi, satu untuk biro SDM & hukum, dan satu untuk biro logistik dan peralatan. Dengan spesifikasi *Pentium* 4 1,6 Ghz, memori 256 MB, *hardisk* 40 GB, sistem operasi *Windows 2000 client*, *CD-ROM*, *Ethernet Card*, *Symantec Antivirus Corporate Edition 9.0 for client*, *Norton Internet Security 2004 for client*, dan *Microsoft Office XP Profesional Corporate Edition.*
    - Dua untuk biro operasi dan pemasaran. Spesifikasinya *Pentium* 4 2,4 Ghz, memori

256 MB, *hardisk* 80 GB, sistem operasi *Windows 2000 client*, *CD-ROM*, *Ethernet Card*, *Symantec Antivirus Corporate Edition 9.0 for client*, *Norton Internet Security 2004 for client*, *Microsoft Office XP Profesional Corporate Edition*, *AutoCAD 2000*, dan *Microsoft Project 2000*.

- *Notebook ACER TM* 3201 *XCi Intel Pentium M Processor* 1,5 GHz, memori 521 MB, *hardisk* 60 GB, *LAN* 10/100 MBPS, sistem operasi *XP Pro*, *Symantec Antivirus Corporate Edition 9.0 for client*, *Norton Internet Security 2004 for client*, *Microsoft Office XP Profesional Corporate Edition*, *AutoCAD 2000*, dan *Microsoft Project 2000*.

4. Lima buah *Printer Laser HP Color Laserjet* 1500.
5. Satu buah *UPS* 1200 VA + 10 buah *UPS* 600 VA.
6. Tujuh buah pesawat telepon sebagai alat telekomunikasi.
7. Satu buah mesin faksimili

6.2 Keamanan Jaringan

Untuk melindungi keamanan jaringan dilakukan beberapa hal sebagai berikut:

- Administratif. Perlindungan administratif dilakukan melalui pembuatan kebijakan, prosedur, standar, dan pedoman keamanan, pelatihan keamanan bagi para pegawai, serta pengawasan oleh divisi TI dan atasan.
- Fisik. Perlindungan secara fisik dilakukan dengan meletakkan komputer *server* di ruangan tersendiri, dan pemisahan *workstation* sehingga tidak berada di satu ruangan, pemasangan *CCTV*, melakukan *backup*, alarm pencuri dan detektor asap, penambahan penerangan diwaktu malam, dan penjagaan satpam yang lebih ketat.

- Teknis. Perlindungan teknis antara lain dilakukan dengan menggunakan *router* dan *switch* yang memiliki kontrol logika untuk menjamin lalu lintas tertentu saja yang menuju segmen dalam jaringan, dan penggunaan enkripsi.

BAB VII

KRIPTOGRAFI, PENGEMBANGAN SISTEM DAN APLIKASI

Kriptografi adalah metode mengirimkan data dalam bentuk yang hanya boleh diketahui untuk yang dapat membaca dan memproses. Tujuan dari kriptografi adalah menyembunyikan informasi dari pihak-pihak luar (*intruder*) yang tidak bertanggungjawab, yang ingin mengambil isi dari informasi tersebut. Berbagai macam algoritma atau teknik kriptografi (enkripsi) bisa digunakan dalam pengiriman data. Misalnya mulai dari menggunakan algoritma konvensional, pengunaan *private key*, *public key* hingga tanda tangan digital (*digital signature*). Namun hal ini sangat tergantung pada kebutuhan dan kepentingan perusahaan dalam hal data yang dikiriman.

Dalam hal ini, perusahaan yang dikaji adalah perusahaan kontraktor dimana data-data yang ada bukanlah data transaksi seperti di Bank yang memerlukan pengamanan yang sangat kuat. Namun data-data perusahaan juga berharga tinggi bagi perusahaan. Perusahaan sudah menggunakan *digital signature* dalam pengiriman *email*, sedangkan data-data yang penting dienkripsi dengan AES.

Keamanan sistem informasi seharusnya dimulai sejak tahap pengembangan. Karena perangkat lunak dan aplikasi yang dipakai tidak dikembangkan sendiri oleh PT. Kontraktor Sipil Jaya, maka fitur keamanan ini tidak dibahas mendalam disini. Yang dapat dilakukan oleh PT. Kontraktor Sipil Jaya adalah memilih sistem atau perangkat lunak atau aplikasi yang handal, tersedia dukungan purna jualnya, dan dikembangkan terus oleh *vendor*nya.

BAB VIII

PEMULIHAN BENCANA DAN KELANGSUNGAN BISNIS

Adanya paradigma pada perusahaan bahwa bencana seperti kebakaran, gempa bumi, atau bahkan terserang virus yang membuat sistem mati (*down*) harus segera diatasi. Upaya penganggulangan ini disebut dengan istilah *Disaster Recovery Plan* dan *Contingency Plan*. Hal ini diperlukan karena bencana itu tidak dapat diprediksi sehingga perlindungan terbaik adalah membuat sebuah rencana.

Disaster Recovery Plan melibatkan pengembangan rencana dan persiapan terhadap bencana sebelum bencana itu terjadi dengan tujuan untuk meminimalkan kerugian (*loss*) dan memastikan sumber daya, orang, dan proses binis dapat berjalan sebagaimana mestinya. *Disaster Recovery Plan* disebut juga dengan tindakan pencegahan. Sedangkan *Contingency Plan* menyediakan metode dan prosedur penanganan jangka panjang setelah terjadi bencana. *Contingency Plan* disebut juga dengan tindakan korektif.

Langkah dalam membuat rencana ini adalah melakukan *Risk Assessment and Analysis* untuk mengevaluasi ancaman potential yang dapat timbul artinya daftar bencana-bencana apa saja yang bisa terjadi kemudian melakukan *Assigning Value to the Assets* yaitu perkiraan kerugian yang diakibatkan oleh ancaman tersebut. Kedua tahapan ini sudah dibahas dan dapat dilihat pada bab sebelumnya yaitu praktek manajemen keamanan.

Kemudian perlu diidentifikasi fungsi bisnis yang penting dan kriteria kerugian secara spesisifik setelah dilakukan evaluasi ancaman potensial. Fungsi bisnis yang penting dalam PT. Kontraktor Sipil Jaya adalah:

- Kegiatan operasional di bidang jasa konstruksi
- Dukungan jaringan komputer dan komunikasi

- Keuangan dan Akuntansi
- Penggajian

Sedangkan kriteria kerugian terdiri dari :

- Hilangnya atau menurunnya reputasi atau citra perusahaan dimata masyarakat
- Kerugian finansial
- Hilangnya keunggulan bersaing
- Meningkatkan pengeluaran perusahaan
- Pegawai melakukan boikot

8.1 Interdependencies

Langkah selanjutnya adalah mengidentifikasi *interrelation* dan *interdependency* yaitu pendefinisian fungsi bisnis penting dan departemen pendukung. Fungsi bisnis penting yang telah disebutkan diatas sebelumnya didukung dan dibawahi oleh departemen atau unit tertentu.

- Kegiatan Operasional di bidang jasa Konstruksi di bawah Biro Operasi, Pemasaran, Logistik dan Peralatan.
- Dukungan jaringan komputer dibawah divisi TI
- Keuangan dan Akuntansi di bawah Biro Keuangan dan Akuntansi
- Penggajian di bawah Biro SDM

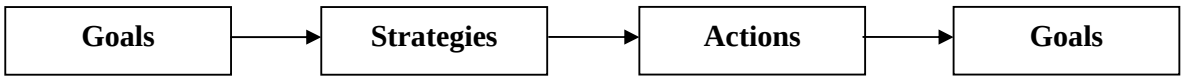
8.2 Contingency Plan Requirements

Untuk membuat *Contingency Plan*, pelu adanya dukungan dari pihak manajemen. Oleh karena itu *Contingency Plan* maupun *Disaster Recovery Plan* pada PT. Kontraktor Sipil Jaya dibuat dengan pendekatan *top-down* (*top down approach*) bukan dengan pendekatan *buttom-up* (*buttom up approach*). Kebijakan dan tujuan dari usaha perencanaan perlu dibuat oleh

pihak manajemen baik untuk *Disaster Recovery* maupun *Contingency Plan*. Sekali pihak manajemen menset tujuan dan kebijakan serta prioritas perusahaan, staf lain yang bertanggung jawab dalam rencana ini akan dapat mengisi sisanya.

8.3 Pembuatan Tujuan Contingency Plan

Membuat tujuan-tujuan adalah penting untuk semua pekerjaan, terutama untuk *Contingency Plan*. Definisi dari tujuan secara langsung membantu mengalokasikan sumber daya dan pekerjaan secara layak, mengembangkan strategi yang penting dan membantu justifikasi ekonomi dari rencana yang dibuat. Tujuan, strategi dan aksi adalah merupakan hubungan yang terintegrasi seperti tergambar pada gambar dibawah ini :



Gambar 8.1 Goals, Strategies and Actions

Untuk menghasilkan tujuan yang berguna, diperlukan kriteria tujuan yang mengandung informasi kunci sebagai berikut :

1. Tanggung jawab dari setiap individu dalam situasi *chaotic*. Tanggung jawab setiap individu dicantumkan secara eksplisit dalam prosedur menghadapi bencana.
2. Otoritas. Perlunya diketahui orang yang bertanggung jawab khususnya jika terjadi krisis. Kerja tim sangat dibutuhkan disini dan tim dapat melakukan ini jika adanya pemimpin yang dipercaya. Dalam menghadapi bencana, setiap manajer pada biro menjadi koordinator anggota bironya masing-masing.
3. Prioritas. Prioritas yang umum perlu dibuat oleh manajemen jika terjadi krisis. Hal ini menyangkut fungsionalitas mana yang ada dalam organisasi termasuk dalam kategori kritis yang berarti perusahaan akan sangat merugi jika fungsionalitas itu tidak berjalan

dalam hitungan hari dan fungsionalitas mana yang termasuk dalam kategori *nice to have* yang berarti perusahaan dapat hidup tanpanya dalam waktu 1 minggu atau 2 minggu jika terjadi bencana. Prioritas juga harus dicantumkan dalam prosedur menghadapi bencana atau krisis.

4. Testing dan Implementasi. Sekali *Disaster Recovery Plan* dan *Contingency Plan* dikembangkan, ini harus dilakukan. Rencana ini juga perlu didokumentasikan dan diletakkan pada tempat yang secara mudah dapat diakses jika terjadi krisis serta orang yang telah diserahi tugas perlu diajarkan dan diinformasikan.

Ada enam langkah pendekatan untuk *contingency planning* yang dapat diberikan sebagai berikut :

1. Indentifikasi fungsionalitas bisnis yang kritis. Pada tahap ini akan dilihat proritas dari funsionalitas bisnis yang ada bagi perusahaan. Bagi PT. Kontraktor Sipil Jaya, proritas dari fungsionalitas bisnis yang ada dalam perusahaan adalah :
    1.1 Data operasional proyek karena pada data tersebut melibatkan data-data untuk keperluan tender dan pelaksanaan proyek. Jika fungsional ini *down*, maka perusahaan kehilangan data atau tidak bisa mengolah data untuk pengajuan tender dan pelaksanaan proyek.
    1.2 Dukungan sistem informasi yang digunakan untuk menjaga agar kondisi jaringan perusahaan sehingga pekerjaan operasional bisa dilakukan.
    1.3 Keuangan dan akuntansi karena digunakan untuk mengelola perhitungan laba rugi perusahaan.
    1.4 Penggajian dianggap penting karena digunakan untuk mengelola pembayaran gaji karyawan perusahaan.
2. Identifikasi sistem dan sumber daya yang diperlukan untuk mendukung fungsi-fungsi kritis sebagai berikut :

Fungsi-Fungsi Kritis	Teknologi Informasi	Personil (Sumber Daya Manusia)
Pengolahan data operasional	Sistem Komputer	A01, A03, A010, A011, A016-A021.
Dukungan jaringan	Sistem Komputer	A06 dan A07
Keuangan dan Akuntansi	Sistem Komputer	A01, A02, A08, A012, A013
Penggajian	Sistem Komputer	A01, A02, A09, A014

Gambar 8.1 Goals, Strategies and Actions

3. Memperkirakan bencana dan ancaman potensial. Hal ini telah dijelaskan pada bab sebelumnya.
4. Pemilihan Strategi Perencanaan. *Disaster Recovery Plan* dan *Contingency Plan* akan terdiri dari *emergency response*, *recovery* dan *resumption activities*. *Emergency response* berhubungan dengan melindungi hidup dan mengurangi dampak kerusakan (praktek manajemen keamanan), *recovery* mencakup langkah-langkah yang penting untuk mengembalikan fungsi-fungsi kritis kembali berjalan. Sedangkan *resumption* merupakan tindakan untuk mengembalikan perusahaan kembali pada operasional (keduanya bisa memanfaatkan dana asuransi).
5. Implementasi Strategi. Setelah penentuan strategi, hal tersebut perlu didokumentasikan.
6. Test dan Revisi Perencanaan. *Disaster Recovery Plan* dan *Contingency Plan* harus diuji secara periodik karena lingkungan terus berubah dan menimbulkan kebutuhan perbaikan. Oleh karena itu rencana-rencana tesebut harus diuji secara terus-menerus supaya perbaikan yang timbul dapat diatasi.

Rencana pemulihan bencana (*disaster recovery plan)* dan kelangsungan bisnis (*contingency plan*) adalah sebagai berikut:

1. Apabila terjadi bencana seperti kebakaran, banjir, atau gempa bumi, maka setiap pegawai harus menjalankan prosedur keamanan menghadapi bencana untuk menyelamatkan aset

perusahaan. Koordinasi diatur oleh setiap manajer pada biro. Berkaitan dengan bencana ini, prioritas keselamatan utama tetap terletak pada nyawa manusia.

2. Gangguan putusnya layanan Internet dalam jangka waktu yang lama harus diatasi dengan menggunakan telkomnet@instan.
3. Apabila bencana yang terjadi mengakibatkan kantor tidak dapat dipergunakan, maka aktivitas perusahaan dihentikan sementara. Semua aset informasi disimpan di rumah direktur utama, sedangkan peralatan pekerjaan konstruksi disimpan secara tersebar di rumah direktur dan manajer yang lain. Kegiatan administratif dilakukan di rumah direktur utama. Komunikasi dengan konsumen harus segera dibangun kembali dari rumah direktur utama. Pegawai lainnya dirumahkan untuk sementara. Oleh karena itu, direktur utama harus secepatnya mengadakan kembali fasilitas fisik dengan menggunakan dana asuransi.

BAB IX

HUKUM, INVESTIGASI, DAN ETIKA

Teknologi informasi yang sangat berkembang seperti *e-commerce* dan *online business* saat ini berhadapan dengan berbagai macam serangan. Hal ini tentu saja membutuhkan hukum, kebijakan dan metode untuk menangkap *bad guys* dan memaksanya untuk membayar kerusakan yang disebabkan. Beberapa hal mengenai bab ini sudah disinggung pada kebijakan penggunaan komputer. Hukum yang dapat dijadikan acuan dalam penggunaan teknologi informasi adalah undang-undang *cyberlaw*.

Etika didasarkan pada berbagai masalah dan pondasi yang berbeda. Etika dapat relatif berbeda terhadap situasi yang berbeda dari individu ke individu. Dalam perusahaan sebenarnya ada kode-kode etik yang harus dipatuhi namun tidak tertulis. Menurut *ISC Code of Ethics* dapat dituliskan beberapa kode etik, yaitu:

- Bertingkah laku jujur, wajar, legal dan melindungi lingkungan.
- Bekerja secara rajin dan menyediakan layanan yang kompeten terhadap keamanan.
- Mendukung perkembangan penelitian.
- Hindari berbagai konflik, hargai kepercayaaan orang lain yang diberikan padamu dan kerjakan pekerjaaan yang hanya sesuai dengan kualifikasimu.
- dan sebagainya

Perusahaan dalam hal ini PT. Kontraktor Sipil Jaya harus mempunyai panduan berupa etika bisnis dan komputer, yang dituangkan dalam kebijakan keamanan perusahaan. Panduan ini dapat dimasukkan sebagai bagian dari *employee handbook*, digunakan dalam orientasi, dikirim dan merupakan bagian dari sesi pelatihan. Etika komputer yang dikeluarkan oleh *The Computer Ethics Institue* yang merupakan organisasi non profit yang bekerja untuk melihat

perkembangan teknologi dari sudut pandang etika dapat disarankan untuk menjadi panduan bagi perusahaan khususnya dalam penggunaan komputer. *Computer Ethics Institute* ini juga adalah kumpulan ilmuwan komputer yang peduli akan dampak perkembangan teknologi komputer terhadap masyarakat. Ada 10 hal yang dianjurkan oleh institut tersebut sebagai berkut :

1. Jangan menggunakan komputer untuk menyakiti orang.
2. Jangan mencampuri pekerjaan komputer orang lain
3. Jangan melihat atau mengambil berkas komputer orang lain.
4. Jangan menggunakan komputer untuk mencuri.
5. Jangan menggunakan komputer untuk menyebar berita bohong.
6. Jangan menggandakan atau menggunakan perangkat lunak *proprietary* jika kamu belum membayarnya.
7. Jangan menggunakan sumber daya komputer orang lain tanpa izin atau kompensasi orang tersebut.
8. Jangan mendekati atau meniru hasil karya intelektual orang lain.
9. Pikirkan tentang konsekuensi sosial dari program yang dibuat atau sistem yang dirancang
10. Gunakan komputer dalam cara yang menjamin konsiderasi dan penghargaan dari orang lain.

BAB X

KEAMANAN OPERASI DAN AUDIT SISTEM INFORMASI

Keamanan operasi berkenaan dengan semua hal yang ada untuk menjaga agar jaringan, sistem komputer, dan lingkungan hidup dan berjalan dengan perlindungan dan cara yang aman.

10.1 Aspek-aspek Keamanan Operasi

Berikut ini akan dibahas aspek-aspek yang berkaitan dengan keamanan operasi di PT. Kontraktor Sipil Jaya.

- Dari sisi manajemen administratif, pelaksanaan pemisahan tanggung jawab dan rotasi pekerjaan belum dilakukan karena jumlah pegawai untuk suatu jabatan masih sedikit.
- Apabila terjadi perubahan konfigurasi jaringan, parameter sistem, dan *setting* karena adanya penambahan teknologi baru, konfigurasi sistem, peralatan, maka semuanya direncanakan dulu oleh Kepala Divisi TI dan rencana perubahan diberitahukan kepada pihak-pihak yang berkepentingan. Perubahan selalu dilakukan pada akhir minggu dan setelah pegawai lain pulang kerja.
- Pengawasan harian terhadap sistem dan peralatan jaringan dilakukan oleh divisi TI. Pengawasan tersebut mencakup pemeriksaan kondisi fisik, pembuatan *check list* yang harus diisi pengguna mengenai pembaharuan *database* virus, pembuatan *check list* yang diisi oleh divisi TI sendiri mengenai pelaksanaan *backup* data, pengawasan terhadap pelaksanaan kebijakan, prosedur, standar, dan pedoman keamanan perusahaan. Selain divisi TI, pengawasan juga dilakukan oleh divisi SDM terhadap satpam, pesuruh,

resepsionis karena mereka juga merupakan bagian dari lingkungan sistem.

- Untuk penggunaan Internet, yaitu pengiriman dan penerimaan *email* untuk keperluan perusahaan sudah menggunakan *digital signature*. Penggunaan *email* hanya diperbolehkan bagi direktur, sekretaris, kepala divisi TI dan manajer. Keamanan *email* dari virus sepenuhnya mengandalkan program anti virus. Koneksi Internet dipantau oleh divisi TI, dan akan dimatikan apabila jam kerja kantor sudah usai. Gangguan terhadap jaringan dari serangan luar selama ini masih bisa ditangani, dan frekuensinya juga relatif rendah. Pegawai lainnya menggunakan Internet untuk meng*update* program komputer.

10.2 Audit Sistem Informasi

Pelaksanaan audit sistem informasi di PT. Kontraktor Sipil Jaya selama ini masih menggunakan auditor eksternal. Dari sisi perusahaan sendiri, persiapan audit dan pelaksanaannya merupakan tanggung jawab divisi TI.

BAB XI

KESIMPULAN

Kegiatan bisnis utama PT. Kontraktor Sipil Jaya adalah jasa konstruksi. Sistem informasi di PT. Kontraktor Sipil Jaya digunakan sebagai pendukung untuk melakukan kegiatan operasional perusahaan. Tindakan pengamanan yang dilakukan cukup menonjol mencakup pengamanan secara fisik, pembuatan kebijakan keamanan, dan perlindungan jaringan dengan menggunakan program *Anti Virus* dan program *Internet Security*. Memang belum semua domain keamanan sistem informasi dilakukan dengan baik, karena disesuaikan juga dengan kebutuhan perusahaan. Arsitektur jaringan perusahaan juga masih sangat sederhana. Penggunaan Internet masih sekedar untuk pengiriman dan penerimaan email, serta *update* program. Belum ada pengiriman atau penerimaan data yang dilakukan melalui Internet.

DAFTAR PUSTAKA

Harris, Shon. 2002. CISS All-in-One Certification Exam Guide. California: McGraw-Hill/Orborne.

Penerapan Segitiga Pengaman *Aspek Penting Melindungi Sistem Teknologi*. Kompas, Senin, 16 Agustus 2004.

New Zealand Security of Information Technology Publication 101. Information Technology Security Policy Handbook Chapter 3 Asset Classification and Control.

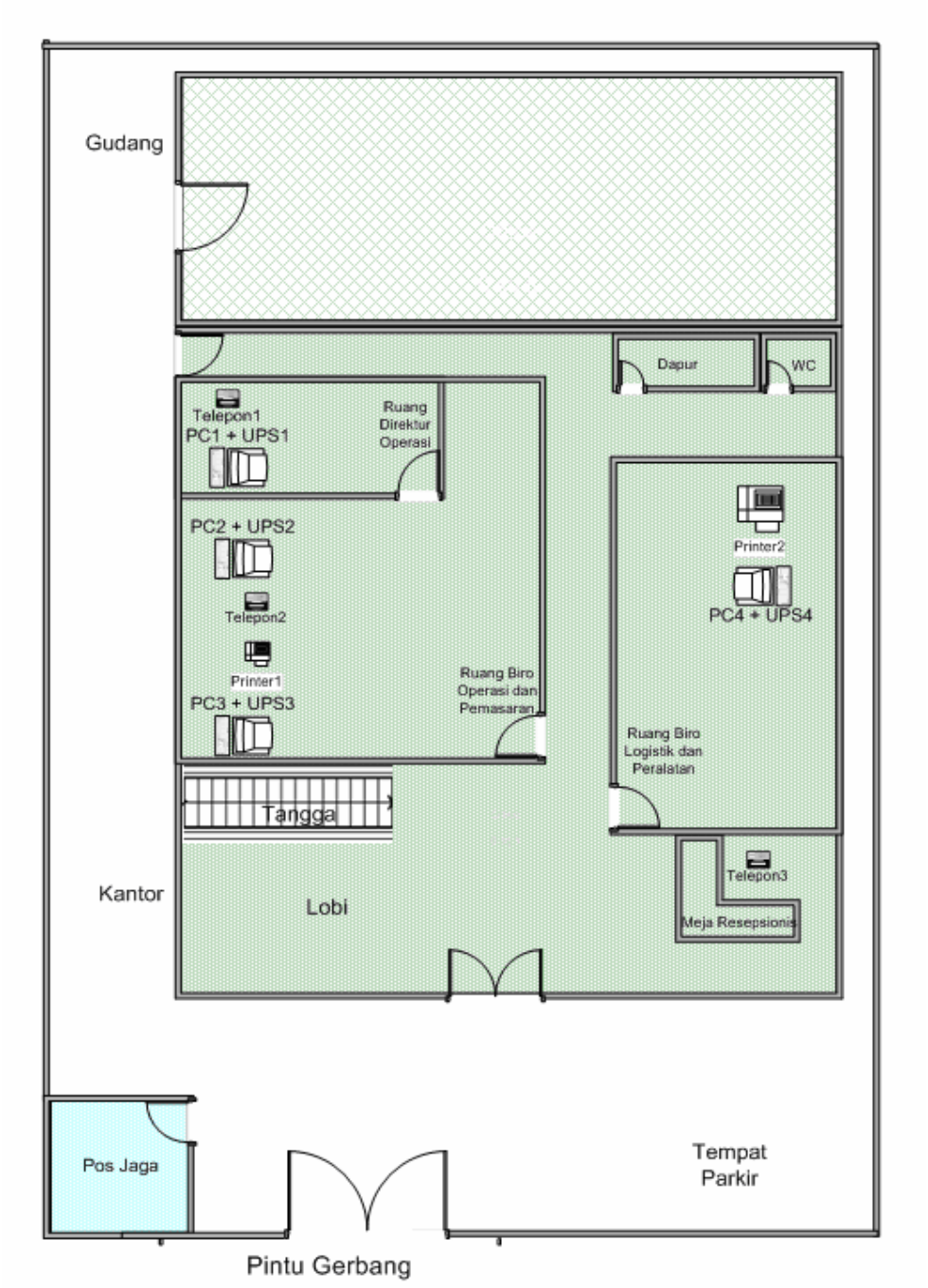
Peraturan Pemerintah Republik Indonesia Nomor 28 Tahun 2000 Tentang Usaha dan Peran Masyarakat Jasa Konstruksi

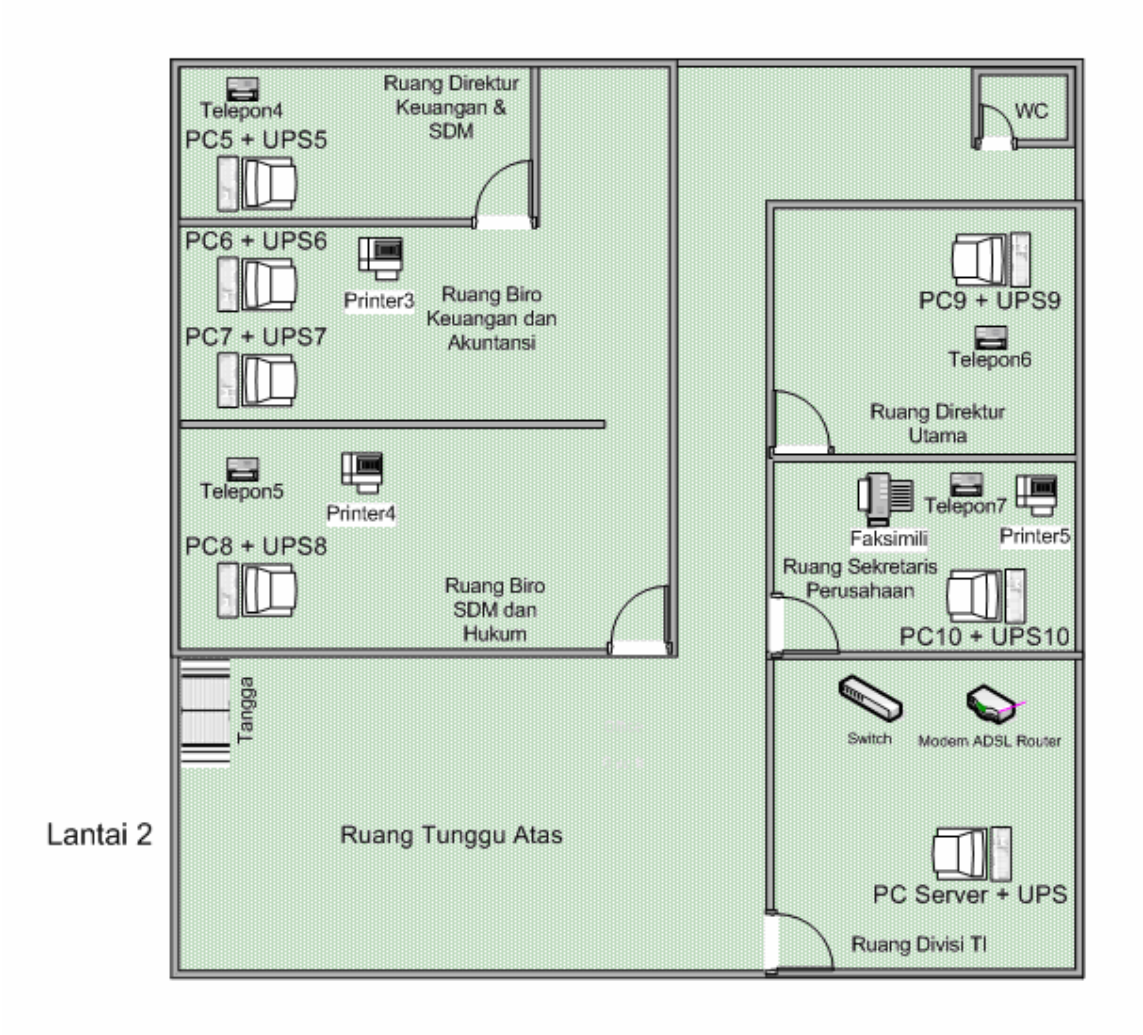
Lembaga Pengembangan Jasa Konstruksi. http://www.lpjk.or.id/

The SANS Security Policy Project. http://www.sans.org/resources/policies/

LAMPIRAN

A. Tata Ruang dan Lokasi Perangkat Komputer





B. Contoh Isi Dokumen Kebijakan, Prosedur, Standar, dan Pedoman

---

KEBIJAKAN PENGGUNAAN KOMPUTER

A. Tujuan

Tujuan dari kebijakan ini adalah sebagai garis besar cara penggunaan komputer yang diperkenankan di PT. Kontraktor Sipil Jaya. Aturan-aturan ini dibuat untuk melindungi pegawai dan PT. Kontraktor Sipil Jaya. Penggunaan yang tidak benar menghadapkan PT. Kontraktor Sipil Jaya terhadap resiko serangan virus, membahayakan sistem dan layanan jaringan, dan masalah-masalah hukum.

B. Ruang Lingkup

Kebijakan ini ditujukan bagi semua pegawai PT. Kontraktor Sipil Jaya, termasuk pihak-pihak lain yang memiliki kepentingan. Kebijakan ini diterapkan pada semua peralatan yang dimiliki atau disewa PT.

Kontraktor Sipil Jaya.

C. Kebijakan

C.1 Penggunaan Umum dan Kepemilikan

1. Oleh karena administrator jaringan PT. Kontraktor Sipil Jaya menghendaki adanya tingkat kerahasiaan yang layak, para pengguna harus sadar bahwa data yang mereka buat pada sistem komputer perusahaan merupakan milik PT. Kontraktor Sipil Jaya. Karena adanya kebutuhan melindungi jaringan komputer PT. Kontraktor Sipil Jaya, pihak manajemen tidak dapat menjamin kerahasiaan informasi pribadi yang disimpan disetiap peralatan jaringan yang dimiliki PT. Kontraktor Sipil Jaya.
2. Pegawai bertanggung jawab untuk melatih penilaiannya secara baik berkaitan dengan kelayakan alasan penggunaan komputer secara pribadi. Biro SDM bertanggung jawab untuk membuat pedoman berkenaan dengan penggunaan komputer dan Internet secara pribadi. Jika ada aspek-aspek yang tidak jelas atau tidak tertulis dan dianggap dapat menimbulkan kesalahpahaman, pegawai harus bertanya kepada biro SDM.
3. Semua informasi yang sensitif atau rawan sesuai dengan klasifikasi yang sudah ditetapkan perusahaan atau menurut pemahaman pengguna harus dienkripsi.
4. Untuk tujuan keamanan dan pemeliharaan jaringan, individu yang diberi wewenang oleh PT. Kontraktor Sipil Jaya dapat memonitor peralatan, sistem dan lalu lintas jaringan setiap saat.
5. PT. Kontraktor Sipil Jaya berhak untuk memeriksa jaringan dan sistem pada periode-periode tertentu untuk menjamin pelaksanaan kebijakan ini.

C.2 Keamanan dan Informasi *Proprietary*

1. Antar muka pengguna dengan informasi yang berada di jaringan harus diklasifikasikan menurut kerahasiaannya, seperti ditetapkan oleh pedoman kerahasiaan perusahaan. Contoh dari informasi rahasia antara lain: data keuangan, data konsumen, strategi perusahaan, rahasia dagang, termasuk rancangan gambar konstruksi. Para pegawai harus mengambil langkah yang diperlukan untuk mencegah pihak-pihak yang tidak berhak mengakses informasi-informasi ini.
2. Jaga *password* dan jangan berbagi *account*. Para pengguna yang diberi wewenang bertanggung jawab atas keamanan *account* dan *password*-nya. *Password* sistem harus diganti dua minggu, sedangkan *password* pengguna harus diganti setiap satu bulan.
3. Semua *PC* dan *notebook* harus diberi *screensaver* dengan *password* pelindung yang aktif secara otomatis setiap 10 menit, atau melalui *log off* bila pengguna meninggalkan komputer.
4. Gunakan enkripsi untuk informasi sesuai dengan kebijakan penggunaan enkripsi.
5. Karena informasi yang berada di *notebook* sangat rawan, maka diperlukan penanganan khusus.

6. Semua *PC* dan *notebook* yang dipakai pengguna yang terhubung dengan jaringan internet PT. Kontraktor Sipil Jaya, baik milik pegawai pribadi maupun PT. Kontraktor Sipil Jaya harus memasang perangkat lunak anti virus dengan *database* virus yang terbaru.
7. Pegawai harus memiliki kewaspadaan yang tinggi ketika membuka *email* yang mengandung *attachment* dari pengirim yang tidak dikenal, yang mungkin berisi virus, *email bomb*, atau *trojan horse*.

C.3 Penggunaan yang Tidak Diperkenankan

Aktivitas-aktivitas berikut secara umum dilarang. Para pegawai dapat dibebaskan dari larangan ini selama dalam bagian tanggung jawab pekerjaan mereka (misalnya administrator jaringan mungkin perlu memutuskan akses jaringan suatu *host*, jika *host* tersebut melakukan aktivitas yang mencurigakan). Bagaimanapun juga seorang pegawai PT. Kontraktor Sipil Jaya tidak diberi wewenang untuk ikut serta dalam aktvitas yang ilegal menurut undang-undang di Indonesia dengan menggunakan sumber daya PT. Kontraktor Sipil Jaya.

Daftar dibawah ini bermaksud memberikan suatu kerangka untuk aktivitas-aktivitas yang termasuk dalam kategori penggunaan yang tidak diperkenankan.

Aktivitas-aktivitas Jaringan dan Sistem

Aktivitas-aktivitas berikut secara tegas dilarang, tanpa kecuali:

1. Pelanggaran hak individu atau perusahaan yang dilindungi oleh hak cipta, rahasia dagang, paten atau hak intelektual lainnya, atau peraturan atau hukum yang mirip, termasuk, tapi tidak terbatas pada, instalasi atau distribusi produk bajakan atau perangkat lunak lainnya yang tidak memiliki izin untuk penggunaan oleh PT. Kontraktor Sipil Jaya.
2. Penggandaan tanpa hak terhadap material dengan hak cipta, termasuk, tapi tidak terbatas pada, digitasi dan distribusi foto dari majalah, buku, atau sumber lain dengan hak cipta, lagu dengan hak cipta, dan instalasi perangkat lunak apapun yang mempunyai hak cipta dimana PT. Kontraktor Sipil Jaya atau pengguna tidak memiliki izin, secara tegas dilarang.
3. Memasukkan program-program jahat (*malicious*) kedalam jaringan atau *server* (seperti virus, *worm*, *trojan horse*, *email bomb*, dan lain-lain).
4. Mengungkapkan *password* kepada orang lain atau memperbolehkan penggunaan *account* oleh orang lain. Ini termasuk keluarga atau anggota keluarga lainnya ketika pekerjaan kantor dikerjakan di rumah.
5. Menggunakan komputer PT. Kontraktor Sipil Jaya untuk secara aktif terlibat dalam mendapatkan atau mengirimkan materi-materi yang mengandung unsur pornografi.
6. Memberikan layanan atau barang secara curang dengan membawa nama PT. Kontraktor Sipil Jaya.

7. Melakukan pembobolan atau gangguan keamanan terhadap komunikasi jaringan. Pembobolan jaringan mencakup, tapi tidak terbatas pada, mengakses data yang bukan haknya atau masuk kedalam *server* atau *account* yang bukan miliknya, kecuali pekerjaan ini masuk dalam daftar pekerjannya. Sedangkan yang termasuk dalam gangguan keamanan, tapi tidak terbatas pada, *network sniffing*, *pinged floods*, *packet spoofing*, *denial of service*, dan menyebarkan informasi palsu untuk tujuan yang jahat.
8. *Port* atau *network scanning* secara tegas dilarang kecuali masuk dalam daftar pekerjaannya.
9. Melakukan pemantauan jaringan dalam bentuk apapun yang akan menangkap data yang tidak ditujukan padanya, kecuali masuk dalam daftar pekerjaannya.
10. Mengelakkan autentikasi pengguna atau keamanan suatu *host*, jaringan, atau *account*.
11. Menginterfensi atau meniadakan layanan kepada pengguna lain.
12. Menggunakan program/*script*/perintah, atau mengirimkan pesan dalam bentuk apapun, dengan maksud mencampuri atau memutuskan sesi pengguna lain dengan cara lokal maupun melalui Internet.
13. Menyediakan informasi mengenai, atau daftar, pegawai PT. Kontraktor Sipil Jaya kepada pihak-pihak diluar PT. Kontraktor Sipil Jaya.

Aktivitas-aktivitas Komunikasi dan Email

1. Mengirimkan pesan-pesan *email* yang tidak diminta, termasuk pengiriman *junk mail* atau materi-materi *advertising* kepada individu yang tidak memintanya.
2. Segala bentuk ganggunan melalui *email*, telepon/hp/pager, apakah melalui perkataan, frekuensi, atau ukuran pesan.
3. Penggunaan yang tidak memiliki izin, atau pemalsuan informasi *header email*.
4. Membuat atau meneruskan surat berantai.

D. Penegakan

Setiap pegawai yang ditemukan melanggar kebijakan ini dapat dikenakan tindakan pendisiplinan hingga pemberhentian kerja.

E. Definisi

- Virus adalah program yang mencari program lain dan menginfeksinya dengan menempelkan salinannya. Ketika program yang terinfeksi dieksekusi, virus yang tertempel ikut tereksekusi, sehingga menyebarkan infeksi.

- *Worm* adalah program yang dapat memperbanyak diri sendiri, tidak seperti virus, dan menyebar melalui *email*, TCP/IP, dan *disk drives*.

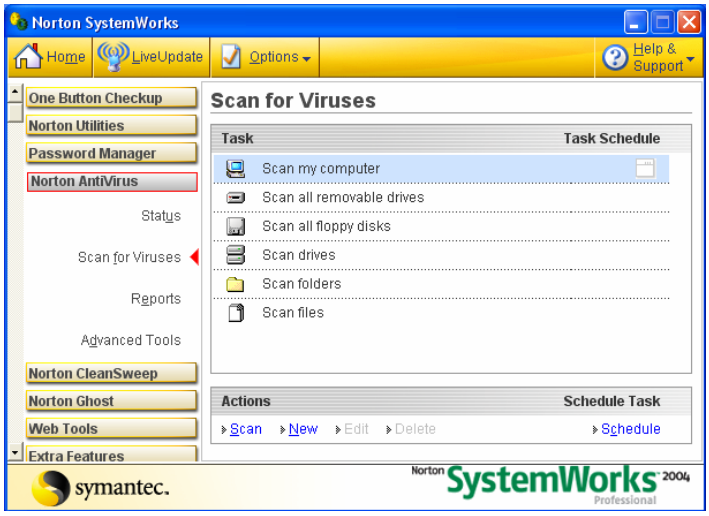
F. Histori Revisi

Versi 1 dibuat tanggal 21 Desember 2004 disetujui Dewan Direksi.

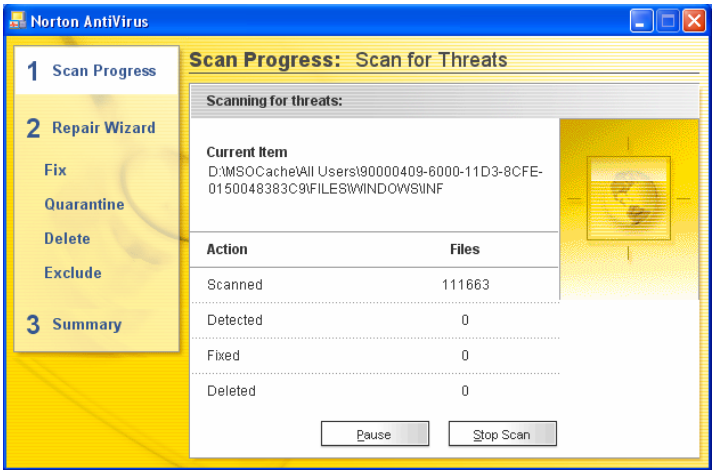
PROSEDUR MELAKUKAN SCAN VIRUS

Dokumen ini menggambarkan proses untuk melakukan pemeriksaan/scan virus.

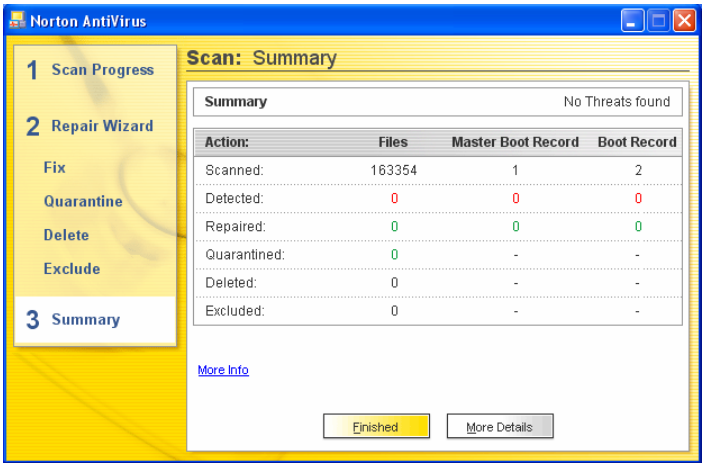
1. Buka aplikasi *Norton SystemWorks*.
2. Pilih *Norton AntiVirus* > *Scan for Viruses* > *Scan my computer*



3. Klik *scan*
4. Akan muncul tampilan berikut, tunggu hingga proses scan berakhir.



5. Apabila proses *scan* sudah selesai, pilih "*fix*" jika ditemui adanya virus atau pilih "*finished*" bila tidak ada.



6. Hubungi divisi TI bila perlu bantuan.

STANDAR ENKRIPSI

Semua informasi konsumen dalam database harus dienkripsi dengan algoritma *AES* dan dikirim dengan teknologi enkripsi *digital signature*.

PEDOMAN PENCEGAHAN VIRUS

Tindakan yang direkomendasikan untuk mencegah masalah virus:

- Selalu perbaharui database virus yang bisa di*download* dari Internet.
- Selalu jalankan standar perangkat lunak anti virus perusahaan secara teratur.
- Jangan buka *attachment* suatu email dari pengirim yang tidak diketahui, mencurigakan, atau sumber yang tidak dapat dipercaya. Hapus *email/attachment* ini segera, kemudian kosongkan *recycle bin*.
- Hapus *spam* dan *junk email*.
- Jangan men*download* files dari sumber yang tidak dikenal atau mencurigakan.
- Hindari pembagian disk secara langsung dengan akses tulis kecuali ada kebutuhan bisnis yang mengharuskan.
- Periksa semua disket dengan perangkat lunak anti virus.
- Buat cadangan data dan konfigurasi sistem secara teratur dan simpan ditempat yang aman

C. Access Control Matrix dan Access Control Lists (ACL)

Access Control Matrix untuk *file 1 – file 12*

No.	Subjek	Jabatan	File 1	File 2	File 3	File 4	File 5	File 6	File 7	File 8	File 9	File 10	File 11	File 12
1.	A01	Direktur Utama	R	R	R	R	R	R	R	R	R	R	R	R
2.	A02	Direktur Keuangan dan SDM	RW	RW	RW	RW	R	R	R	R	R	R	R	R
3.	A03	Direktur Operasi	R	R	R	R	RW	R	R	R	R	R	R	R
4.	A04	Sekretaris Perusahaan	NA	NA	NA	NA	RW	RW	NA	NA	R	NA	NA	NA
5.	A05	Staf Sekretaris Perusahaan	NA	NA	NA	NA	RW	RW	NA	NA	R	NA	NA	NA
6.	A06	Kepala Divisi TI	NA	NA	NA	NA	NA	NA	RW	RW	RW	NA	NA	NA
7.	A07	Staf Divisi TI	NA	NA	NA	NA	NA	NA	RW	RW	RW	NA	NA	NA
8.	A08	Manajer Keuangan & Akuntansi	RW	RW	RW	R	R	NA	NA	NA	R	NA	NA	NA
9.	A09	Manajer SDM & Hukum	R	R	R	RW	RW	NA	NA	NA	R	NA	NA	NA
10.	A010	Manajer Operasi & Pemasaran	R	R	R	NA	RW	NA	NA	NA	R	R	R	R
11.	A011	Manajer Logistik & Peralatan	NA	NA	NA	NA	NA	NA	NA	NA	R	RW	RW	R
12.	A012	Staf Divisi Keuangan	RW	RW	RW	R	R	NA	NA	NA	R	NA	NA	NA
13.	A013	Staf Divisi Akuntansi	RW	RW	RW	R	R	NA	NA	NA	R	NA	NA	NA
14.	A014	Staf Divisi SDM	NA	NA	NA	RW	NA	NA	NA	NA	R	NA	NA	NA
15.	A015	Staf Divisi Hukum	NA	NA	NA	NA	RW	NA	NA	NA	R	NA	NA	NA
16.	A016	Staf Divisi Arsitektur	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R

17.	A017	Staf Divisi Mekanikal	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
18.	A018	Staf Divisi Elektrikal	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
19.	A019	Staf Divisi Pemasaran	NA	NA	NA	NA	NA	NA	NA	NA	R	NA	NA	NA
20.	A020	Staf Divisi Logistik	NA	NA	NA	NA	NA	NA	NA	NA	R	RW	R	R
21.	A021	Staf Divisi Peralatan	NA	NA	NA	NA	NA	NA	NA	NA	R	R	RW	R
22.	A022	Kepala Proyek	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
23.	A023	Kepala Proyek	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
24.	A024	Kepala Kontruksi	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
25.	A025	Kepala Kontruksi	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
26.	A026	Kepala Bagian Proyek	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
27.	A027	Kepala Bagian Proyek	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
28.	A028	Kepala Urusan Keuangan	NA	NA	NA	NA	NA	NA	NA	NA	R	R	NA	NA
29.	A029	Kepala Urusan Arsitektur	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
30.	A030	Kepala Urusan Mekanikal	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
31.	A031	Kepala Urusan Elektrikal	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
32.	A032	Kepala Urusan Logistik	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
33.	A033	Kepala Urusan Peralatan	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
34.	A034	Staf Urusan Keuangan	NA	NA	NA	NA	NA	NA	NA	NA	R	R	NA	NA
35.	A035	Staf Urusan	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R

		Arsitektur												
36.	A036	Staf Urusan Arsitektur	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
37.	A037	Staf Urusan Mekanikal	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
38.	A038	Staf Urusan Mekanikal	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
39.	A039	Staf Urusan Elektrikal	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
40.	A040	Staf Urusan Elektrikal	NA	NA	NA	NA	NA	NA	NA	NA	R	R	R	R
41.	A041	Staf Urusan Logistik	NA	NA	NA	NA	NA	NA	NA	NA	R	RW	R	R
42.	A042	Staf Urusan Peralatan	NA	NA	NA	NA	NA	NA	NA	NA	R	R	RW	R
43.	A043	Juru Gambar Arsitektur	NA	NA	NA	NA	NA	NA	NA	NA	R	NA	NA	RW
44.	A044	Juru Gambar Mekanikal	NA	NA	NA	NA	NA	NA	NA	NA	R	NA	NA	RW
45.	A045	Juru Gambar Elektrikal	NA	NA	NA	NA	NA	NA	NA	NA	R	NA	NA	RW
46.	A046	Resepsionis	NA	NA	NA	NA	NA	NA	NA	NA	R	NA	NA	NA
47.	A047	Pesuruh	NA	NA	NA	NA	NA	NA	NA	NA	R	NA	NA	NA
48.	A048	Supir Perusahaan	NA	NA	NA	NA	NA	NA	NA	NA	R	NA	NA	NA
49.	A049	Satpam	NA	NA	NA	NA	NA	NA	NA	NA	R	NA	NA	NA
50.	A050	Satpam	NA	NA	NA	NA	NA	NA	NA	NA	R	NA	NA	NA

Keterangan:
R = Read-Only, A = Append (Only Write), E = Execute (cannot read and write), RW = Read-Write, NA = No Access
File 1 = Neraca.xls, File 2 = Laba Rugi.xls, File 3 = Akuntansi.xls, File 4 = Gaji Pegawai.xls, File 5 = Kontrak Proyek.doc, File 6 = Surat Masuk dan Keluar.doc, File 7 = Inventaris Jaringan.xls, File 8 = HW dan SW setting.doc, File 9 = Keamanan.doc, File 10 = Logistik.xls, File 11 = Peralatan.db, File 12 = Gambar Konstruksi.dwg

ACL untuk *PC*1

No.	Pengguna	
1.	A03	*Full Control*
2.	A06	*Full Control* dengan ijin A03
3.	A07	*Full Control* dengan ijin A03
4.	Lainnya	*No Access*

ACL untuk *PC*2 dan *PC*3

No.	Pengguna	
1.	A010	*Full Control*
2.	A016	*Full Control*
3.	A017	*Full Control*
4.	A018	*Full Control*
5.	A019	*Full Control*
6.	A043	*Full Control*
7.	A044	*Full Control*
8.	A045	*Full Control*
9.	A06	*Full Control* dengan ijin A010
10.	A07	*Full Control* dengan ijin A010
11.	Lainnya	*No Access*

ACL untuk *PC*4

No.	Pengguna	
1.	A011	*Full Control*
2.	A020	*Full Control*
3.	A021	*Full Control*
4.	A06	*Full Control* dengan ijin A011
5.	A07	*Full Control* dengan ijin A011
6.	Lainnya	*No Access*

ACL untuk *PC*5

No.	Pengguna	
1.	A02	*Full Control*
2.	A06	*Full Control* dengan ijin A02
3.	A07	*Full Control* dengan ijin A02
4.	Lainnya	*No Access*

ACL untuk *PC*6 dan *PC*7

No.	Pengguna	
1.	A08	*Full Control*

2.	A012	*Full Control*
3.	A013	*Full Control*
4.	A06	*Full Control* dengan ijin A08
5.	A07	*Full Control* dengan ijin A08
6.	Lainnya	*No Access*

ACL untuk *PC*8

No.	**Pengguna**	
1.	A09	*Full Control*
2.	A014	*Full Control*
3.	A015	*Full Control*
4.	A06	*Full Control* dengan ijin A09
5.	A07	*Full Control* dengan ijin A09
6.	Lainnya	*No Access*

ACL untuk *PC*9

No.	**Pengguna**	
1.	A01	*Full Control*
2.	A06	*Full Control* dengan ijin A01
3.	A07	*Full Control* dengan ijin A01
4.	Lainnya	*No Access*

ACL untuk *PC*10

No.	**Pengguna**	
1.	A04	*Full Control*
2.	A05	*Full Control*
3.	A06	*Full Control* dengan ijin A04
4.	A07	*Full Control* dengan ijin A04
5.	Lainnya	*No Access*

ACL untuk *Notebook*

No.	**Pengguna**	
1.	A022	*Full Control*
2.	A023	*Full Control*
3.	A026	*Full Control* dengan ijin A022 atau A023
4.	A027	*Full Control* dengan ijin A022 atau A023
5.	A06	*Full Control* dengan ijin A022 atau A023
6.	A07	*Full Control* dengan ijin A022 atau A023
7.	Lainnya	*No Access*

ACL untuk *PC Server*, *Switch*, dan Modem ADSL Router

No.	Pengguna	
1.	A06	*Full Control*
2.	A07	*Full Control*
3.	Lainnya	*No Access*

ACL untuk Printer1

No.	Pengguna	
1.	A03	*Print*
2.	A010	*Print*
3.	A016	*Print*
4.	A017	*Print*
5.	A018	*Print*
6.	A019	*Print*
7.	A043	*Print*
8.	A044	*Print*
9.	A045	*Print*
10.	Lainnya	*No Access*

ACL untuk Printer2

No.	Pengguna	
1.	A011	*Print*
2.	A020	*Print*
3.	A021	*Print*
4.	Lainnya	*No Access*

ACL untuk Printer3

No.	Pengguna	
1.	A02	*Print*
2.	A08	*Print*
3.	A012	*Print*
4.	A013	*Print*
5.	Lainnya	*No Access*

ACL untuk Printer4

No.	Pengguna	
1.	A09	*Print*
2.	A014	*Print*
3.	A015	*Print*
4.	Lainnya	*No Access*

ACL untuk Printer5

No.	Pengguna	
1.	A01	*Print*
2.	A04	*Print*
3.	A05	*Print*
4.	Lainnya	*No Access*

ACL untuk Telepon1

No.	Pengguna	
1.	A03	*Full Control*
2.	Lainnya	*No Access*

ACL untuk Telepon2

No.	Pengguna	
1.	A010	*Full Control*
2.	A016	*Full Control*
3.	A017	*Full Control*
4.	A018	*Full Control*
5.	A019	*Full Control*
6.	A043	*Full Control*
7.	A044	*Full Control*
8.	A045	*Full Control*
9.	Lainnya	*No Access*

ACL untuk Telepon3

No.	Pengguna	
1.	A046	*Full Control*
2.	Lainnya	*No Access*

ACL untuk Telepon4

No.	Pengguna	
1.	A02	*Full Control*
2.	Lainnya	*No Access*

ACL untuk Telepon5

No.	Pengguna	
1.	A08	*Full Control*
2.	A09	*Full Control*

3.	A012	*Full Control*
4.	A013	*Full Control*
5.	A014	*Full Control*
6.	Lainnya	*No Access*

ACL untuk Telepon6

No.	**Pengguna**	
1.	A01	*Full Control*
2.	Lainnya	*No Access*

ACL untuk Telepon7

No.	**Pengguna**	
1.	A04	*Full Control*
2.	A05	*Full Control*
3.	Lainnya	*No Access*

ACL untuk Faksimili

No.	**Pengguna**	
1.	A04	*Full Control*
2.	A05	*Full Control*
3.	Lainnya	*No Access*