

Draft Makalah

Proteksi dan Teknik Keamanan Sistem Informasi

Studi Kasus: PT. OraKelar



Disusun Oleh :

Alex Ferdinansyah (7203010049)

Yudo Budi Pramono (7203012319)

Robertus Nursuksma (7203012211)

Setyo Kuncoro (7203012246)

DAFTAR ISI

BAB 1 PENDAHULUAN	4
1.1 Pengantar	4
1.2 Profil Perusahaan	4
BAB 2 PRAKTEK MANAJEMEN KEAMANAN	9
2.1 Manajemen Resiko	9
2.1.1 <i>Identifikasi Aset</i>	9
2.1.2 <i>Analisa Resiko</i>	17
2.1.3 <i>Penanggulangan Resiko</i>	23
2.2 Kebijakan Keamanan	27
2.2.1 <i>Kebijakan</i>	28
2.2.2 <i>Prosedur</i>	31
2.2.3 <i>Standar</i>	31
2.2.4 <i>Pedoman</i>	31
2.3 Pendidikan Keamanan	32
BAB 3 AKSES KONTROL	33
3.1 Identifikasi, Autentikasi, Autorisasi, dan Akuntabilitas.....	33
3.1.1 <i>Identifikasi</i>	33
3.1.2 <i>Autentikasi</i>	34
3.1.3 <i>Autorisasi</i>	34
3.1.4 <i>Akuntabilitas</i>	40
BAB 4 KEAMANAN FISIK	41
4.1 Manajemen Fasilitas	41
4.2 Konstruksi	42
4.3 Ruang Komputer.....	42
4.4 Security Must	42
4.5 Security Should	42
4.6 Backup	43
BAB 5 KEAMANAN JARINGAN DAN TELEKOMUNIKASI	44

5.1	Peralatan Jaringan dan Telekomunikasi	44
5.2	Keamanan Jaringan	45
BAB 6 PEMULIHAN BENCANA DAN KELANGSUNGAN BISNIS		46
6.1	Interdependencies	47
6.2	Contingency Plan Requirements	47
6.3	Pembuatan Tujuan Contingency Plan	47

BAB 1

PENDAHULUAN

1.1 Pengantar

Keamanan komputer tidak dapat dilepaskan dari pengembangan sistem secara keseluruhan, namun masih banyak pengembang dan organisasi yang belum menyadari pentingnya hal tersebut. Ketersediaan informasi yang diperlukan pada saat yang tepat, dengan isi informasi yang benar, penyajian informasi pada pihak yang berhak menjadi tugas dari keamanan sistem informasi.

Ketersediaan informasi dengan karakteristik diatas dapat dicapai apabila sebuah organisasi memiliki pengetahuan mengenai domain keamanan sistem informasi. Makalah ini bertujuan untuk membahas keamanan sistem informasi sebuah organisasi UKM pada sebelas domain keamanan yang ada. Domain keamanan yang akan dibahas adalah praktek manajemen keamanan, metodologi dan sistem kontrol akses, arsitektur dan model keamanan, keamanan fisik, keamanan jaringan, kriptografi, pemulihan bencana dan kelangsungan bisnis, hukum investigasi dan etika, pengembangan sistem dan aplikasi serta audit dan jaminan.

1.2 Profil Perusahaan

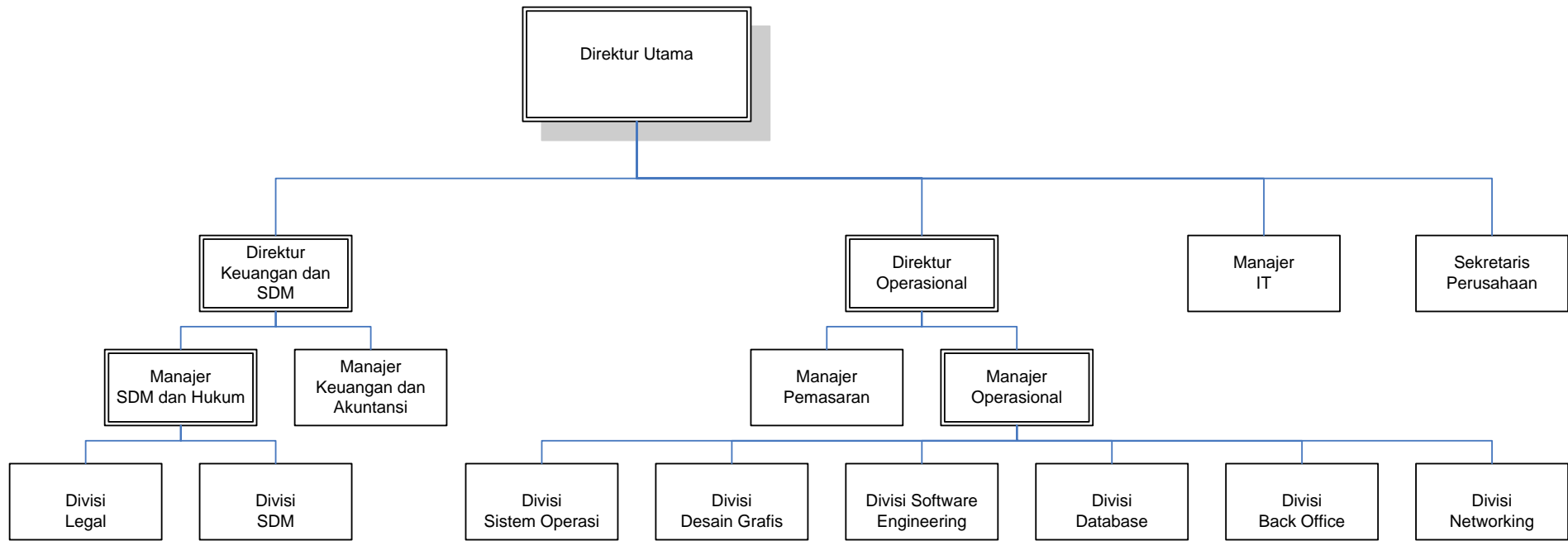
LPK OraKelar merupakan sebuah lembaga yang berdiri pada tahun 1994 dan berlokasi di Jakarta. Lembaga ini memiliki sebuah kantor pusat yang merangkap menjadi tempat pelatihan utama.

Pada mulanya perusahaan ini hanya memfokuskan diri pada pelatihan perangkat lunak yang dibutuhkan oleh kalangan pelajar, seperti aplikasi office, dan bahasa pemrograman Visual Basic. Visi dari lembaga ini adalah menyediakan sarana pelatihan yang berkualitas dengan menekankan pada penguasaan konsep dan praktek pada kasus dunia nyata. Visi yang cukup unik ini didukung jaringan kerjasama dengan beberapa perusahaan konsultan IT lokal yang bersedia melakukan *outsourcing* SDM kepada peserta LPK OraKelar. Selama masa praktek peserta akan dibantu oleh para pengajar untuk menyelesaikan proyek tersebut. Keuntungan yang didapat peserta adalah kesempatan belajar sambil bekerja dengan kemungkinan memperoleh imbalan riil dari perusahaan IT yang bersangkutan

Bertambahnya tenaga pengajar yang berkualitas dan berhasilnya jalinan kerjasama antara LPK ini dengan beberapa vendor IT dan perusahaan konsultan IT lokal membuat LPK

OraKelar membuka beberapa kelas baru untuk menambah kelas yang lama. Beberapa materi yang diajarkan mencakup pelatihan perangkat lunak, pelatihan desain web/grafis, pelatihan jaringan, pelatihan operating system, pelatihan back office, dan pelatihan database.

Segmen pasar dari LPK OraKelar adalah para profesional IT, kalangan pelajar dan masyarakat umum. Pelatihan memiliki jangka waktu yang bervariasi serta pembagian level yang menentukan derajat penguasaan dari peserta. Pada akhir pelatihan, LPK OraKelar juga menawarkan ujian sertifikasi untuk masing-masing bidang, hal ini bisa dilakukan setelah LPK OraKelar menjalin kerja sama dengan pihak-pihak penyedia jasa sertifikasi profesional IT seperti Inixindo dan Balicamp.



No	Nama	Jabatan
1	A01	Direktur Utama
2	A02	Direktur Keuangan dan SDM
3	A03	Direktur Operasional
4	A04	Manajer Keuangan dan Akuntansi
5	A05	Manajer SDM dan Hukum
6	A06	Manajer Operasional
7	A07	Manajer Marketing
8	A08	Manajer IT
9	A09	Staff Keuangan
10	A10	Staff Keuangan
11	A11	Staff Accounting
12	A12	Staff Accounting
13	A13	Staff Payroll
14	A14	Staff Payroll
15	A15	Staff Legal
16	A16	Staff Legal
17	A17	Staff Marketing Corporate
18	A18	Staff Marketing Public
19	A19	Staff Pengajar Software Engineering
20	A20	Staff Pengajar Software Engineering
21	A21	Staff Pengajar Software Engineering
22	A22	Staff Pengajar Desain Grafis
23	A23	Staff Pengajar Desain Grafis
24	A24	Staff Pengajar Desain Grafis
25	A25	Staff Pengajar Sistem Operasi
26	A26	Staff Pengajar Sistem Operasi
27	A27	Staff Pengajar Sistem Operasi
28	A28	Staff Pengajar Networking
29	A29	Staff Pengajar Networking
30	A30	Staff Pengajar Networking
31	A31	Staff Pengajar Database
32	A32	Staff Pengajar Database
33	A33	Staff Pengajar Database
34	A34	Staff Pengajar Back Office
35	A35	Staff Pengajar Back Office
36	A36	Staff Pengajar Back Office
37	A37	Staff IT - Jaringan
38	A38	Staff IT - Jaringan
39	A39	Staff IT - Database
40	A40	Staff IT - Administrator
41	A41	Sekretaris Direksi
42	A42	Sekretaris Umum
43	A43	Resepsionis
44	A44	Resepsionis
45	A45	Satpam
46	A46	Satpam
47	A47	Satpam
48	A48	Satpam
49	A49	Pesuruh
50	A50	Pesuruh
51	A51	Pesuruh
52	A52	Sopir

Penjelasan singkat mengenai tugas masing-masing:

Dewan Direksi

Bertanggung jawab dalam mengelola PT. OraKelar antara lain dengan merumuskan strategi dan kebijakan, memelihara dan mengelola aset, serta memastikan perkembangan pencapaian hasil dan tujuan usaha. Komposisi Dewan Direksi terdiri dari Direktur Utama, Direktur Keuangan dan SDM, dan Direktur Operasional.

Direktur Utama

Bertanggung jawab memimpin dan mengendalikan serta memberikan petunjuk kepada para Direktur dan pegawai dalam rangka melaksanakan keputusan Direksi.

Direktur Keuangan dan SDM

Bertugas membantu Direktur Utama dalam memimpin dan mengendalikan kegiatan pengelolaan keuangan dan akuntansi, sumber daya manusia, dan aspek hukum perusahaan.

Direktur Operasional

Bertugas membantu Direktur Utama dalam memimpin dan mengendalikan kegiatan operasional dan pemasaran.

Sekretaris Perusahaan

Berfungsi sebagai penghubung antara PT. OraKelar 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.

Manajer IT

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.

Resepsionis

Mempunyai tugas menerima telepon yang masuk, menerima tamu, dan mengantarkan tamu.

Satpam

Bertugas menjaga keamanan di PT. OraKelar dan mengelola parkir.

Sopir

Mempunyai tugas mengantar dan menjemput pimpinan pegawai PT. OraKelar dalam rangka tugas kantor.

Office Boy

Mempunyai tugas membersihkan kantor dan peralatannya, membuat minuman, melayani permintaan pimpinan dan pegawai PT. Orakelar.

BAB 2

PRAKTEK MANAJEMEN KEAMANAN

Manajemen Keamanan dalam suatu organisasi, memiliki tujuan untuk melindungi data organisasi dan menjaga nilai dari data atau informasi perusahaan tersebut. Faktor yang sangat penting dijaga dalam perlindungan data/informasi tersebut adalah: *Confidentiality* (Kerahasiaan data), *Integrity* (Integritas atau Keutuhan data) dan *Availability* (Ketersediaan) data/informasi.

Untuk mencapai tujuan dari Praktek Manajemen Keamanan tersebut ada langkah-langkah yang harus diambil yang merupakan tanggung jawab dari Manajer. Langkah-langkah tersebut akan dijelaskan lebih rinci seperti berikut, bagaimana PT OraKelar melakukan Praktek Manajemen Keamanan pada perusahaannya.

2.1 Manajemen Resiko

Aspek pertama dari Manajemen Keamanan adalah Manajemen Resiko, bagaimana perusahaan melakukan tindakan-tindakan untuk meminimalisir kemungkinan terjadinya resiko pada aset perusahaan atau bagaimana perusahaan melakukan *recovery* setelah terjadinya suatu *disaster* besar maupun kecil. Menghilangkan sama sekali resiko terhadap suatu aset perusahaan adalah tidak mungkin.

2.1.1 Identifikasi Aset

Dalam melakukan Manajemen Resiko, kita harus melakukan identifikasi dan membuat suatu daftar yang berisi dari semua aset perusahaan. Identifikasi ini juga berguna untuk mengetahui resiko apa saja yang mungkin dialami oleh suatu aset perusahaan dengan jenis tertentu.

Berikut adalah daftar aset milik PT OraKelar:

Sebuah Gedung Kantor Pusat dimana semua kegiatan administrasi dan kegiatan pengajaran dilakukan. Gedung kantor memiliki 3 tingkat dengan tiap lantai memiliki luas 10 x 16 m persegi dengan pembagian sebagai berikut:

Lantai I:

4 ruang kelas dengan ukuran 4 x 5 m persegi

Ruang Receptionist

Lantai II:

Ruang Kantor Staff dan Pengajar, sebuah *hall* berukuran 4 x 10 m persegi yang dibagi-bagi dengan kubikal.

Lab Komputer dengan ukuran 4 x 10 M persegi.

Ruang *Server* dengan ukuran 4 x 4 m persegi.

Lantai III:

Ruang Direktur Utama dengan ukuran 4 x 5 m persegi.

Ruang Direktur Keuangan & SDM dengan ukuran 4 x 4 m persegi.

Ruang Direktur Operasional dengan ukuran 4 x 4 m persegi.

Ruang Manager I, merupakan kantor dari Manager SDM & Hukum, Manager Keuangan & Akuntansi dan Manajer Pemasaran. Ukuran ruangan ini adalah 3 x 8 m persegi.

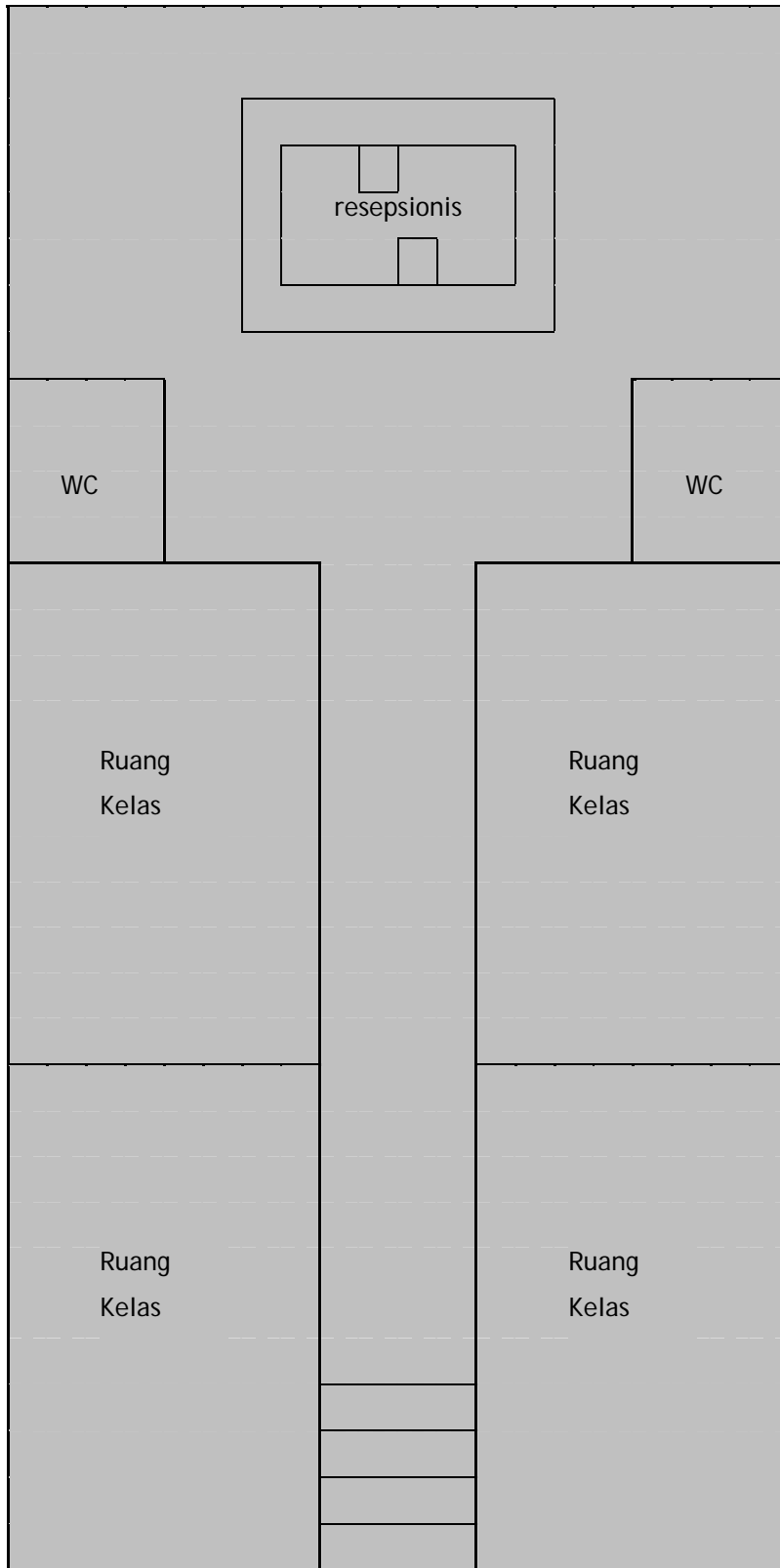
Ruang Manager II, kantor dari Manager Operasional dan Manager IT. Ukuran ruangan ini adalah 3 x 8 m persegi.

Ruang *meeting* besar dengan ukuran 6 x 5 m persegi.

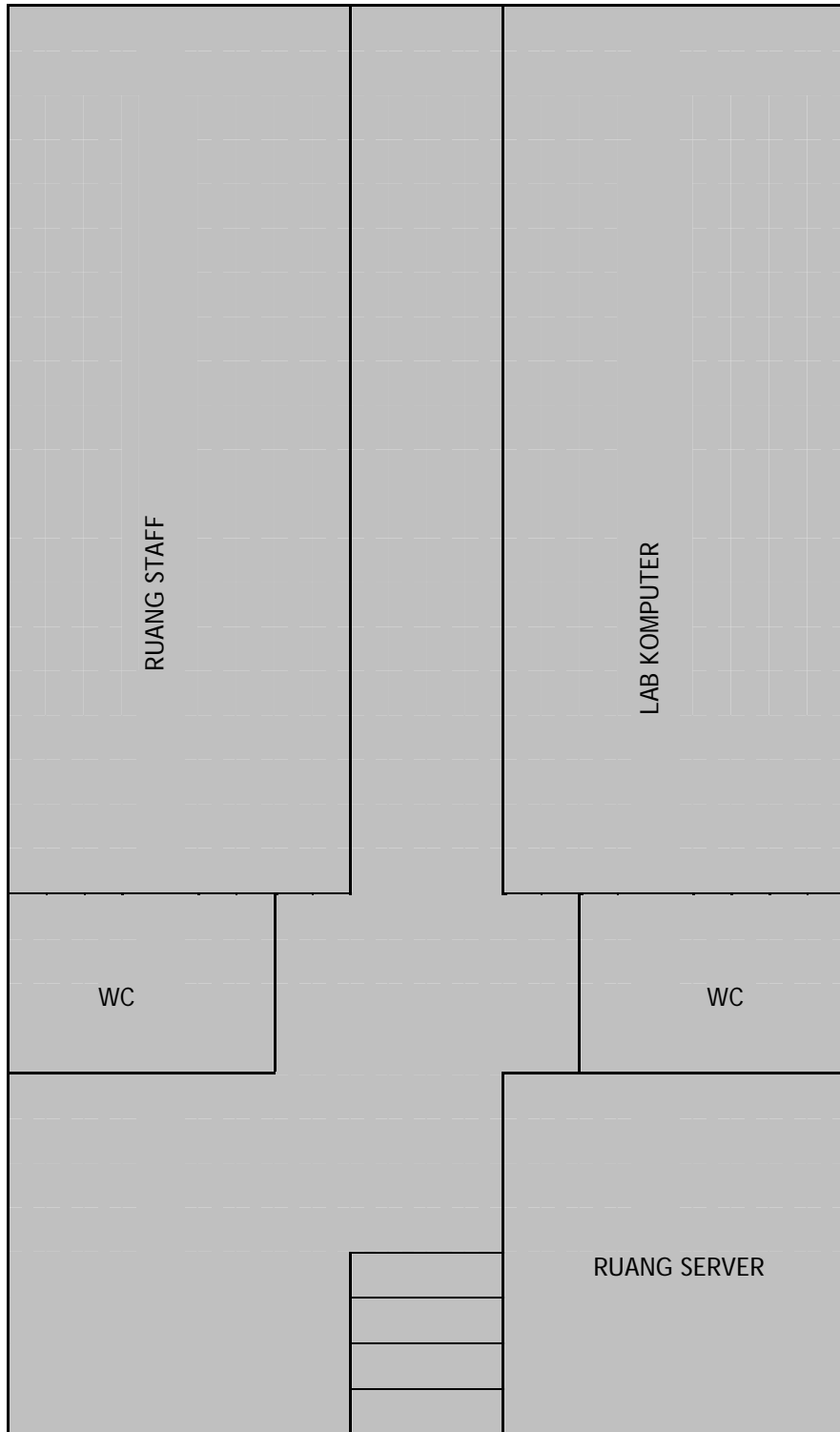
Ruang *meeting* kecil dengan ukuran 3 x 5 m persegi.

Dengan skema per lantai sebagai berikut:

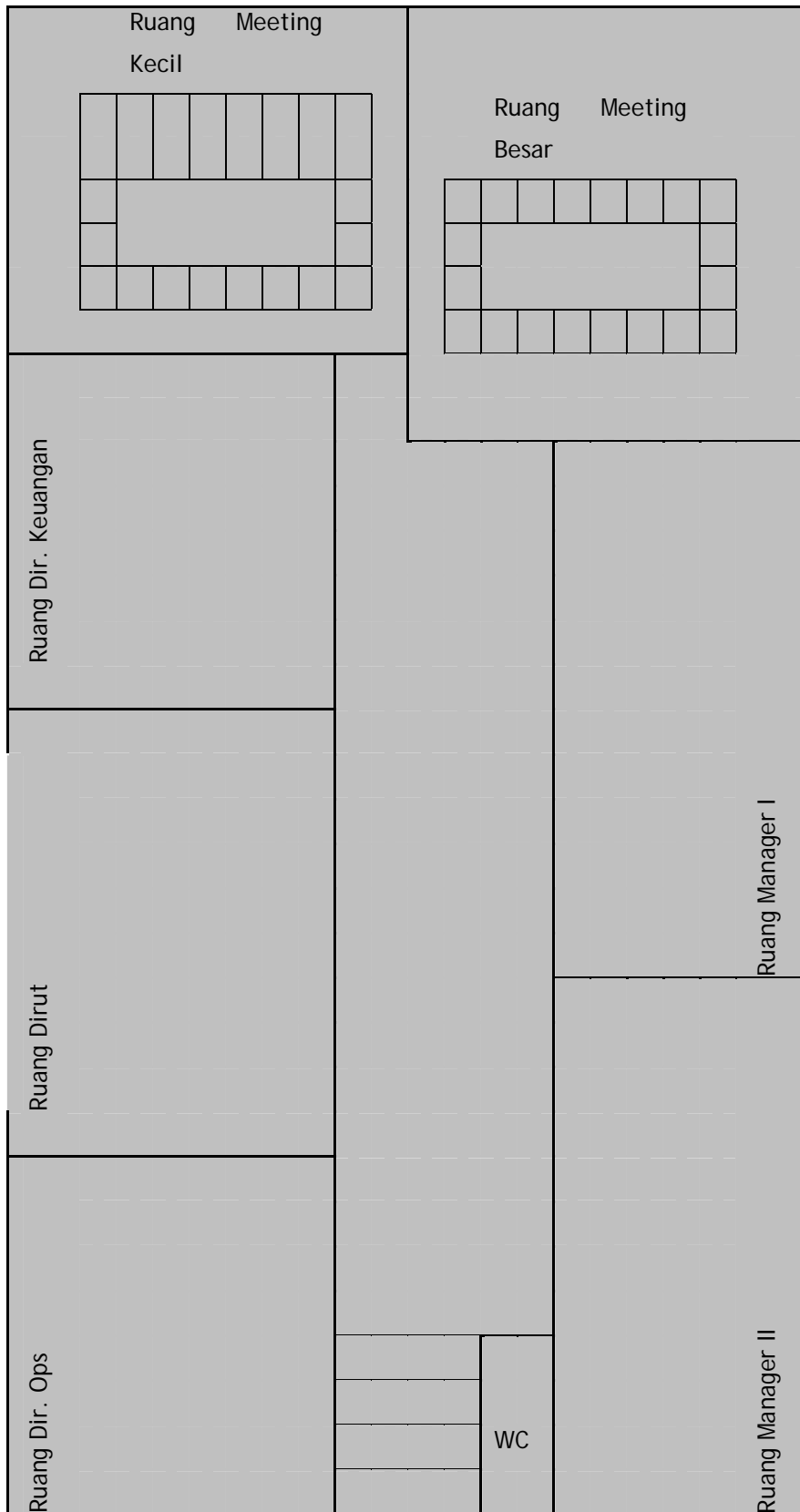
Lantai I



Lantai II



Lantai III



Aset lain selain gedung:

No	Item	Jml	Keterangan	Lokasi	Nilai Satuan
2	ADSL Router 1 Port	1		Ruang Server	2,500,000
3	Switch 32 Port	2	Melayani PC di Lantai 1 dan 2	Ruang Server	12,000,000
4	Switch 32 Port	2	Melayani PC Ruang LAB dan Kelas	Ruang Server	12,000,000
5	Server Database	1	P4, HDD: 240Gb, Mem: 1GB	Ruang Server	15,000,000
6	Server Aplikasi dan Web	1	P4, HDD: 120Gb, Mem: 1GB	Ruang Server	13,000,000
7	Server Mail dan Domain Controller	1	P4, HDD: 120Gb, Mem: 1GB	Ruang Server	13,000,000
8	Gateway Server dan Firewall	1	P4, HDD: 100Gb, Mem: 2GB	Ruang Server	13,000,000
9	PC Karyawan Staff + OS	32	P4, HDD: 80Gb, Mem: 128Mb	Ruang Kantor It II	4,000,000
10	PC Manager + OS	5	P4, HDD: 80Gb, Mem: 128Mb	Ruang Manager Masing- masing	4,000,000
11	PC Sekretaris + OS	2	P4, HDD: 80Gb, Mem: 128Mb	Lt III	4,000,000
12	Notebook + OS	3	P4, HDD: 80Gb, Mem: 128Mb	Masing- masing direktur	15,000,000
13	PC Kelas + OS	4	P4, HDD: 80Gb, Mem: 128Mb	Masing- masing Kelas, Lt I	4,000,000

14	PC Lab + OS	50	P4, HDD: 80Gb, Mem: 128Mb	Lab Lt II	4,000,000
15	Printer Siswa	2	Laser	Lab Lt II	1,000,000
16	Printer Karyawan	2	Laser	Ruang Karyawan Lt II	2,000,000
17	UPS 1200Watt	1	Untuk Server	Ruang Server	16,000,000
18	UPS 1200Watt	10	Untuk PC Karyawan	Ruang Kerja Lt II & Lt III	16,000,000
19	Integrated LAN	1	seluruh gedung	Seluruh Gedung	5,000,000
20	Pesawat Telpon	20		Lt I, II, III	100,000
21	Facsimili	1		Ruang Kerja Lt II	1,000,000
22	PABX	1		Ruang Server	10,000,000
23	Nomor Telepon	4			5,000,000
24	Layanan Internet ADSL	1			12,000,000
25	Software untuk pengajaran				30,000,000
26	Data				20,000,000

2.1.2 Analisa Resiko

Dari daftar hasil identifikasi aset diatas, kita dapat melanjutkan Manajemen Resiko dengan melakukan Analisa Resiko, yaitu mengidentifikasi Resiko dan menilai kerusakan dan frekuensi kerusakan yang mungkin terjadi pada tiap aset kita. Dari analisa ini diharapkan kita bisa

mendapatkan perbandingan kuantitatif antara aset kita dengan tanpa perlindungan (manajemen resiko) dengan aset kita dengan penjagaan bila terjadi resiko yang kita perkirakan akan terjadi.

Dengan begitu analisa ini bisa menjadi justifikasi kita dalam melakukan investasi dalam manajemen resiko ini.

Dalam analisa resiko ini, kita dibantu dengan analisa:

SLE (Single Lost Expectancy)

Kerugian Finansial yang muncul dalam terjadi satu kali disaster (Resiko):

$SLE = \text{Asset Value} \times \text{Exposure Factor}$

Exposure Factor: Persentasi kerugian yang kemungkinan dialami dalam SATU kali bencana.

ARO (Annualized Rate of Occurance)

Frekuensi resiko terjadi diperkirakan dalam satu tahun.

Misal: Diperkirakan akan terjadi banjir besar 6 tahun sekali, maka ARO: 1/6

Misal: Diperkarak terjadi pemutusan hubungan listrik 12 kali setahun, ARO: 12

ALE (Annualized Lost Expectancy)

$ALE = SLE \times ARO$

No	Item	Jml	Keterangan	Nilai Satuan	Nilai Total	Klasifikasi	Resiko	EF (%)	SLE	ARO	ALE
1	Gedung	1		5,000,000,000	5,000,000,000	Fisik	Kebakaran	50	2,500,000,000	0.0250	62,500,000
2	ADSL Router Port	1		2,500,000	2,500,000	Fisik	Pencurian	100	2,500,000	0.2500	625,000
3	Switch Port	32	Melayani PC di Lantai 1 dan 2	12,000,000	24,000,000	Fisik	Pencurian	50	12,000,000	0.2500	3,000,000
4	Switch Port	32	Melayani PC Ruang LAB dan Kelas	12,000,000	24,000,000	Fisik	Pencurian	50	12,000,000	0.2500	3,000,000
5	Server Database	1	P4, HDD: 240Gb, Mem: 1GB	15,000,000	15,000,000	Fisik	Pencurian	100	15,000,000	0.2500	3,750,000
6	Server Aplikasi dan Web	1	P4, HDD: 120Gb, Mem: 1GB	13,000,000	13,000,000	Fisik	Pencurian	100	13,000,000	0.2500	3,250,000
7	Server Mail dan Domain Controllor	1	P4, HDD: 120Gb, Mem: 1GB	13,000,000	13,000,000	Fisik	Pencurian	100	13,000,000	0.2500	3,250,000
8	Gateway	1	P4, HDD:	13,000,000	13,000,000	Fisik	Pencurian	100	13,000,000	0.2500	3,250,000

	Server dan Firewall		100Gb, Mem: 2GB								
9	PC Karyawan Staff + OS	32	P4, HDD: 80Gb, Mem: 128Mb	4,000,000	128,000,000	Fisik	Pencurian	70	89,600,000	0.3333	29,866,667
10	PC Manager + OS	5	P4, HDD: 80Gb, Mem: 128Mb	4,000,000	20,000,000	Fisik	Pencurian	100	20,000,000	0.3333	6,666,667
11	PC Sekretaris + OS	2	P4, HDD: 80Gb, Mem: 128Mb	4,000,000	8,000,000	Fisik	Pencurian	50	4,000,000	0.3333	1,333,333
12	Notebook + OS	3	P4, HDD: 80Gb, Mem: 128Mb	15,000,000	45,000,000	Fisik	Pencurian	100	45,000,000	0.5000	22,500,000
13	PC Kelas + OS	4	P4, HDD: 80Gb, Mem: 128Mb	4,000,000	16,000,000	Fisik	Pencurian	20	3,200,000	0.3333	1,066,667
14	PC Lab + OS	50	P4, HDD: 80Gb,	4,000,000	200,000,000	Fisik	Pencurian	50	100,000,000	0.3333	33,333,333

			Mem: 128Mb								
15	Printer Siswa	2	Laser	1,000,000	2,000,000	Fisik	Pencurian	50	1,000,000	0.3333	333,333
16	Printer Karyawan	2	Laser	2,000,000	4,000,000	Fisik	Pencurian	50	2,000,000	0.3333	666,667
17	UPS 1200Watt	1	Untuk Server	16,000,000	16,000,000	Fisik	Pencurian	20	3,200,000	0.3333	1,066,667
18	UPS 1200Watt	10	Untuk PC Karyawan	16,000,000	160,000,000	Fisik	Pencurian	20	32,000,000	0.3333	10,666,667
19	Integrated LAN	1	seluruh gedung	5,000,000	5,000,000	Fisik	Rusak	75	3,750,000	0.2000	750,000
20	Pesawat Telpon	20		100,000	2,000,000	Fisik	Pencurian	50	1,000,000	0.5000	500,000
21	Facsimili	1		1,000,000	1,000,000	Fisik	Pencurian	40	400,000	0.5000	200,000
22	PABX	1		10,000,000	10,000,000	Fisik	Pencurian	50	5,000,000	0.3333	1,666,667
23	Nomor Telepon	4		5,000,000	20,000,000	Layanan	Putus	50	10,000,000	4.0000	40,000,000
24	Layanan Internet ADSL	1		12,000,000	12,000,000	Layanan	Putus	75	9,000,000	6.0000	54,000,000
25	Software untuk pengajaran	1		30,000,000	30,000,000	Software	Virus\Worm	50	15,000,000	2.0000	30,000,000

26	Data Layanan	1	20,000,000	20,000,000	data	Virus\Worm	70	14,000,000	2.0000	28,000,000
27	Listrik	1	60,000,000	60,000,000	Layanan	Putus	70	42,000,000	4.0000	168,000,000
Total Kerugian Per tahun										513,241,667

2.1.3 Penanggulangan Resiko

Dari daftar resiko diatas, kita dapat melakukan grouping beerdasarkan jenis resiko seperti dibawah ini, ranking tertinggi dari kerugian perusahaan akibat pencurian.

Pencurian

Berikut detaidari kerugian akibat pencurian:

No	Item	Jml	Resiko	ALE
1	ADSL Router 1 Port	1	Pencurian	625,000
2	Switch 32 Port	2	Pencurian	3,000,000
3	Switch 32 Port	2	Pencurian	3,000,000
4	Server Database	1	Pencurian	3,750,000
5	Server Aplikasi dan Web	1	Pencurian	3,250,000
6	Server Mail dan Domain Controller	1	Pencurian	3,250,000
7	Gateway Server dan Firewall	1	Pencurian	3,250,000
8	PC Karyawan Staff + OS	32	Pencurian	29,866,667
9	PC Manager + OS	5	Pencurian	6,666,667
10	PC Sekretaris + OS	2	Pencurian	1,333,333
11	Notebook + OS	3	Pencurian	22,500,000
12	PC Kelas + OS	4	Pencurian	1,066,667

13	PC Lab + OS	50	Pencurian	33,333,333
14	Printer Siswa	2	Pencurian	333,333
15	Printer Karyawan	2	Pencurian	666,667
16	UPS 1200Watt	1	Pencurian	1,066,667
17	UPS 1200Watt	10	Pencurian	10,666,667
18	Pesawat Telpon	20	Pencurian	500,000
19	Facsimili	1	Pencurian	200,000
20	PABX	1	Pencurian	1,666,667
Total Kerugian Per tahun				129,991,667

Dengan kerugian sebesar 130 juta per tahun, patutlah perusahaan mengambil langkah-langkah untuk mengurangi resiko terjadinya kecurian. Berikut langkah-langkah yang diambil oleh pihak manajemen PT OraKelar dalam memperkecil kemungkinan resiko terjadinya pencurian aset perusahaan:

Penambahan dua orang anggota satuan keamanan pada shift malam, menjadi 3 orang. Sedang pada shift pagi dan sore, tetap masing-masing satu orang satpam.

Penambahan fasilitas keamanan konvensional. Antara lain pemasangan teralis besi pada tiap jendela dan penambahan pintu teralis besi pada pintu masuk dari luar.

Pemasangan kamera digital di tiap lantai untuk merekam siapa saja orang yang masuk kedalam gedung. Kamera akan dipasang di ujung lorong tiap lantai. Kamera ini akan merekam setiap terjadi pergerakan di lorong dan langsung merekam gambar yang langsung disimpan kedalam server aplikasi di ruang server.

Perusahaan mulai mengasurnasikan asetnya pada sebuah perusahaan asuransi terkemuka.

Berikut rincian minimalisasi resiko pencurian:

No	Kegiatan penanggulangan pencurian	Jumlah	Biaya per tahun	Biaya Resiko per tahun
1	Penambahan anggota	2 orang	8,000,000	

	Satpam			
2	Teralis besi di tiap jendela dan gerbang	1 set	20,000,000	
3	Kamera digital di tiap lantai	3 buah	15,000,000	
4	Asuransi Aset		1,000,000	
			44,000,000	129,991,667

Kebakaran

Resiko kebakaran yang diperkirakan akan dialami oleh PT OraKelar adalah 62,5 juta pertahun.

No	Item	Jml	Resiko	ALE
1	Gedung	1	Kebakaran	62,500,000
Total Kerugian Per tahun				62,500,000

Berikut adalah tindakan yang diambil PT OraKelar untuk meminimalisir kemungkinan terjadinya resiko kebakaran:

No	Kegiatan penanggulangan kebakaran	Jumlah	Biaya per tahun	Biaya Resiko per tahun
1	Pembelian alat pemadam kebakaran 2 buah untuk tiap lantai	6 tabung	8,000,000	
2	Alarm Asap untuk tiap ruangan	20 buah	500,000	
3	Asuransi Kebakaran		1,000,000	
			9,500,000	62,500,000

Rusak

No	Item	Jml	Resiko	ALE
1	Integrated LAN	1	Rusak	750,000
Total Kerugian Per tahun				750,000

Terjadinya kerusakan pada LAN di gedung perusahaan merugikan perusahaan sebesar 0,75 juta per tahunnya. Kerusakan ini terjadi karena bertamahnya umur kabel dan sebab wajar lainnya. Untuk kerugian yang relatif kecil per tahun ini, PT OraKelar tidak melakukan tindakan apapun untuk mencegahnya.

Putus (Terhentinya pelayanan):

No	Item	Jml	Resiko	ALE
1	Nomor Telepon	4	Putus	40,000,000
2	Layanan Internet ADSL	1	Putus	54,000,000
3	Layanan Listrik	1	Putus	168,000,000
Total Kerugian Per tahun				262,000,000

Terputusnya layanan telpon dan layanan internet ADSL belum bisa dicari jalan untuk meminimalkan resiko terjadinya. Untuk resiko terputusnya layanan listrik oleh PLN, PT OraKelar telah membeli 2 buah Generator yang dapat menghasilkan tenaga listrik sebesar 5000 watt seharga Rp 6.000.000 sebuahnya:

No	Kegiatan penanggulangan terputusnya layanan listrik	Jumlah	Biaya per tahun	Biaya Resiko per tahun
1	Pembelian Generator listrik 5000 watt	1	12,000,000	
			12,000,000	168,000,000

Virus\Worm:

No	Item	Jml	Resiko	ALE
1	Software untuk pengajaran	1	Virus\Worm	30,000,000
2	Data	1	Virus\Worm	28,000,000
Total Kerugian Per tahun				58,000,000

Berikut tindakan yang diambil PT OraKelar untuk menanggulangi resiko kehilangan data karena Virus atau Worm:

No	Kegiatan penanggulangan terputusnya layanan listrik	Jumlah	Biaya per tahun	Biaya Resiko per tahun
1	Pembelian AntiVirus: 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™ 2005 Professional Small Office Pack		8,000,000	
			14,134,400	58,000,000

2.2 Kebijakan Keamanan

Untuk penerapan manajemen keamanan yang optimal, upaya-upaya yang bersifat teknis seperti diatas, dilengkapi lagi dengan kebijakan-kebijakan perusahaan yang bertujuan pencapaian optimal dari penggunaan *resource* yang dimiliki oleh perusahaan.

2.2.1 Kebijakan

Kebijakan adalah serangkaian peraturan tertulis yang dikeluarkan oleh pihak manajemen perusahaan sebagai visi keamanan yang berlaku di perusahaan. Beberapa kebijakan yang telah dibuat oleh PT OraKelar meliputi sebagai berikut:

Kebijakan penggunaan PC di Lab lantai II oleh para Siswa.

Kebijakan IT secara umum berkaitan dengan penggunaan fasilitas IT oleh karyawan PT OraKelar.

Kebijakan departemen IT mengenai ruang *server*.

Berikut ini akan ditunjukkan salah satu kebijakan PT OraKelar: Kebijakan penggunaan PC di Lab lantai II oleh para Siswa:

LPK OraKelar

Kebijakan Penggunaan PC di Laboratorium IT oleh Para Siswa

Pendahuluan

Dalam kegiatannya menyelenggarakan pelatihan Komputer kepada para siswanya, LPK OraKelar menyediakan fasilitas laboratorium Teknologi Informasi diperuntukan paa siswa LPK OraKelar, dengan tujuan dapat menunjang proses pengajaran keahlian IT para siswanya.

Hak dan Kewajiban

Komputer dan Jaringan yang tersedia terhubung dengan *resource* yang ada didalam maupun diluar kampus, termasuk komunikasi dengan *user* lain diseluruh dunia. Dengan kemampuan akses yang terbuka demikian luas, diharapkan tiap siswa dapat bertindak dengan bertanggung jawab. Siswa, dalam hal ini *user* atau pengguna dari fasilitas IT ini harus menghormati hak dari *user* lain, diluar maupun di dalam lingkungan LPK.

Siswa memiliki hak untuk mengakses semua informasi miliknya yang tersimpan dalam PC-nya atau didalam jaringan. *System Administrator* sebagai petugas LPK yang bertugas untuk menjaga integritas sistem dan jaringan IT LPK, berhak untuk mwngakses file-file yang tersimpan didalam fasilitas IT dilingkungan LPK OraKelar Misalnya, sistem administrator berhak dan wajib memeriksa, mebuca dan menghapus file-file atau *accounts* yang dicurigai telah melakukan pelanggaran atau telah rusak atau terjangkit virus/worm.

Contoh pelanggaran

Berikut beberapa contoh pelanggaran yang mungkin dilakukan oleh siswa, tindakan lain yang tidak tersebut didalam daftar ini ada kemungkinan termasuk dalam golongan pelanggaran bila bertentangan dengan peraturan LPK OraKelar secara umum maupun khusus:

Menggunakan *computer account* (*username* dan *password*) yang bukan milik anda. Mendapatkan password tanpa diizinkan oleh pemilik account.

Menggunakan jaringan LPK untuk melakukan *unauthorized access* atau akses ilegal ke sistem lain.

Secara sadar melakukan tindakan yang akan mengganggu kelancaran sistem komputer, terminal, *peripherals* atau jaringan.

Secara sadar menyuruh orang untuk atau melakukan sendiri: menjalankan, meng-install suatu program yang berujuan untuk merusak sistem komputer atau jaringan LPK. Hal ini termasuk melakukan penyebaran virus, worm, trojan horse atau bentuk lainnya.

Secara sadar menghabiskan *resource* komputer.

Menggunakan e-mail untuk mengganggu user lain, didalam maupun diluar lingkungan LPK.

Melakukan *posting* si *bulletin board* LPK atau portal LPK bahan-bahan yang bertentangan dengan hukum dan norma yang berlaku.

Mencoba untuk mengutak-utik komunikasi elektronik yang dilakukan *user* lain atau membaca, mengkopi, merubah, menghapus data user lain tanpa izin secara eksplisit dari user yang bersangkutan.

Kegiatan tidak akan dianggap pelanggaran bila dilakukan dengan izin dari petuas LPK. Misalnya dalam kegiatan pelatihan dan lain-lain.

Sanksi dan hukuman

Sanksi dan hukuman akan dikenakan kepada siswa yang terbukti melakukan pelanggaran. Sanksi dan hukuman dapat berupa hukuman administratif maupun hukuman verbal.

Pelanggaran ringan atau pelanggaran tidak sengaja biasanya akan ditangani dengan peringatan melalui e-mail atau teguran langsung. Pelanggaran yang lebih serius akan ditangani secara lebih formal. Dalam beberapa kasus, pelanggaran dapat dikenakan hukuman berupa pencabutan hak untuk mengkases fasilitas LPK untuk mencegah berulangnya pelanggaran selama pembuktian kasus masih berlangsung.

Pelanggaran berat oleh siswa dapat mengakibatkan pencabutan hak akses secara sementara atau secara tetap. Pelanggaran yang berhubungan dengan hukum yang berlaku di Indonesia dapat dilaporkan kepada pihak kepolisian.

Tertanda,

Manajemen LPK OraKelar

2.2.2 Prosedur

Salah satu prosedur yang ada di PT OraKelar adalah prosedur *update* virus data untuk anti virus PC yang berada di lingkungan PT OraKelar. Berikut adalah prosedur nya:

PROSEDUR UPDATE DATA VIRUS UNTUK ANTI VIRUS PC ANDA

Masuk ke portal perusahaan dengan alamat: <http://www.OraKelar-kelar.co.id>.

Klik ke link yang berbunyi: "Update Virus Data anti virus anda" di ujung atas *welcome screen*.

Bila system memberikan pilihan:

"Download file" atau "Execute this File"

Pilih "Execute this file"

Program *update* akan secara otomatis berjalan di komputer anda.

Bila telah keluar layar yang bertulisan:

"YOU HAVE SUCCESSFULLY UPDATED YOUR VIRUS DATA"

Berarti anda telah berhasil dalam meng-*update* virus data di anti virus PC anda.

2.2.3 Standar

PT OraKelar tidak memiliki standar baku didalam sistem keamana nya. *Hardware* atau *Software* yang dipilih harus melalui proses *review* sebelum bisa digunakan di lingkungan PT OraKelar. *Review Hardware* atau idilakukan oleh departemen IT PT OraKelar.

2.2.4 Pedoman

Pedoman yang dibuat oleh departemen IT untuk par pengguna fasilitas IT, staff dan para siswa, di perusahaan adalah pedoman pencegahan agar virus dan worm tidak menjangkiti jaringan di PT OraKelar.

Dibuatnya pedoman ini adala ketika sedang maraknya *worm* yang masuk kedalam sistem IT perusahaan dan mengganggu jaringan PT OraKelar. Isi pedoman pencegahan virus dan Worm tersebut adalah sebagai berikut:

PEDOMAN PENCEGAHAN VIRUS DAN WORM

Hapus segera bila menerima e-mail dari orang yang tida dikenal atau mencurigakan.

Segera hapus *junk-mail* atau *spam mail* yang anda terima.

Bila menerima e-mail dengan *attachment* yang berekstension exe, pif, vbs, com, atau bat, harap jangan dibuka, tindakan paling tepat adalah dengan langsung men-*delete* mail tersebut.

Jalankan aplikasi anti virus di komputer anda secara teratur dan berkala. Hal ini akan memperkecil kemungkinan masuknya Virus atau Worm memasuki PC anda.

Update data virus Anti Virus di komputer Anda, dengan cara mendownload Data virus terbaru dari portal perusahaan secara teratur. Prosedur download dan update virus data ini diterangkan di sini.

Hindari *browsing* atau *download* file dari *home page* yang tidak resmi atau mencurigakan.

Jangan sembarangan membuka file yang ada didalam *diskette*. Semua *diskette harus terlebih dahulu di-scan* oleh program anti virus sebelum dapat dibuka.

Lakukan *backup* terhadap file-file penting anda secara teratur, misalnya sebulan sekali. *Burn* backup ini pada sebuah CD-ROM, dan simpan ditempat yang aman.

Bila PC anda telah terlanjur terjangkit oleh Virus atau Worm, harap hubungi petugas IT segera.

2.3 Pendidikan Keamanan

Agar Kebijakan, Prosedur dan Pedoman Kemanan di PT OraKelar senantiasa diketahui dan dipraktekan oleh para karyawannya, dilakukan beberapa upaya sebagai berikut:

Penyediaan informasi mengenai kebijakan perusahaan di *portal* perusahaan dan secara berkala di *update* oleh pemilik kebijakan.

Himbauan secara teratur oleh para direktur dalam pesan-pesan kepada karyawan.

Enforcement top-down dari atasan terhadap bawahan agar mengikuti segala kebijakan yang dikeluarkan perusahaan.

Memberlakukan *reward and punishment* sistem terhadap karyawan yang mengikuti aturan perusahaan atau yang melanggarnya.

Tidak ada pelatihan formil dilakukan PT OraKelar untuk sosialisasi kebijakan perusahaan, langkah-langkah diatas dirasakan sudah efektif dalam sosialisasi kebijakan perusahaan tersebut.

BAB 3

AKSES KONTROL

Dalam menjaga penggunaan *resource* yang dimiliki perusahaan, PT OraKela menerapkan Manajemen Akses Kontrol pada beberapa resource nya. Antara lain adalah:

System IT perusahaan

Meliputi penggunaan Komputer karyawan perusahaan dan jaringannya, dan penggunaan Komputer non-karyawan dan jaringannya, yaitu murid dan pengajar. Selain penggunaan PC system IT juga meliputi *Printer, Switch, Modem* dan lain-lain. Akses kontrol resource ini diatur oleh Manajer IT.

Ruangan kantor, kelas dan laboratorium.

Ruangan-ruangan yang terdapat pada perusahaan meliputi kantor dan kelas. Pengaturan penggunaan ruangan kantor dan kelas diatur oleh Manajer Operasional.

Telepon

Akses sambungan telepon dan Facsimili yang ada pada perusahaan. Seperti juga pada penggunaan Ruang kantor dan kelas, penggunaan sambungan telepon diatur oleh Manajer Operasional.

Masing-masing *resource* diatas dilindungi agar penggunaannya selalu dapat dipertanggungjawabkan dan melindungi *resource* dari penggunaan yang berlebihan atau penggunaan oleh orang yang tidak berwenang.

3.1 Identifikasi, Autentikasi, Autorisasi, dan Akuntabilitas

3.1.1 Identifikasi

Agar suatu *resource* perusahaan dapat digunakan, calon pengguna harus memberitahu kepada *system* siapakah dirinya. Untuk itu di PT OraKela, diperlakukan kegiatan identifikasi *resource* sebagai berikut.

Identifikasi pada penggunaan System IT perusahaan adalah dengan penerapan *Username* pada setiap user yang ingin menggunakan System IT perusahaan. System IT untuk karyawan dibedakan dengan System IT non-karyawan (murid dan pengajar). Dalam pengaturan antara System IT Karyawan dan Non-Karyawan, dengan menggunakan 2 domain yang berbeda.

Dalam menggunakan Ruang kantor maupun kelas di gedung PT OraKela, diterapkan proses identifikasi sebagai berikut;

Ruang Kelas, diperlakukan aturan sebagai berikut; Ruang kelas hanya boleh digunakan bila hanya ada kegiatan pengajaran yang menggunakan kelas tersebut.

Ruang Lab IT, diperlakukan aturan, hanya yang merupakan murid atau pengajar di PT OraKelar yang boleh menggunakan fasilitas Lab IT.

Ruang Kantor di PT OraKelar menggunakan Akses Kontrol identifikasi berupa *proximity card*. Pemilik *Proximity Card* yang dikeluarkan oleh divisi SDM hanya merupakan karyawan dari PT OraKelar.

Tiap penggunaan telepon di PT OraKelar, harus selalu memasukan password yang merupakan rangkaian 4 digit tertentu yang menggambarkan siapa calon pengguna telepon tersebut. Calon pengguna telepon dapat memasukan 4 digit password nya di pesawat telepon manapun di lingkungan perusahaan.

3.1.2 Autentikasi

Setelah memberitahu *system* jati dirinya, calon pengguna *resource*, diharuskan melakukan kegiatan autentikasi yang bertujuan untuk membuktikan bahwa jati diri yang ia informasikan ke *system* adalah memang jati dirinya. Penjabarannya adalah sebagai berikut:

Calon pengguna System IT, harus memasukan *password* yang sesuai dengan *username* yang telah ia masukan pada poses identifikasi. Adalah aturan perusahaan untuk tidak boleh memberitahukan *password* kepada siapapun.

Untuk menggunakan ruang kelas dan lab, tidak ada proses autentikasi, karena hanya diatur oleh suatu prosedur perusahaan. Petugas yang berwenang secara berkala akan melihat kedalam lab untuk menjaga penggunaan lab dalam batas yang diperbolehkan dan oleh orang yang diperbolehkan.

Sedangkan untuk ruangan kantor, setelah menunjukkan *proximity card* pada sensor, calon pengguna harus memasukan rangkaian 5 digit angka sebagai *password* nya (PIN Number). Adalah aturan perusahaan untuk tidak boleh memberitahukan PIN kepada siapapun.

Calon pengguna sambungan telepon yang telah memasukan 4 digit password telepon telah bisa menggunakan telepon, ini artinya proses identifikasi dan autentikasi disatukan dalam penggunaan *resource* sambungan telepon. Peraturan perusahaan melarang *sharing* pin password telepon.

3.1.3 Autorisasi

Setelah melakukan identifikasi dan autentikasi, calon pengguna akan dapat menggunakan resource sesuai alokasi level penggunaan yang diizinkan oleh perusahaan untuk pengguna tertentu, berikut *Access Control List* yang mengatur penggunaan *resource* perusahaan;

Pengguna System IT:

PC LAB/Kelas		
No	User	Access Right
1	Murid	User
2	Pengajar	Power User
3	Karyawan	No Access
4	Administrator	Administrator

PC Kantor		
No	User	Access Right
1	Murid	No Access
2	Pengajar	No Access
3	Karyawan	Power User
4	Administrator	Administrator

Printer LAB		
No	User	Access Right
1	Murid	User
2	Pengajar	User
3	Karyawan	No Access
4	Administrator	Administrator

Printer Kantor		
No	User	Access Right
1	Murid	No Access
2	Pengajar	No Access
3	Karyawan	User
4	Administrator	Administrator

Switch, Modem, Server		
No	User	Access Right
1	Murid	No Access
2	Pengajar	No Access
3	Karyawan	No Access
4	Administrator	Administrator

No Access : Tidak bisa menggunakan sama sekali

User :

Boleh menggunakan dengan penggunaan alokasi *diskspace* yang telah ditentukan (*Read-Wright-Execute*).

Boleh mengakses *shared resource*.

Tidak boleh Install aplikasi.

Tidak boleh menggunkan *Remote-Access*.

Tidak boleh merubah *setting* PC.

Power User :

Boleh menggunakan dengan penggunaan alokasi *diskspace* yang telah ditentukan (*Read-Wright-Execute*).

Boleh mengakses *shared resource*.

Boleh Install aplikasi.

Boleh menggunkan *Remote-Access*.

Tidak boleh merubah *setting* PC.

Administrator : *No Restriction*

Pengguna Ruang di Gedung

Kelas/LAB		
No	User	Access Right
1	Murid	Full Access
2	Pengajar	Full Access
3	Karyawan	No Access
4	Administrator	Full Access

Ruang Kantor		
No	User	Access Right
1	Murid	No Access
2	Pengajar	Full Access
3	Karyawan	Full Access
4	Administrator	Full Access

Ruang Server		
--------------	--	--

No	User	Access Right
1	Murid	No Access
2	Pengajar	No Access
3	Karyawan	No Access
4	Administrator	Full Access

Full Access : Boleh menggunakan

No Access : Tidak Boleh Menggunakan

Penggunaan Sambungan Telepon

Telepon & Facsimili		
No	User	Access Right
1	Murid	No Access
2	Pengajar	Local Call (Time Limited)
3	Karyawan Biasa	Local Call (Time Limited)
4	Ka. Div.	Local Call, Interlocal (Time Limited)
5	Menejer	Local Call, Interlocal
6	BOD	Local Call, Interlocal

Berikut adalah *Access Control List* untuk data di perusahaan:

No	Jabatan	Kategori Data										
		Keu.	SDM	Ops.	Legal	Akuntansi	Marketing	IT	Materi	Nilai	Umum	
1	Direktur Utama	R	R	R	R	R	R	R	R	R	R	RW
2	Direktur Keuangan dan SDM	RW	RW	R	R	RW	R	R	R	R	NA	RW
3	Direktur Operasional	R	R	RW	R	R	R	R	R	R	NA	RW
4	Manajer Keuangan dan Akuntansi	RW	R	R	R	RW	R	R	R	R	NA	RW
5	Manajer SDM dan Hukum	R	RW	R	RW	R	R	R	R	R	NA	RW
6	Manajer Operasional	R	R	RW	R	R	R	R	R	R	R	RW
7	Manajer Marketing	R	R	R	R	R	RW	R	R	R	NA	RW
8	Manajer IT	R	R	R	R	R	R	RW	R	R	NA	RW
9	Staff Keuangan	RW	NA	R	NA	R	R	NA	R	NA	NA	RW
10	Staff Accounting	R	R	R	NA	RW	R	NA	R	NA	NA	RW
11	Staff Payroll	RW	R	R	R	R	R	NA	R	NA	NA	RW
12	Staff Legal	R	R	R	RW	R	R	NA	R	NA	NA	RW
13	Staff Marketing Corporate	NA	NA	R	R	NA	RW	NA	R	NA	NA	RW
14	Staff Marketing Public	NA	NA	R	R	NA	RW	NA	R	NA	NA	RW
15	Staff Pengajar Software Eng.	NA	NA	NA	NA	NA	NA	NA	RW	RW	RW	RW
16	Staff Pengajar Desain Grafis	NA	NA	NA	NA	NA	NA	NA	RW	RW	RW	RW
17	Staff Pengajar Sistem Operasi	NA	NA	NA	NA	NA	NA	NA	RW	RW	RW	RW
18	Staff Pengajar Networking	NA	NA	NA	NA	NA	NA	NA	RW	RW	RW	RW
19	Staff Pengajar Database	NA	NA	NA	NA	NA	NA	NA	RW	RW	RW	RW
20	Staff Pengajar Database	NA	NA	NA	NA	NA	NA	NA	RW	RW	RW	RW
21	Staff Pengajar Back Office	NA	NA	NA	NA	NA	NA	NA	RW	RW	RW	RW
22	Staff IT - Jaringan	R	R	R	R	R	R	RW	R	NA	NA	RW
23	Staff IT - Database	R	R	R	R	R	R	RW	R	NA	NA	RW
24	Staff IT - Administrator	R	R	R	R	R	R	RW	R	NA	NA	RW
25	Sekretaris Direksi	R	R	R	R	R	R	NA	R	NA	NA	RW
26	Sekretaris Umum	NA	NA	NA	NA	NA	NA	NA	R	NA	NA	RW
27	Resepsionis	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	RW
28	Satpam	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	RW

29	Pesuruh	NA	NA	NA	NA	NA	NA	NA	NA	NA	RW
30	Sopir	NA	NA	NA	NA	NA	NA	NA	NA	NA	RW

R = Read-Only

A = Append (Only Write),

E = Execute (cannot read and
write)

RW = Read-Write,

NA = No Access

3.1.4 Akuntabilitas

Pengguna *resource* perusahaan selalu dituntut untuk menggunakan *resource* perusahaan didalam batas-batas yang ditentukan, untuk meng-*enforce* kebijakan ini, sistem-sistem IT, Penggunaan Ruang dan Penggunaan Sambungan Telepon memiliki tingkat akuntabilitas tertentu sebagai berikut:

System IT menggunakan beberapa fasilitas audit sebagai berikut:

System-level events, fasilitas ID yang sudah terdapat pada level *Operating System* yang dapat mengetahui percobaan *login*, *login ID*, waktu *login*, *lockouts*, *resource* yang dipakai, *file* yang diakses, fungsi-fungsi yang dilakukan, dan lain-lain.

Application-level events, sistem audit yang disediakan oleh masing-masing aplikasi yang digunakan, misalnya Microsoft Office, Aplikasi kesiswan dan lain-lain. Dapat memonitor kegiatan-kegiatan sebagai berikut: pesan-pesan kesalahan aplikasi, *file* yang dibuka dan ditutup, modifikasi *file*, perubahan-perubahan record yang dilakukan, pelanggaran keamanan terhadap aplikasi dan lain-lain.

User-level events memonitor kegiatan-kegiatan seperti; percobaan identifikasi dan autentikasi, *file*-servis-dan sumber daya yang dipakai, perintah yang diberikan, dan pelanggaran keamanan. Ruang Kelas dan Lab tidak memiliki sistem monitor secara khusus, pengguna yang menggunakan ruang harus mengisi *roster* atau absen pada saat masuk ruangan dan pada saat meninggalkan ruangan, dengan begini, dapat diketahui siapa saja pengguna ruangan pada rentang waktu tertentu dan kegiatan yang dilakukan.

Sedang untuk ruang kantor, dengan menggunakan Kontrol Akses *proximity Card* dan Nomor Pinya, tiap orang yang masuk atau keluar ruangan akan tercatat dalam *database*-nya.

Tiap penggunaan telepon didalam lingkungan perusahaan akan selalu tercatat dalam *database* PABX. Data-data yang tercatat antara lain adalah: Data Penelpon (sesuai dengan Pin Password), nomor telepon tujuan, waktu mulai panggilan, waktu selesai panggilan dan lain-lain.

Dengan adanya aspek akuntabilitas ini, dalam level tertentu dapat mejamin pengguna bertanggung jawab atas tindakan mereka. Audit dapat dilakukan oleh auditor internal (Administrator, Menejer, Ka Div dan lain-lain) atau juga dilakukan oleh Auditor Independen.

BAB 4

KEAMANAN FISIK

Keamanan fisik dan infrastruktur merupakan hal yang sangat penting. Fisik yang dimaksudkan disini adalah aset yang berwujud seperti orang, gedung, perlengkapan, peralatan, dan sistem yang ada diperusahaan.

Keamanan fisik dapat dicapai melalui kondisi sarana dan prasarana bangunan yang memadai (listrik, air), area yang minim tindak kejahatan, prasarana perlindungan umum seperti pemadam kebakaran dan polisi.

Kondisi-kondisi diatas dapat dicapai dengan melakukan berbagai macam kegiatan pengamanan fisik seperti dibawah ini:

1. Kontrol Administratif:
 - a. Pembuatan kebijakan, peraturan dan standar penggunaan fasilitas fisik.
 - b. Pengawasan personil.
2. Kontrol Teknis:
 - a. Pemasangan kamera pengawas.
 - b. Pemasangan detektor kebakaran.
 - c. Pemasangan tabung pemadam kebakaran.
 - d. Pemasangan *genset*.
 - e. Pemasangan kontrol akses gedung.
3. Kontrol Fisik:
 - a. Pemasangan kunci elektronik pada ruang server dan kelas komputer.
 - b. Patroli satpam ke setiap ruangan dalam durasi waktu tertentu
 - c. Penambahan pencahayaan di daerah sekitar gedung.

Sentralisasi penyimpanan kunci.

4.1 Manajemen Fasilitas

Pemilihan gedung didaerah yang ditempati sekarang dilakukan setelah meninjau berbagai macam aspek manajemen fasilitas dibawah ini:

- Visibilitas: Gedung LPK terlihat dengan sangat jelas dari seluruh penjuru jalan raya, dengan papan nama yang cukup besar.
- Area lingkungan: LPK ini dikelilingi oleh perumahan penduduk di utara, gedung pemerintahan di selatan, dan taman kota di daerah timur dan barat.

- Kemudahan Akses: terletak di daerah kota dimana lokasi rumah sakit, kantor polisi maupun pemadam kebakaran relatif dekat.
- Bencana Alam: lokasi yang ditempati relatif tinggi sehingga kemungkinan bahaya banjir tidaklah besar.

4.2 Konstruksi

Pengelola LPK cukup beruntung dengan mendapatkan gedung baru dimana semua material yang digunakan termasuk kategori baik.

Penambahan yang dilakukan meliputi:

- Jendela : pemasangan jendela berteralis pada setiap ruangan.
- Pintu : pemasangan pintu tahan api pada ruang server
- Langit-langit : penambahan kawat diatas ruang server untuk meningkatkan keamanan.
- Pendingin Udara : ekstra pendingin udara diletakkan pada ruangan server
- Pendeteksi Kebakaran : disetiap ruangan dan koridor gedung.

4.3 Ruangan Komputer

Setiap ruangan komputer harus diawasi sebanyak minimal 10 kali dalam setiap shift jaga satpam. Satpam juga bertanggung jawab mencatat setiap orang yang keluar masuk ke ruang server, memastikan otorisasi manual terhadap identitas peserta les maupun tenaga pengajar.

Ruangan server memiliki pengamanan berlapis yaitu pintu tahan api yang hanya bisa dibuka oleh pihak yang menggunakan id card elektronik. Kemudian pintu lapisan kedua dengan kunci manual. Didalam ruang server setiap orang wajib menggunakan gelang statik untuk menghindari rusaknya perangkat keras didalam ruang server. Sebuah kamera pengawas akan memantau kegiatan didalam ruangan server. Deteksi kebakaran akan dilakukan oleh 3 buah alat deteksi yang dipasang sepanjang jalur utama ruangan server.

4.4 Security Must

Perangkat yang harus ada di dalam gedung LPK adalah detektor asap, tanda keluar gedung yang jelas, penerangan yang cukup, serta pintu untuk keluar masuk gedung sebanyak dua buah.

4.5 Security Should

Aspek keamanan-keamanan dibawah ini merupakan *security should* yang sudah diterapkan oleh LPK:

- Penilaian kondisi gedung secara menyeluruh
- Pendidikan dan pelatihan satpam

- Penggantian kunci dalam interval tertentu
- Pengawasan internal terhadap karyawan maupun peserta

4.6 Backup

Backup dilakukan secara rutin oleh internal IT dengan menggunakan media CD dan DVD. Mekanisme backup digambarkan secara mendetil dalam Standar Operasi Divisi IT yaitu setiap hari pada pukul 12 malam, mingguan dan bulanan pada jam-jam non operasional.

BAB 5

KEAMANAN JARINGAN DAN TELEKOMUNIKASI

Telekomunikasi adalah pengiriman dan penerimaan tiap jenis tanda, gambar, suara, dan informasi dalam bentuk apapun melalui sistem kawat, optik, radio atau sistem elektromagnetik lainnya. Jaringan telekomunikasi adalah rangkaian perangkat telekomunikasi dan kelengkapannya yang digunakan dalam rangka bertelekomunikasi.

Keamanan jaringan dan telekomunikasi memiliki implikasi terhadap dua entitas besar diatas yaitu terhadap data dan media penyaluran data. Pembahasan mengenai keamanan jaringan akan dimulai dengan identifikasi peralatan jaringan dan telekomunikasi serta data yang harus dilindungi.

5.1 Peralatan Jaringan dan Telekomunikasi

1. 5 buah Zoom Hayes ADSL X4 Modem/Router : Cable/dsl router, external, firewall, NAT, DHCP, 4 LAN ports
2. 4 buah 3Com SuperStack 3 Switch 4400 48-Port
3. Server Jaringan yang terbagi atas
 - a. Mail Server : Pentium IV 2,8 GHz, Memori 1 Gbyte, HD 80 Gbyte.
 - b. Web Server : Pentium IV 2,8 GHz, Memori 2 Gbyte, HD 80 Gbyte.
 - c. Database Server : Pentium IV 2,8 GHz, Memori 2 Gbyte, HD 80 Gbyte.
 - d. Application Server : Pentium IV 2,8 GHz, Memori 2 Gbyte, HD 80 Gbyte.
 - e. Proxy Server : Pentium IV 2,8 GHz, Memori 1 Gbyte, HD 40 Gbyte.
4. 100 PC Desktop Client @ Pentium IV 2,4 GHz, Memori 1 Gbyte, HD 30 Gbyte, Ethernet Card, Mouse, Keyboard, Monitor.
5. 10 Notebook Acer 2500.
6. 5 Printer Laser HP Color LaserJet 1500
7. 5 buah UPS 1200 VA + 100 UPS 600 VA
8. Satu buah mesin faksimili Panasonic KX-FLB756
9. Satu buah mesin *photocopy* Xerox WorkCentre™ C2424
10. Satu buah UKF-2083C SOHO PABX SYSTEM Exchange& Telecom Device

5.2 Keamanan Jaringan

Untuk melindungi jaringan dapat dilakukan hal-hal sebagai berikut:

1. Administratif: kebijakan, prosedur, standar pemakaian dari masing-masing peralatan telekomunikasi.
2. Fisik: pembuatan ruangan server khusus (pintu tahan api, id scanner), tenaga sekuriti di depan ruang server, pembuatan ruangan kelas yang cukup jauh dari ruang server, pemasangan detektor kebakaran dan tabung pemadam api di setiap ruang kelas, tenaga teknisi kelistrikan yang mudah untuk dihubungi, penambahan penerangan di sekitar lokasi LPK.

Teknis: firewall, antivirus, backup server.

BAB 6

PEMULIHAN BENCANA DAN KELANGSUNGAN BISNIS

Upaya dan rencana penganggulangan bencana yang menyebabkan sistem maupun proses bisnis berhenti (*down*) disebut dengan istilah *Business Contingency Plan* (BCP) dan *Disaster Recovery Plan* (DRP). Hal ini diperlukan karena bencana itu tidak dapat diprediksi sehingga dibutuhkan strategi perlindungan yang terbaik.

BCP melibatkan pengembangan rencana dan persiapan terhadap bencana sebelum bencana itu terjadi dengan tujuan untuk meminimalkan kerugian (*loss*) dan memastikan sumber daya, orang, dan proses bisnis dapat berjalan sebagaimana mestinya. Prosesnya (otomatis maupun manual) dirancang untuk mengurangi ancaman terhadap fungsi-fungsi penting organisasi, sehingga menjamin kontinuitas layanan bagi operasi yang penting. Guna mengantisipasi kasus terburuk, BCP harus mempertimbangkan strategi jangka pendek (*short-term*) dan strategi jangka panjang (*long-term*). BCP disebut juga dengan tindakan pencegahan.

DRP menyediakan metode dan prosedur penanganan jangka panjang setelah terjadi bencana. DRP disebut juga dengan tindakan korektif.

Langkah dalam membuat rencana ini adalah melakukan *Risk Assessment and Analysis* untuk mengevaluasi ancaman potensial 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.

Berikut ini beberapa ancaman yang kemungkinan timbul:

- Kebakaran
- Banjir
- Serangan Virus
- Sabotase
- Gangguan listrik dan komunikasi
- Gangguan software, hardware dan jaringan

Kerugian yang bisa terjadi:

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

6.1 Interdependencies

Langkah selanjutnya adalah mengidentifikasi interrelation dan interdependency yaitu pendefinisian fungsi bisnis penting dan departemen pendukung.

Fungsi bisnis penting harus didukung dan dibawahahi oleh departemen atau unit tertentu.

- Kegiatan operasional di bidang Lembaga Pendidikan Komputer.
Didukung oleh Biro Operasional.
- Dukungan software, hardware dan jaringan komputer.
Didukung oleh Divisi IT
- Keuangan dan Akuntansi
Didukung oleh Biro Keuangan
- Administrasi Penggajian
Didukung oleh Divisi SDM

6.2 Contingency Plan Requirements

Untuk membuat BCP, perlu adanya dukungan dari pihak manajemen. Oleh karena itu BCP maupun DRP pada PT. Orakelar 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 BCP maupun DRP. Sekali pihak manajemen menset tujuan dan kebijakan serta prioritas perusahaan, staf lain yang bertanggung jawab dalam rencana ini akan dapat mengisi sisanya.

6.3 Pembuatan Tujuan Contingency Plan

Membuat tujuan-tujuan adalah penting untuk semua pekerjaan, terutama untuk BCP. 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 :

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 disertai tugas perlu diajarkan dan diinformasikan.

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

1. Identifikasi fungsionalitas bisnis yang kritis. Pada tahap ini akan dilihat prioritas dari fungsionalitas bisnis yang ada bagi perusahaan. Bagi PT. Kontraktor Sipil Jaya, prioritas 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.
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 tersebut harus diuji secara terus-menerus supaya perbaikan yang timbul dapat diatasi.

Rencana pemulihan bencana (*Disaster Recovery Plan*) dan kelangsungan bisnis (*Business 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.