Laporan Studi Kasus

PROTEKSI & TEKNIK KEAMANAN SI/TI : IKI83408T

PROTEKSI DAN TEKNIK KEAMANAN SI/TI
PT EASY VALAS

Money Changer

Disusun oleh :

Kelompok 104

Dwi Hartanto	**720301205X**
Iman Noersetiyadi	**7203012084**
Nadjamuddin Abror	**720301219X**

PROGRAM MAGISTER TEKNOLOGI INFORMASI

UNIVERSITAS INDONESIA

2005

DAFTAR ISI

DAFTAR ISI 0
BAB I 2
PENDAHULUAN 2
1.1 Pengantar 2
1.2 Tujuan Penulisan Makalah 2
1.3 Profil Perusahaan 3
1.4 Struktur Organisasi 5
1.5 Modal Disetor 6
BAB II 0
PRAKTEK MANAJEMEN KEAMANAN 0
2.1 Manajemen Resiko 0
2.2 Pendidikan Keamanan 1
BAB III 2
KONTROL AKSES 2
3.1 Access Control Systems & Methodology 2
3.2 Controls 3
3.3 Akuntabilitas 4
BAB IV 0
TELECOMMUNICATIONS DAN NETWORK SECURITY 0
SERTA SECURITY MANAGEMENT PRACTICES 0
4.1 Telecommunications and Network security 0
4.2 Security Management Practices 1
BAB V 3
APPLICATION DAN SYSTEM DEVELOPMENT SECURITY 3
SERTA CRYPTOGRAPHY 3
5.1 Application & Systems Development Security 3
5.2 Cryptography 3
BAB VI 5
SECURITY ARCHITECTURE DAN MODEL 5
SERTA OPERATION SECURITY 5
6.1. Security Architecture & Models 5
6.2. Operations Security 5
BAB VII 0
DISASTER RECOVERY DAN BUSINESS CONTINUITY PLAN 0
SERTA LAWS, INVESTIGATION DAN ETHICS 0
7.1 Disaster Recovery & Business Continuity Plan 0
7.2. Laws, Investigations & Ethics 1
BAB VIII 3
PHYSICAL SECURITY 3
SERTA AUDITING DAN ASSURANCE 3
8.1 Physical Security 3
8.2 Auditing & Assurance 6

BAB I
PENDAHULUAN

1.1 Pengantar

Sistem Keamanan merupakan salah satu bagian penting dalam setiap proses pengembangan suatu bisnis dan investasi, karena dengan sistem keamanan yang baik resiko atas kehilangan sejumlah nilai yang diinvestasikan menjadi lebih kecil. Dengan pesatnya perubahan tehnologi dan usaha menerapkannya sebagai salah satu sarana berbisnis menyebabkan perubahan nilai informasi, sehingga mempengaruhi proses bisnis yang sedang berjalan. Melihat dari kondisi tersebut, membuat keamanan sistem informasi menjadi salah satu perhatian yang harus direncanakan dengan sebaik-baiknya. 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 salah satu bagian dari organisasi perusahaan, sehingga menghasilkan suatu solusi tanpa melihat dan menyesuaikan dengan proses bisnis yang ada. Artinya, perangkat sistem keamanan tercanggih pun sering kali belum mencukupi atau terlalu berlebihan untuk diterapkan. 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.

Pada kesempatan ini kelompok membahas tentang apa saja yang perlu diperhatikan untuk menerapkan suatu sistem keamanan, serta menyesuaikan dengan proses bisnis yang berlaku yaitu pertukaran mata uang. Penerapan sistem keamanan yang digunakan menyesuiakan dengan teori yang diberikan pada kelas proteksi dan sistem keamanan sistem informasi dan tehnologi informasi.

1.2 Tujuan Penulisan Makalah

Makalah ini bertujuan untuk membahas kesebelas domain dalam keamanan sistem informasi pada sebuah perusahaan Money Changer yang berdomisili di Jakarta yaitu PT. Easy Valas. Kesebelas domain keamanan tersebut adalah:

1. Praktek manajemen keamanan,
2. Metodologi dan sistem kontrol akses,
3. Arsitektur dan model keamanan,
4. Keamanan fisik,
5. Keamanan jaringan dan telekomunikasi,

6. Kriptografi,
7. Pemulihan bencana dan kelangsungan bisnis,
8. Hukum-investigasi-dan etika,
9. Pengembangan sistem dan aplikasi,
10. Keamanan operasi,
11. Audit dan jaminan.

1.3 Profil Perusahaan

PT. Easy Valas merupakan perusahaan yang bergerak pada bidang pertukaran mata uang. Didirikan pada tahun 2003 dengan lokasi di kelapa gading sebagai kantor perdana. Pada awal berdirinya, perusahaan ini memiliki tujuan menambah pendapatan dari pertukaran mata uang yang dimiliki oleh perorangan, sesuai dengan perubahan jaman dan semakin berkembangnya kebutuhan akan mata uang asing dari pihak perusahaan serta melihat potensi dari proses bisnis yang ada mencukupi maka segmen pasar diperluas dan menjadikan sebuah tantangan yang baru.

Melihat dari kondisi perusahaan yang semakin baik dan terdapat peluang untuk menerapkan ditempat lain yang memiliki kondisi yang hampir sama dengan yang berjalan selama ini maka dibentuk cabang perusahaan di beberapa tempat diwilayah jakarta. Cabang tersebut beroperasi selama 6 x 24 jam (minggu libur) dengan 2 shift waktu kerja (Shift I 08.00 – 20.30 WIB dan 20.00 – 08.30 WIB Shift II). Setiap cabang terdiri memiliki **10 orang** karyawan yaitu **1 orang Kepala Cabang** yang memiliki otorisasi tertinggi di cabang dan bertanggung jawab kepada direktur perusahaan di pusat, **2 orang kasir** yang bergantian yang bertanggung jawab kepada kepala cabang dan dipercaya dalam administrasi dan keuangan serta bertanggung jawab terhadap keluar masuk mata uang dan keabsahannya kedalam tempat penyimpanan di cabang, **4 orang Frontdesk** (3 orang untuk siang dan 1 orang malam) bertugas melayani dan berhadapan langsung dengan para konsumen yang ingin melakukan pembelian, penjualan atau sekedar menanyakan informasi mengenai nilai tukar mata uang yang berlaku. **2 orang petugas keamanan** yang secara bergantian berjaga dan **1 orang sebagai office boy** untuk operasional kebersihan. Di pusat terdapat **1 orang direktur** dan **1 orang sekertaris direktur** serta seluruh fungsi yang sama pada cabang.

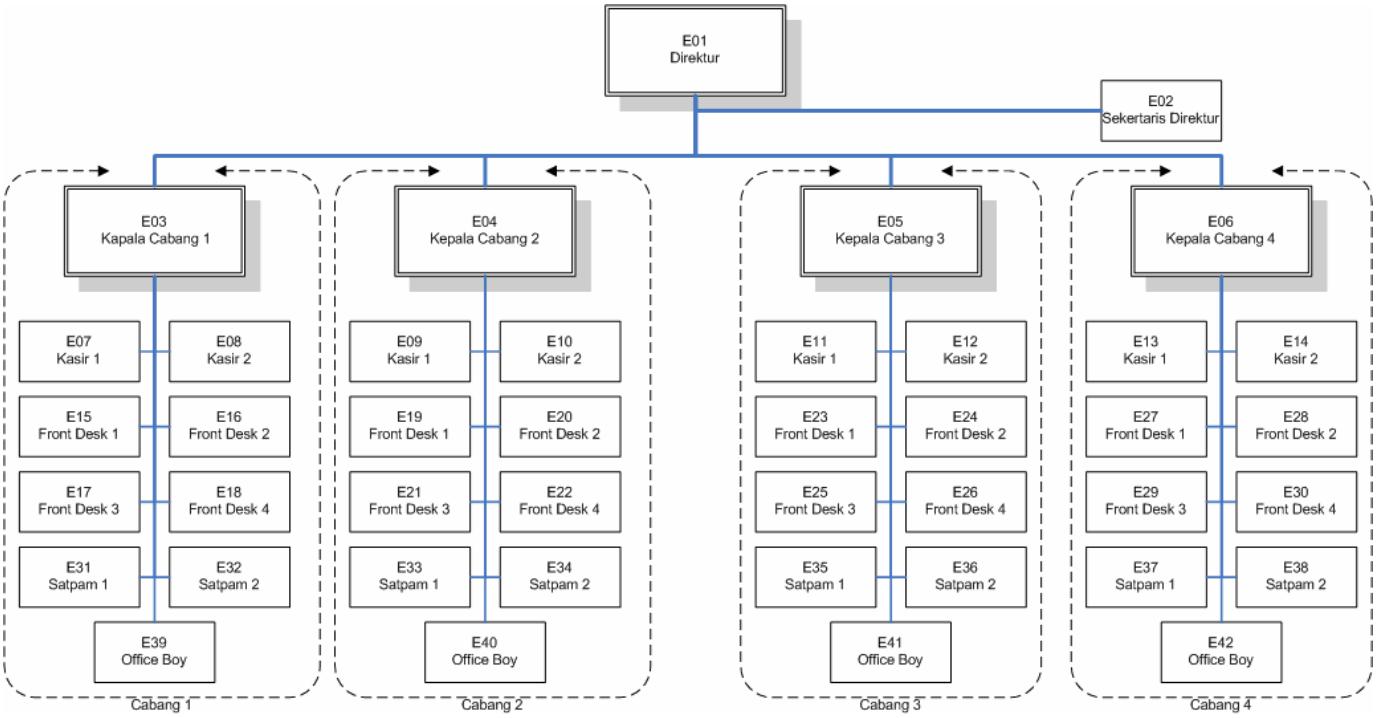
Guna membantu kegiatan operasional, setiap cabang memiliki perangkat kerja **1 unit** Server, **4 unit** komputer**,** dan **2 unit** printer yang terhubung secara lokal dan memiliki modem yang digunakan sebagai salah satu alternatif berhubungan dengan pusat serta alat pemeriksaan uang dollar, UPS pada server dan Brankas besar. Perusahaan telah memiliki aplikasi pembukuan dan keuangan, aplikasi Point of Sale serta time attendant pada setiap cabang dan aplikasi payroll hanya terdapat di pusat. Pada setiap hari jam 09.00, 15.00 dan 21.00 WIB cabang harus

melakukan download data nilai tukar dari pusat, sedangkan setiap jam 08.00 dan 20.00 harus membuat laporan harian yang diupload ke pusat. Sistem oparasi yang digunakan masih beragam karena dipengaruhi oleh aplikasi yang berjalan, seperti aplikasi pembukuan dan keuangan masih menggunakan versi dos, untuk time attendant dan payroll serta point of sale sudah berbasis windows sedangkan server masih menggunakan sistem operasi novel.

Karena produk yang diperjual belikan adalah mata uang, maka dibutuhkan perencanaan sistem keamanan yang sangat baik untuk menunjang kegiatan dan persaingan dengan para kompetitor. Sistem keamanan yang dibuat harus bisa diterapkan dengan melihat kemampuan dari karyawan dan lingkungan tempat perusahaan melakukan kegiatan, baik secara tehnologi maupun secara fisik. Pembuatan kebijakan perusahaan dan tingkat otorisasi jangan sampai menghambat kegiatan tapi juga harus mampu meminimalisasi kemungkinan terjadinya kecurangan dan atau perusakan terhadap sistem keamanan yang diterapkan.

1.4 Struktur Organisasi

Dalam menjalankan bisnisnya, maka PT. Easy Valas membutuhkan tenaga kerja untuk menunjang operasional bisnisnya. Oleh karena itu manajemen telah menyusun suatu struktur organisasi yang diharapkan dapat menunjang bisnis yang sedang dijalankan. Secara detail berikut struktur organisasi yang ada di PT. Easy Valas



Gambar 1.1 Struktur Organisasi PT. Easy Valas

Jabatan / fungsi	**Penjelasan**
Direktur	Bertanggung jawab kepada pemilik modal dalam memberikan laporan performa dari perusahaan.
Sekertaris Direktur	Bertanggung jawab memberikan informasi dan jadwal pertemuan yang telah diatur sebelumnya.
Kepala Cabang	Mengawasi seluruh kegiatan di cabang baik kegiatan operasional maupun administratif dan mengambil bagian penting sebagai penyelenggara TI sederhana untuk kantornya.
Kasir	Bertugas menerima pemeriksaan mata uang serta pembayaran yang dilakukan dari dan oleh pelanggan dengan dokumentasi yang sesuai
Front Desk	Melakukan pelayanan baik secara manual maupun melalui telepon
Satpam	Bertugas menjaga keamanan di lingkungan kerja
Office Boy	Membantu personal cabang yang lain dalam hal fotokopi, pembelian atk, dan lain-lain.

1.5 Nilai Investasi dan Pendapatan

Dalam menjalankan bisnisnya, maka PT. Easy Valas membutuhkan biaya untuk menunjang operasional bisnisnya. Oleh karena itu manajemen telah menyusun perkiraan nilai investasi dan biaya yang diharapkan dapat menunjang bisnis yang sedang dijalankan. Secara detail berikut terlampir nilai investasi dan biaya yang terdapat di PT. Easy Valas.

Tabel 1.1 Biaya Pegawai

Biaya Pegawai				
Nama Jabatan	**Gaji/bulan**	**Jumlah**	**Total Biaya**	
1.1 Direktur (E01)	Rp 7,500,000	1	Rp	7,500,000
1.2 Sekretaris Direktur (E02)	Rp 3,000,000	1	Rp	3,000,000
1.3 Kepala Cabang (E03, E04, E05, E06)	Rp 4,000,000	4	Rp	16,000,000
1.4 Front Desk (E15, E16,…,E30)	Rp 1,500,000	16	Rp	24,000,000
1.5 Kasir (E07, E08,…,E14)	Rp 2,000,000	8	Rp	16,000,000
1.6 Satpam (E31, E32,…,E38)	Rp 1,000,000	8	Rp	8,000,000
1.7 Office Boy (E39, E40,E41,E42)	Rp 900,000	4	Rp	3,600,000
		Sub Total:	**Rp**	**78,100,000**

Tabel 1.2 Belanja Barang dan Jasa

Belanja Barang dan Jasa				
Jenis Pengeluaran	**Biaya/bln/lokasi**	**Jumlah**	**Total Biaya**	
2.1 Transportasi Operasional	Rp 5,000,000	4	Rp	20,000,000
2.2 Telekomunikasi	Rp 1,000,000	4	Rp	4,000,000
2.3 Sewa Ruang / Kantor	Rp 5,000,000	4	Rp	20,000,000
2.4 Listrik	Rp 400,000	4	Rp	1,600,000
2.5 Air	Rp 200,000	4	Rp	800,000
2.6 Alat Tulis Kantor	Rp 500,000	4	Rp	2,000,000
		Sub Total:	**Rp**	**48,400,000**

Tabel 1.3 Biaya Pemeliharaan

Biaya Pemeliharaan				
Jenis Pengeluaran	**Biaya/bln/lokasi**	**Jumlah**	**Total Biaya**	
3.1 Penyusutan Peralatan IT	Rp 5,122,222	4	Rp	20,488,889
3.2 Penyusutan Asset Kantor	Rp 1,008,333	4	Rp	4,033,333
3.3 Peralatan Operasi dan Kantor	Rp 500,000	4	Rp	2,000,000
3.4 Lain-lain	Rp 1,000,000	4	Rp	4,000,000
		Sub Total:	**Rp**	**30,522,222**

dengan jenis asset untuk investasi sebagai berikut :

Tabel 1.4 Peralatan IT

Peralatan IT					
Nama Asset	**Harga**		**Qty**	**Total Investasi**	
Server	Rp	20,000,000	4	Rp	80,000,000
PC	Rp	5,000,000	16	Rp	80,000,000
UPS	Rp	1,000,000	4	Rp	4,000,000
Modem	Rp	750,000	4	Rp	3,000,000
Hub	Rp	350,000	4	Rp	1,400,000
Printer	Rp	2,000,000	8	Rp	16,000,000
			Sub Total:	**Rp**	**184,400,000**

Tabel 1.5 Asset Kantor

Asset Kantor					
Nama Asset	**Harga**		**Qty**	**Total Investasi**	
Brankas	Rp	10,000,000	4	Rp	40,000,000
Pesawat Telepon	Rp	500,000	8	Rp	4,000,000
Mesin Fax	Rp	750,000	4	Rp	3,000,000
Mesin Pemeriksa Uang Dollar	Rp	5,000,000	4	Rp	20,000,000
Mesin Hitung	Rp	500,000	4	Rp	2,000,000
Meja	Rp	1,000,000	32	Rp	32,000,000
Kursi	Rp	500,000	40	Rp	20,000,000
			Sub Total:	**Rp**	**121,000,000**

Tabel 1.6 Pendapatan

Asumsi Pendapatan	**Pendapatan/bln**	**Jml Cab.**	**Total Pendapatan**
10 orang/hari x $300/orang x 9500/$ x 30 hari/bln	Rp 855,000,000	4	Rp 3,420,000,000
	Minimum Profit (Selisih kurs) =		6.05%
	Keuntungan Kotor:		Rp 207,022,222

Spesifikasi PC lebih jelasnya terdifinisi sebagai berikut:

Tabel 1.7 Spesifikasi Produk IT

		Server	Client 1	Client 2	Client 3	Client 4
Software	**Sistem Operasi**	Novel 4	Windows XP	Windows XP	Windows XP	Windows XP
	Aplikasi		MS Word XP MS Excel XP MS Acces XP PC Any Where 9.0 McAfee Virus Scan 7.03 Pro	MS Word XP MS Excel XP MS Acces XP PC Any Where 9.0 McAfee Virus Scan 7.03 Pro	MS Word XP MS Excel XP MS Acces XP PC Any Where 9.0 McAfee Virus Scan 7.03 Pro	MS Word XP MS Excel XP MS Acces XP PC Any Where 9.0 McAfee Virus Scan 7.03 Pro
Hardware	**CPU**	Pentium IV Xeon 3.06 GHz	Pentium III 700 MHz	Pentium III 700 MHz	Pentium III 700 MHz	Pentium III 700 MHz
	HDD	Maxtor 80 GB	Quantum 40 GB	Quantum 40 GB	Quantum 40 GB	Quantum 40 GB
	Printer	Tidak ada	LX-800	Tidak ada	LX-300	Tidak Ada
	Lan Card	NIC 10/100 Ethernet Card	NIC 10/100 Ethernet Card	NIC 10/100 Ethernet Card	NIC 10/100 Ethernet Card	NIC 10/100 Ethernet Card
	Modem	External V90 US Robotic	Tidak ada	Tidak ada	Tidak ada	Tidak ada
	HUB	Dlink 8 Port	Tidak ada	Tidak ada	Tidak ada	Tidak ada
Connection	**Intranet**	IPX	TCP/IP, IPX	TCP/IP, IPX	TCP/IP, IPX	TCP/IP, IPX
	Internet	Dial-up	Tidak ada	Tidak ada	Tidak ada	Tidak ada

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 Asset

Asset dari PT. Easy Valas adalah sebagai berikut :

1. Gedung
2. Komputer (PC dan Server)
3. Printer
4. Modem
5. UPS
6. Hub
7. Brangkas
8. Pesawat Telepon
9. Mesin Fax
10. Mesin Pemeriksaan Uang Dollar
11. Mesin Hitung
12. Meja
13. Kursi

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. Berikut tabel analisa resiko yang terdifinisi yaitu :

Tabel 2.1 Analisa Resiko

No	Aset	Klasifikasi Asset	Resiko
1	Data	Informasi	terinfeksi virus / worm, dicuri
2	Dokumen perusahaan	Informasi	dicuri, hilang, terbakar
3	Dokumen jaringan komputer	Informasi	dicuri, hilang, terbakar
4	Sistem operasi server	perangkat lunak	terinfeksi virus / worm, dicuri
5	Aplikasi perkantoran	perangkat lunak	terinfeksi virus / worm, dicuri
6	Aplikasi payroll	perangkat lunak	terinfeksi virus / worm, dicuri
7	Aplikasi time attendant	perangkat lunak	terinfeksi virus / worm, dicuri
8	Aplikasi Accounting system	perangkat lunak	terinfeksi virus / worm, dicuri
9	Aplikasi Point of sale	perangkat lunak	terinfeksi virus / worm, dicuri
10	PC Server	fisik	dicuri, hilang, terbakar, rusak
11	PC Client	fisik	dicuri, hilang, terbakar, rusak
12	Modem	fisik	dicuri, hilang, terbakar, rusak
13	Hub	fisik	dicuri, hilang, terbakar, rusak
14	UPS	fisik	dicuri, hilang, terbakar, rusak
15	Printer	fisik	dicuri, hilang, terbakar, rusak
16	Pesawat Telepon	fisik	dicuri, hilang, terbakar, rusak
17	Mesin Fax	fisik	dicuri, hilang, terbakar, rusak
18	Brangkas	fisik	dicuri, hilang, terbakar, rusak
19	Mesin Pemeriksa Uang Dollar	fisik	dicuri, hilang, terbakar, rusak
20	Mesin Hitung	fisik	dicuri, hilang, terbakar, rusak
21	Meja	fisik	dicuri, hilang, terbakar, rusak
22	Kursi	fisik	dicuri, hilang, terbakar, rusak
23	Jaringan computer	layanan	putus
24	Jaringan Internet	layanan	putus
25	Jaringan telepon	layanan	putus
26	Listrik	layanan	padam

2.2 Pendidikan Keamanan

Agar resiko menjadi lebih kecil maka perlu disosialisasikan kepada semua pegawai. Caranya dengan memberikan pendidikan 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.

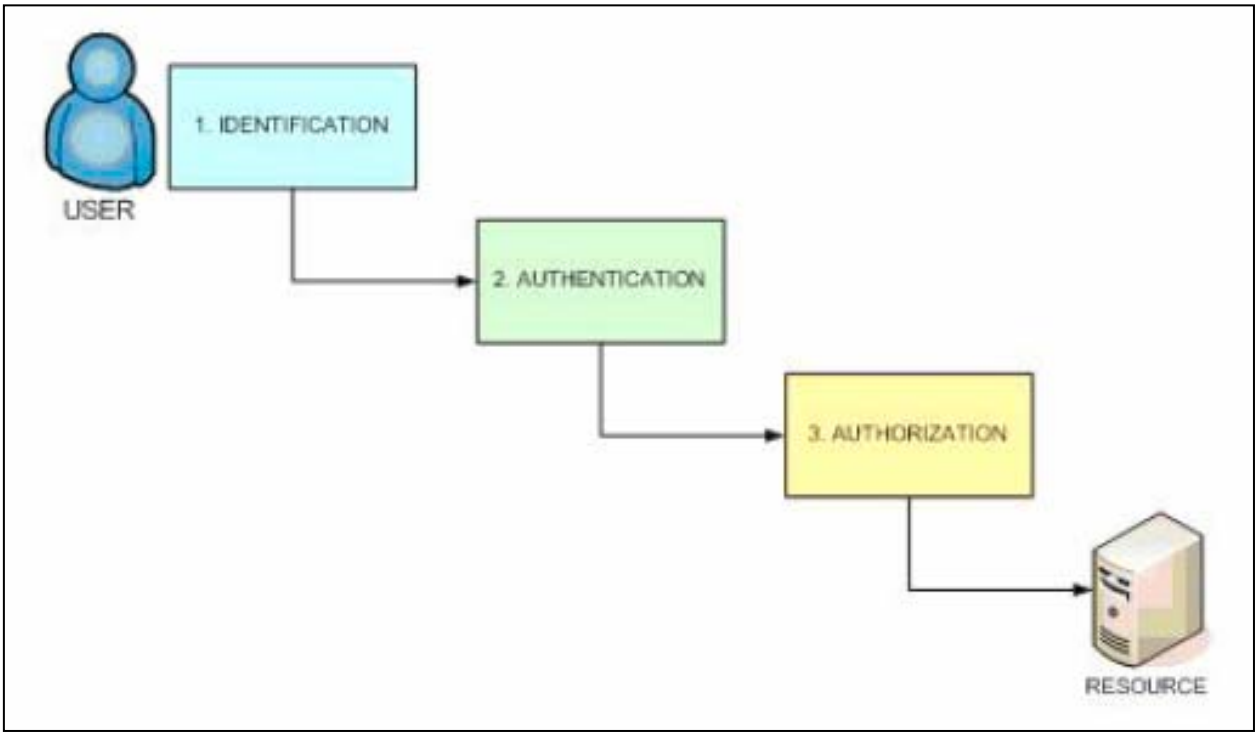
BAB III
METODOLOGI DAN SISTEM KONTROL AKSES

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 Access Control Systems & Methodology

Access Control Systems & Methodology adalah mekanisme dan metode yang dipergunakan para administrator/manager untuk mengendalikan apa yang boleh diakses pemakai (*user)*, termasuk apa yang boleh dilakukan setelah otentikasi dan otorisasi, termasuk pemantauannya.

Berikut ini adalah gambar yang mengilustrasikan tahapan dalam mengakses sistem informasi mata uang pada PT. Easy Valas.



Gambar 3.1 Tahapan user masuk ke dalam sistem

3.1.1 Identification

Untuk proses identifikasi ini sistem akan menanyakan *user id* dan *password* dari pegawai yang akan menggunakan sistem ini. Dan sebagai identifikasi fisik dari seorang pegawai diberi tanda pengenal yang diberikan nomor pegawai.

3.1.2 Authentication

Dalam melakukan *authentication*, PT. Easy Valas hanya menggunakan tipe yang pertama saja yaitu "*Something you know*" dengan menerapkan *password* setiap kali *user* akan masuk ke dalam sistem. Pada periode waktu yang telah ditetapkan, password harus dirubah oleh user itu sendiri.

3.1.3 Authorization

Setelah proses autentifikasi maka sistem akan menentukan aplikasi-aplikasi mana yang menjadi wewenang dari *user* tersebut. Authorization berarti pemberian izin bagi seseorang untuk mengakses atau melakukan sesuatu.

3.2 Controls

3.2.1 Administrative controls

o *Background checks*

Proses pemilihan pegawai dilakukan dengan melihat latar belakang pendidikan dan pengalaman dari calon pegawai tersebut. Dan salah satu hal penting adalah sikap dasar calon pegawai. Perusahaan tidak ingin menerima pegawai yang terlalu menyombongkan kepandaiannya. Orang semacam ini nantinya akan menjadi penghambat majunya perusahaan.

o *Separation of duties*

Setiap pegawai pada PT. Easy Valas sudah memiliki *jobdescription* nya masing masing sehingga tanggung jawab untuk suatu pekerjaan menjadi jelas.

3.2.2 Logical controls

o *Password*s

Masing-masing pegawai yang berwenang menggunakan sumber daya tekno*log*i informasi memiliki *password* yang unik yang dapat diganti kapan saja oleh pengguna (*user*) yang bersangkutan dan administrator. Perusahaan menganjurkan agar *password* tersebut diganti secara berkala untuk menghindari pencurian *password*.

3.2.3 Physical controls

o *Guards*

Untuk physical security PT. Easy Valas menggunakan satpam untuk menjaga pintu utama tempat keluar masuknya pegawai dan pelanggan.

o *Locks*

Pada setiap pintu diberikan kunci agar tidak dapat dimasuki oleh sembarang orang, dan jika jam kerja sudah selesai maka pintu utama akan dikunci oleh satpam.

o Safety Box

Terdapat minimal satu safety box anti api selama 8 jam pada setiap kantor dengan kombinasi angka dan kunci utama yang disesuaikan dengan kebutuhan.

3.3 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).

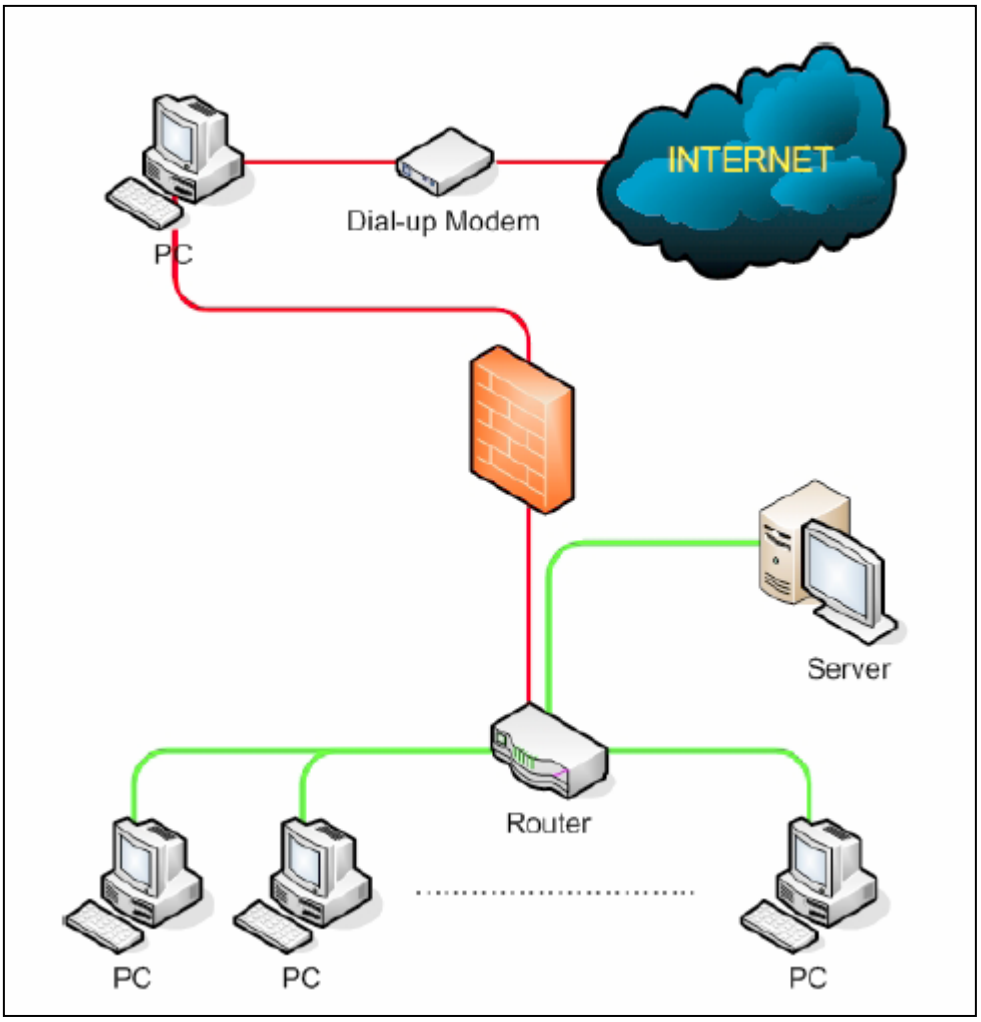
• *Application-level events* (pesan-pesan kesalahan aplikasi, *file* yang dibuka dan ditutup, modifikasi *file*, dan pelanggaran keamanan terhadap aplikasi).

• *User-level events* (percobaan identifikasi dan autentikasi, *file*-servis-dan sumber daya yang dipakai, perintah yang diberikan, dan pelanggaran keamanan).

BAB IV
TELECOMMUNICATIONS DAN NETWORK SECURITY SERTA SECURITY MANAGEMENT PRACTICES

4.1 Telecommunications and Network security

Tujuan *Telecommunications and Network Security* adalah mempelajari berbagai aspek keamanan yang terkait dengan berbagai jenis jaringan komputer / telekomunikasi. Berikut ini adalah gambar yang mengilustrasikan jaringan yang menghubungkan perangkat teknologi informasi (menggunakan topo*log*i tree) yang terdapat pada PT. Easy Valas.



Tabel 4.1 Design Jaringan

Dapat dilihat pada gambar diatas bahwa jaringan pada PT. Easy Valas. Terhubung ke Internet melalui sebuah modem *dial up* sehingga akses ke Internet hanya dilakukan untuk periode waktu yang terbatas (tidak selalu *online*), kemudian koneksi dari modem *dial up* tersebut dihubungkan ke sebuah PC. PC yang

memiliki koneksi ke Internet tersebut dihubungkan ke sebuah *hub* yang terdapat di belakang sebuah *firewall*. Selama koneksi ke Internet PC tersebut diputuskan dari jaringan untuk menghindari ancaman dari jaringan Internet.

Server dan PC lain tidak dapat mengakses Internet. Setelah PC tersebut mengakses Internet maka harus dilakukan prosedur pengecekan menggunakan aplikasi anti *virus* baru dapat dihubungkan kembali ke jaringan.

Apabila dilihat pada gambar diatas ancaman yang datang dari jaringan diluar kemungkinan besar adalah *virus*, trojan, *worm*, dan *spyware*, karena ancaman-ancaman seperti inilah yang banyak terdapat pada Internet, dan untuk mengantisipasi hal tersebut maka pada saat PC yang dapat melakukan koneksi ke Internet diputuskan pada jaringan selama koneksi ke Internet, selain itu setiap perangkat komputer dan server dilengkapi dengan aplikasi anti *virus* dan sistem operasi yang digunakan selalu diupdate secara berkala (setiap minggu sekali).

Serangan lain seperti Dos, *smurf*, *teardrop*, *flood*, atau Ddos kemungkinan terjadinya sangat kecil karena server pada jaringan PT. Easy Valas tidak terhubung ke Internet, sehingga penyerangan menggunakan metode tersebut akan tidak mungkin dilakukan oleh penyerang yang berasal dari jaringan diluar PT. Easy Valas. Kemungkinan besar penyerangan dilakukan dari dalam jaringan itu sendiri, tetapi hal ini akan diatasi oleh penerapan kebijakan-kebijakan yang akan dibahas pada domain keamanan yang lain.

4.2 Security Management Practices

Tujuan *Security Management Practices* adalah mempelajari cara untuk mengidentifikasi asset perusahaan (terutama *information asset*), berikut cara terbaik untuk menentukan tingkat pengamanannya, serta anggaran yang patut untuk implementasi keamanannya. Pada PT. Easy Valas praktek manajemen keamanan dilakukan untuk melindungi aset-aset perusahaan, baik itu aset *log*ikal dan aset fisik. Aset *log*ikal adalah informasi yang terdapat pada sistem informasi mata uang, praktek-praktek manajemen keamanan untuk aset *log*ikal ini adalah sebagai berikut :

- *Password* sistem informasi mata uang tidak boleh diberitahukan kepada siapa pun.
- *Password* harus diganti secara berkala / periodik.
- Apabila pihak manajemen mengetahui adanya kebocoran *password* dari salah seorang pegawai maka pegawai tersebut akan dikenakan sangsi, sesuai kebijakan manajemen.
- Penerapan metode *password* yang baik (gabungan karakter dan angka minimal enam buah karakter dan menghindari penggunaan *password* berupa tanggal, nama, dan kata2 yang terdapat pada kamus), hal ini untuk menghindari dictionary attack atau birthday attack.

- Penulisan *password* pada suatu media hardcopy seperti kertas, sticknote, dan media lainnya tidak boleh ditaruh pada meja ruang kerja, hal ini termasuk laci, lemari pada ruang kantor.

Sedangkan aset fisik adalah aset perusahaan seperti perangkat tekno*log*i informasi, berkas-berkas, kas perusahaan, perangkat-perangkat lain didalam kantor. Praktek-praktek manajemen untuk menjaga keamanan aset fisik ini adalah :

- Mengandalkan keamanan dalam hal ini satpam yang dilengkapi dengan perangkat komunikasi yang dapat langsung terhubung ke pos polisi terdekat.
- Dalam jam kerja pengamanan juga dilakukan oleh semua pegawai dalam perusahaan tanpa pengecualian, berkoordinasi dengan satpam (pengamanan yang sudah biasa tidak tertulis apabila mendapatkan sesuatu yang mencurigakan maka menghubungi satpam untuk ditindak lanjuti).
- Apabila ada pihak yang menemukan berkas / form berserakan, maka berkas itu harus segera diberikan kepada pegawai pada bagian yang bersangkutan, berkas tersebut dilarang keras untuk dibuang, tanpa perintah dari pegawai yang berwenang.

BAB V
APPLICATION DAN SYSTEM DEVELOPMENT SECURITY SERTA CRYPTOGRAPHY

5.1 Application & Systems Development Security

Tujuan *Application & Systems Development Security* adalah mempelajari berbagai aspek keamanan kontrol-kontrol yang terkait pada pengembangan sistem informasi. Dalam pengembangan sistem informasi pertukaran Mata Uang pada PT. Easy Valas aspek keamanan juga sudah diterapkan. Beberapa komponen pengamanan yang dikembangkan pada saat pengembangan sistem informasi pertukaran Mata Uang adalah :

- Pengembangan sistem keamanan berdasarkan *username* dan *password* dan tingkatan akses.
- Pengawasan data yang akan diinputkan ke dalam sistem, misalnya :
  - *field* yang meminta input angka, maka sistem akan menolak input berupa karakter.
  - Sistem tidak akan menerima input lebih besar dari yang dapat ditampung (misal apabila *field* nama dibatasi 15 karakter maka sistem tidak akan menerima karakter ke-16 dan seterusnya).
  - Sistem mampu menganalisa kemungkinan adanya input yang berupa perintah sql (mencegah *sql injection*).
- Pengembangan sistem untuk pencatatan aktifitas akses (*log* akses).
- Pengaturan sistem keamanan dalam database server (jadi hanya sistem informasi dan administrator yang dapat mengakses database server).
- Pengawasan berkala akan kinerja sistem informasi pertukaran Mata Uang sehingga kesalahan-kesalahan ataupun kelemahan-kelemahan sistem akan dapat dipantau dan segera diperbaiki.

5.2 Cryptography

Tujuan *Cryptography* adalah mempelajari berbagai metode dan teknik penyembunyian data menggunakan kriptografi. Pada sistem informasi mata uang yang dimiliki oleh PT. Easy Valas data yang di proteksi hanya data *password* untuk tiap *user* yang digunakan untuk mengakses sistem informasi mata uang. Data *password* ini terdapat pada database server sistem informasi mata uang. Sedangkan data lain yang terdapat pada database server tidak diproteksi secara langsung hanya mengandalkan sistem keamanan yang built-in pada database server dan sistem operasi Novel.

Alasan utama mengapa hanya data *password* yang diproteksi adalah karena apabila penyusup berhasil menyusup ke dalam database server maka penyusup hanya akan mendapatkan data yang tersebar di dalam tabel-tabel database dan untuk menggabungkan informasi tersebut akan rumit sekali, tetapi apabila penyusup berhasil mendapatkan *password* maka penyusup dapat memasuki sistem informasi mata uang

dan informasi-informasi yang terdapat di dalam sistem informasi tersebut dapat dengan mudah dimengerti, dibandingkan dengan data-data yang langsung diambil dari database server.

BAB VI
SECURITY ARCHITECTURE DAN MODEL SERTA OPERATION SECURITY

6.1. Security Architecture & Models

Tujuan *Security Architecture & Models* adalah mempelajari berbagai konsep, prinsip dan standar untuk merancang dan mengimplementasikan aplikasi, sistem operasi, dan sistem yang aman. Ilustrasi arsitektur pada PT. Easy Valas dapat dilihat pada gambar 6.1.

6.1.1 *Security Models*

Untuk memformalkan kebijakan keamanan dalam organisasi, PT. Easy Valas menggunakan *Access Control Matrix Model*, yang menentukan apa yang boleh dan yang tidak boleh diakses oleh *user*. Sistem informasi pada PT. Easy Valas merupakan sistem yang tertutup dan tidak bisa di akses dari luar kantor PT. Easy Valas.

Access Control Matrix Model untuk aset logikal yang terdapat dalam sistem informasi pertukaran Mata Uang dapat dilihat pada tabel di bawah ini. *Access Control Matrix Model* untuk aset fisik yang merupakan hasil *hardcopy* sistem informasi pertukaran Mata Uang atau berkas-berkas fisik lainnya dapat dilihat pada tabel 6.1. *Access Control Matrix Model* untuk aset fisik peralatan TI lainnya dapat dilihat pada tabel 6.1.

6.2. Operations Security

Tujuan *Operations Security* adalah mempelajari teknik-teknik kontrol pada operasi personalia SI, sistem informasi dan perangkat keras.

6.2.1 Administrative Management

Untuk mengatur fungsi-fungsi dalam sistem informasi mata uang yang berhubungan dengan keamanan sistem diserahkan kepada seorang administrator yang dipegang oleh Kepala Cabang. Administrator ini memiliki beberapa *job description*s, yaitu :

- *Least privilege*

Administrator dalam hal ini menentukan apa yang boleh dan yang tidak boleh diakses oleh *user*. Ada 3 macam ketentuan dari *least privilege* yaitu :

- *Read only* : hanya dapat membaca saja.
- *Read / Write* : dapat menulis tetapi tidak dapat merubah data asli.
- *Access change* : dapat merubah data dari tempat asalnya.

- *Separations of duties*

Administrator menentukan *job description* dari masing-masing pegawai sehingga jelas pekerjaan apa saja yang menjadi tanggung jawab mereka.

- *Need to know*

Administrator membatasi data-data apa saja yang perlu diketahui oleh *user*.

- *Job rotation*

PT. Easy Valas tidak melakukan *job rotation* karena jumlah sumber daya yang terbatas.

- *Mandatory vacation*

PT. Easy Valas tidak melakukan *mandatory vacation* tetapi pada bagian-bagian tertentu yang rentan terhadap kecurangan dilakukan pengawasan yang cukup ketat. Misalnya pada bagian Kasir, Kepala Cabang melakukan pengawasan ketat terhadap uang yang keluar maupun uang yang masuk.

6.2.2 Control

a. Categories of Control

- *Preventive Control*

  Preventive control dilakukan untuk mengurangi jumlah dan akibat yang ditimbulkan oleh *error*. Hal ini dilakukan dengan cara membatasi akses *user* ke dalam sistem, sehingga hanya *user* yang memiliki wewenang saja yang boleh mengakses sistem tersebut.

- *Detective Control*

  Apabila *error* tersebut tidak dapat dihindari dan tetap terjadi juga, maka perlu adanya pendeteksian mengapa *error* tersebut sampai terjadi. Salah satu cara untuk mendeteksi hal ini adalah dilakukan dengan cara memeriksa *log file* dari sistem.

- *Corrective (recovery) Control*

  Jika terjadi *error* maka perlu adanya penanganan cepat untuk mengembalikan fungsi dari sistem informasi bengkel tersebut. Hal ini dapat dengan cepat dilakukan dengan menggunakan data-data *backup* sistem pada hari sebelumnya.

b. Record retention

Data-data mengenai nilai mata uang dan perubahannya seperti data pelanggan, data nilai mata uang pada saat tertentu dan data transaksi dipertahankan selama 3 bulan di dalam sistem. Setelah itu data-data tersebut di *backup* ke dalam media penyimpanan yang terpisah. Dan diletakkan di lokasi yang berbeda.

c. Privilege Entity Control

Hanya jajaran direksi yang memiliki akses menyeluruh terhadap data-data yang ada dalam sistem informasi mata uang.

6.2.3 Email

Tidak ada pengamanan khusus untuk email dari dan keluar kantor ini. Untuk pengiriman email digunakan protokol *Simple Mail Transfer Protoco*l (SMTP) dan untuk pengambilan email menggunakan protokol POP3 dengan *user name* dan *password* yang unik. *Signature* yang sederhana digunakan untuk

setiap pengiriman email. Untuk menanggulangi *spam* yang masuk ke dalam email *account* kantor, PT. Easy Valas hanya menggunakan filter yang disediakan oleh perangkat lunak penanganan email.

6.2.4 *Attacking: Terms and Methods*

Serangan-serangan yang mungkin terjadi pada PT. Easy Valas diantaranya adalah :

- Pencurian data baik data *log*ikal maupun berkas / form hasil print out. Contohnya pencurian *password* dengan shoulder surfing, eavesdroping, dan lain-lain.
- Pengubahan data pada sistem informasi pertukaran Mata Uang.
- Penyusupan sistem dengan komponen perusak seperti *virus*, *worm*, *spyware*, dan lain-lain.
- Perusakan sistem informasi pertukaran Mata Uang dengan merusak peralatan tekno*log*i informasi secara fisik.

Tabel 6.1 ***Access Control Matrix Model***

Jabatan	Server Pusat	Server Cabang	Komputer Pusat	Komputer Cabang	Internet	Payroll System	Time Attendent	Accounting System	Point of Sale	Telepon	Fax
Direktur	R	R	R	R	F	R	R	R	R	F	F
Sekretaris Direktur	R	R	R	R	F	F	F	F	R	F	F
Kepala Cabang 1	R	F	N	R	F	R	R,U	R	R	F	F
Kepala Cabang 2	R	F	N	R	F	R	R,U	R	R	F	F
Kepala Cabang 3	R	F	N	R	F	R	R,U	R	R	F	F
Kepala Cabang 4	R	F	N	R	F	R	R,U	R	R	F	F
Kasir 1 Cabang 1	N	N	N	N	N	N	R,U	F	R,U	F	F
Kasir 2 Cabang 1	N	N	N	N	N	N	R,U	F	R,U	F	F
Kasir 1 Cabang 2	N	N	N	N	N	N	R,U	F	R,U	F	F
Kasir 2 Cabang 2	N	N	N	N	N	N	R,U	F	R,U	F	F
Kasir 1 Cabang 3	N	N	N	N	N	N	R,U	F	R,U	F	F
Kasir 2 Cabang 3	N	N	N	N	N	N	R,U	F	R,U	F	F
Kasir 1 Cabang 4	N	N	N	N	N	N	R,U	F	R,U	F	F
Kasir 2 Cabang 4	N	N	N	N	N	N	R,U	F	R,U	F	F
Front Desk 1 Cabang 1	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 2 Cabang 1	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 3 Cabang 1	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 4 Cabang 1	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 1 Cabang 2	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 2 Cabang 2	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 3 Cabang 2	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 4 Cabang 2	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 1 Cabang 3	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 2 Cabang 3	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 3 Cabang 3	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 4 Cabang 3	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 1 Cabang 4	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 2 Cabang 4	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 3 Cabang 4	N	N	N	N	N	N	R,U	N	F	F	F
Front Desk 4 Cabang 4	N	N	N	N	N	N	R,U	N	F	F	F
Satpam 1 Cabang 1	N	N	N	N	N	N	R,U	N	N	N	N

Satpam 2 Cabang 1	N	N	N	N	N	N	R,U	N	N	N	N
Satpam 1 Cabang 2	N	N	N	N	N	N	R,U	N	N	N	N
Satpam 2 Cabang 2	N	N	N	N	N	N	R,U	N	N	N	N
Satpam 1 Cabang 3	N	N	N	N	N	N	R,U	N	N	N	N
Satpam 2 Cabang 3	N	N	N	N	N	N	R,U	N	N	N	N
Satpam 1 Cabang 4	N	N	N	N	N	N	R,U	N	N	N	N
Satpam 2 Cabang 4	N	N	N	N	N	N	R,U	N	N	N	N
Office Boy Cabang 1	N	N	N	N	N	N	R,U	N	N	N	N
Office Boy Cabang 2	N	N	N	N	N	N	R,U	N	N	N	N
Office Boy Cabang 3	N	N	N	N	N	N	R,U	N	N	N	N
Office Boy Cabang 4	N	N	N	N	N	N	R,U	N	N	N	N

BAB VII
DISASTER RECOVERY DAN BUSINESS CONTINUITY PLAN SERTA LAWS, INVESTIGATION DAN ETHICS

7.1 Disaster Recovery & Business Continuity Plan

Tujuan *Disaster Recovery & Business Continuity Plan* adalah mempelajari bagaimana aktifitas bisnis dapat tetap berjalan meskipun terjadi gangguan atau bencana.

7.1.1 Asuransi.

PT. Easy Valas mengasuransikan seluruh peralatan dan gedung yang digunakan untuk kegiatan operational kantor. Asuransi ini dilakukan untuk mengantisipasi apabila terjadi bencana yang menimpa kantor tersebut.

7.1.2 *Backup*

PT. Easy Valas melakukan *disaster recovery* dengan melakukan *backup database* secara berkala. Proses *backup* ini dilakukan setiap hari pada saat kegiatan perubahan shift kerja sudah selesai. Media *backup* yang digunakan adalah CD-RW untuk harian sebanyak 6 buah (Senin sampai Sabtu) agar dapat ditimpa terus menerus dan untuk *backup* bulanan menggunakan CD-R biasa, data *backup* ini kemudian disimpan pada brankas kecil / wadah penyimpanan yang dapat dibawa-bawa. Data *backup* disimpan pada dua tempat yang berbeda, yaitu di dalam kantor PT. Easy Valas (*hot site*) dan di luar komplek PT. Easy Valas (*cold site*).

Berikut ini adalah prosedur apabila terjadi kerusakan data dalam sistem informasi mata uang, yaitu :

- Apabila terdeteksi adanya data yang terkorupsi, pegawai administrasi harus menghubungi kepala cabang untuk meminta ijin untuk memasukkan data hasil *backup*.
- Apabila diijinkan dengan pengawasan dari kepala cabang data *backup* diambil dari tempat penyimpanan.
- Masukkan data hasil backup hari kemarin ke sistem informasi.
- Deteksi apakah data tersebut mengalami kerusakan apa tidak, apabila ya ulangi langkah kedua untuk data backup untuk hari sebelum kemarin dan seterusnya.
- Apabila masalah telah teratasi simpan kembali data *backup* ke tempat semula.

Berikut ini adalah prosedur apabila terjadi kerusakan sistem operasi, yaitu :

- Hubungi kepala cabang dan pegawai administrasi untuk meng-*install* ulang sistem operasi.
- Ambil program sistem operasi dari tempat penyimpanan.
- Pegawai administrasi meng-*install* ulang sistem operasi.

- Apabila sudah selesai instalasi program sistem operasi dikembalikan ke tempat penyimpanan.

Berikut ini adalah prosedur apabila terjadi kerusakan perangkat TI yang tidak dapat ditangani oleh pegawai administrasi, yaitu :

- Hubungi kepala cabang.
- Kemudian kepala cabang menghubungi *vendor* peralatan TI tersebut, untuk meminta bantuan teknis.
- Setelah bantuan teknis dari vendor sudah datang, kepala cabang dapat menyuruh pegawai administrasi untuk mengawasi perbaikan peralatan TI, apabila peralatan tersebut harus dibawa untuk diperbaiki maka harus ada surat bukti pengambilan barang.

7.1.3 *Recovery Plan Testing.*

Proses pengujian media *backup* ini sudah dilakukan pada awal pembangunan sistem dan setiap setengah tahun sekali dilakukan pengujian ulang terhadap media *backup* ini yang diikuti oleh orang-orang yang terkait langsung dengan sistem.

7.1.4 *Business Continuity Plan*

Sebelum adanya Sistem Informasi yang digunakan sebagai alat bantu kegiatan operasional cabang, PT. Easy Valas sudah memiliki sistem prosedur manual yang sudah berjalan dengan baik. Sistem manual ini dilakukan menggunakan form-form khusus pada masing-masing kegiatan operasional. Untuk *business continuity plan* apabila terjadi kerusakan pada sistem informasi bengkel, PT. Easy Valas menggunakan form-form tersebut untuk mencatat kegiatan operasional cabang untuk sementara. Dan apabila sistim informasi mata uang sudah berjalan kembali, data-data yang terdapat dalam form-form manual tersebut di *entry* ke dalam sistem.

7.2. Laws, Investigations & Ethics

Tujuan *Laws, Investigations & Ethics* adalah mempelajari berbagai jenis aturan yang terkait dengan kejahatan komputer dan legalitas transaksi elektronik, serta membahas masalah etika dalam dunia komputer. Pada PT. Easy Valas kemungkinan kejahatan yang terjadi, adalah :

- Pencurian data baik data *log*ikal maupun berkas / form hasil *print out.*
- Pengubahan data pada sistem informasi pertukaran Mata Uang.
- Penyusupan sistem dengan komponen perusak seperti *virus, worm, spyware,* dan lain-lain.
- Perusakan sistem informasi pertukaran Mata Uang dengan merusak peralatan tekno*log*i informasi secara fisik.

Penanggulanagan terhadap kemungkinan kejahatan diatas sudah diantisipasi dan penindaklanjutan terhadap kegiatan kejahatan tersebut dapat dilihat pada domain-domain yang lain. Mengenai tindakan hukum maka kejahatan untuk pencurian data, pengubahan data, dan perusakan sistem dapat dilaporkan pada yang berwajib, tetapi biasanya masalah tersebut di Indonesia diselesaikan dengan cara kekeluargaan apabila hal tersebut masih memungkinkan, sedangkan untuk kejahatan seperti *virus*, *worm*, trojan, dan lain-lain belum ada perangkat hukum di Indonesia yang dapat mengakomodasikan tindak-tindak kejahatan seperti ini.

BAB VIII
PHYSICAL SECURITY
SERTA AUDITING DAN ASSURANCE

8.1 Physical Security

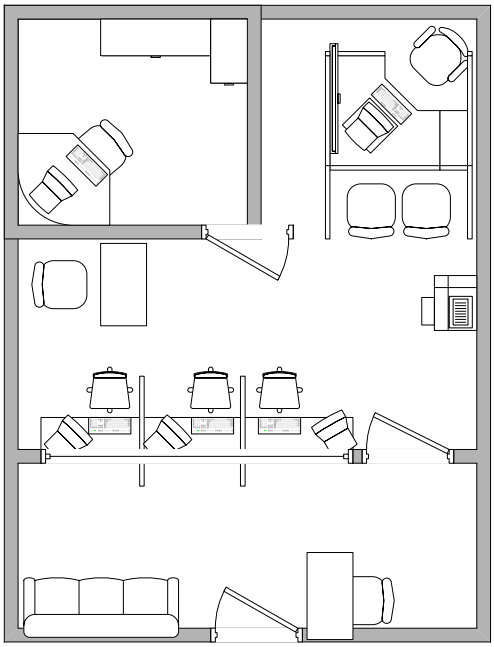
Tujuan *Physical Security* adalah mempelajari berbagai ancaman, resiko dan kontrol untuk pengamanan fasilitas sistem informasi. Untuk *physical security* PT. Easy Valas mengaplikasikan beberapa metode pengamanan untuk menjaga fasilitas sistem informasi mata uang. Metode-metode tersebut diantaranya adalah :

1. Hanya ada satu pintu utama yang digunakan arus untuk keluar dan masuk ke dalam lingkungan kantor. Ini disebabkan karena jumlah pelanggan yang lewat sangat bervariasi.
2. Pintu utama ini dijaga oleh satpam selama 24 jam dengan dibagi menjadi 3 *shift*. *Shift* pertama adalah jam 06.00 sampai dengan jam 14.00, shift kedua jam 13.00 sampai dengan jam 21.00 dan shift terakhir 20.00 sampai jam 07.00. Tugas dari satpam ini adalah untuk menjaga keamanan lingkungan kantor dan mencatat nomor polisi dari mobil yang ada di lingkungan kantor.
3. Pada area kantor yang sangat padat ini pasti terdapat resiko kebakaran. Resiko kebakaran ini termasuk cukup besar untuk sebuah kantor yang beroperasi 24 jam. Untuk mencegahnya adalah dengan cara memberikan pelatihan-pelatihan kebakaran (fire drill) untuk menanggulangi apabila terjadi kebakaran. Pelatihan ini dilaksanakan dengan mengundang petugas dari Dinas Kebakaran. Untuk mencegah resiko kebakaran yang diakibatkan karena konsleting dari arus listrik PT. Easy Valas menggunakan sebuah stabiliser listrik dengan kapasitas sedang. Apabila memang kebakaran tidak dapat dihindari lagi maka harus dilakukan tindakan yang cepat untuk menanggulanginya. Pada PT. Easy Valas terdapat 2 buah keran air yang ditempatkan pada depan dan belakang kantor sehingga pendistribusian air cukup merata di sekitar kantor. Selain menggunakan air sebagai media pencegahan pertama apabila terjadi kebakaran di lingkungan kantor, PT. Easy Valas menyediakan sebuah peralatan pemadam api (*fire extinguisher*) berkapasitas 5 kg.
4. Ruang Kantor utama PT. Easy Valas terdapat di dalam sekat berkaca satu arah yang hanya memiliki satu pintu masuk, ruangan paling depan adalah ruangan tunggu tamu, setelah itu terdapat beberapa ruangan yang didalamnya terdapat aset-aset perusahaan seperti perangkat tekno*log*i informasi, berkas-berkas (*form-form*), dan kas kantor. Ruangan yang berisi aset ini hanya boleh diakses oleh pegawai yang berwenang, selain dari pegawai yang berwenang dilarang masuk, kecuali atas ijin dan pengawasan dari pegawai yang berwenang. Hal ini juga berlaku bagi petugas cleaning service dan satpam, mereka hanya boleh masuk apabila diijinkan dan diawasi oleh pegawai yang berwenang. Dalam keadaan yang membahayakan seperti kebakaran pada malam hari, apabila petugas keamanan (satpam) tidak mampu menangani kobaran api maka ia diperbolehkan untuk masuk menggunakan

kunci darurat untuk menyelamatkan aset-aset perusahaan terutama data-data *backup* sistem informasi. Kunci darurat disimpan ditempat yang hanya diketahui oleh kepala cabang dan satpam, kunci ini disimpan dalam wadah tertutup sehingga untuk mengambil kunci ini maka diperlukan usaha untuk membuka paksa wadah tersebut (wadah yang sudah rusak tidak dapat diperbaiki kembali, konsepnya sama seperti alarm kebakaran pada gedung-gedung atau mall-mall yang tertutup kaca dan apabila dirusak maka wadah itu akan tetap rusak), kemudian ia harus melaporkan kepada kepala cabang mengenai kejadian ini.

5. Selain itu untuk membantu sistem keamanan maka pada pos satpam juga dilengkapi dengan sebuah alat komunikasi yang dapat melakukan hubungan langsung ke Pos polisi dan atau kantor polisi terdekat, ini memungkinkan untuk memberikan informasi secara cepat dan efisien kepada pihak yang terkait.

Selanjutnya layout ruangan setiap Cabang PT EASY VALAS dapat dilihat pada Gambar berikut ini.



Gambar. Layout Ruangan PT EASY VALAS

8.1.1 Prosedur penanganan kebakaran dan musibah

Terdapat beberapa prosedur yang ditetapkan PT. Easy Valas dalam menangani kebakaran dan musibah, yang harus dipatuhi oleh semua pegawai untuk menjamin keselamatan jiwa para pegawai PT. Easy Valas. Prosedur yang harus dilakukan pegawai PT. Easy Valas pada saat terjadi kebakaran adalah :

- Berusahalah untuk tetap tenang (tidak panik).
- Bunyikan tanda kebakaran yang tersedia (alarm).
- Segera laksanakan prosedur evakuasi yang telah ditetapkan, yaitu pergi ke pintu keluar dengan tenang (hal ini berlaku untuk semua pegawai) apabila api sudah tidak dapat dikendalikan lagi, apabila api belum besar maka harus dilakukan proses penyemprotan api dengan alat pemadam kebakaran oleh pegawai yang terdekat dengan peralatan pemadam kebakaran tersebut. Satpam berusaha membantu proses evakuasi pegawai keluar dari komplek bengkel, apabila hal tersebut dirasa masih memungkinkan.
- Bila terjebak asap, berusahalah supaya asap tidak terlalu banyak terhirup. Bila asap terlalu tebal, usahakan supaya posisi Anda serendah mungkin. Gunakan kain atau tissue basah untuk menutupi hidung.
- Hubungi pihak pemadam kebakaran.

Prosedur yang harus dilakukan pegawai PT. Easy Valas apabila pakaian mereka terbakar api adalah :

- BERHENTI di mana Anda berada.
- JATUHKAN DIRI ke lantai.
- BERGULING terus menerus, tutupi wajah dan mulut Anda dengan telapak tangan (hal ini akan mencegah api membakar wajah dan asap masuk ke paru-paru). Bergulinglah hingga api padam.
- DINGINKAN luka bakar dengan air selama 10 - 15 menit. Cari bantuan dari paramedik bila diperlukan.

Prosedur dalam menggunakan alat pemadam kebakaran *portable* (*fire extinguisher*) adalah :

- Perhatikan jenis pemadam, dari label yang tertera pada dinding tabung,
- Cabut pen pengaman,
- Pegang tabung pengaman dengan kuat,
- Ambil jarak secukupnya lalu arahkan corong pemadam pada api yang akan dipadamkan,
- Tekan tuas pembuka dan lakukan gerakan menyapu dari sisi ke sisi hingga api padam.

Prosedur yang harus dilakukan pegawai PT. Easy Valas pada saat terjadi bencana gempa bumi adalah :

- Berusahalah untuk tetap tenang.
- Bila Anda berada di luar ruangan, segera menuju daerah terbuka yang jauh dari pohon atau gedung.
- Bila Anda berada di dalam ruangan, bersembunyilah di bawah meja atau perabot yang dapat melindungi Anda.
- Setelah getaran berhenti, segera menuju ke pintu keluar dengan tetap tenang.
- Jangan mencoba kembali ke dalam gedung, sebelum ada pemberitahuan dari pihak berwenang.

Prosedur yang harus dilakukan pegawai PT. Easy Valas pada saat terjadi kecelakaan dalam pekerjaan adalah :

- Hentikan aktifitas pekerjaan yang berada dalam radius jarak 10 meter dari tempat terjadinya kecelakaan untuk menghindari terjadinya kecelakaan lebih lanjut.
- Segera lakukan pertolongan pertama dengan peralatan P3K.
- Apabila memungkinkan pindahkan korban ke tempat perawatan (di dalam kantor).
- Hubungi ambulans atau berusaha membawa korban ke rumah sakit terdekat, apabila kecelakaan tersebut tidak dapat ditangani.

Berikut ini adalah daftar nomor telepon penting yang dapat digunakan apabila terjadi kebakaran dan musibah, yaitu :

- Polisi 110
- Ambulans 118
- Pemadam Kebakaran 113
- P.L.N. 123

8.2 Auditing & Assurance

Tujuan *Auditing & Assurance* adalah memperkenalkan konsep dasar auditing sistem informasi terkait dengan masalah keamanan sistem informasi. Pada PT. Easy Valas konsep audit sistem informasi sudah dijalankan dengan cara mengamati / memantau kinerja sistem informasi mata uang dan operational secara berkala. Pengauditan sistem informasi secara berkala ini dijalankan untuk mencegah (*prevention*), mengetahui / mendeteksi (*detection*), dan mengambil tindakan yang diperlukan untuk mengatasi kesalahan yang sudah terjadi (*correction*). Pengauditan berkala ini dilakukan dilakukan tiap hari untuk skala pengoperasian (apabila ada kesalahan yang bukan tergolong kesalahan human *error*, seperti kesalahan ketik atau input, dalam pengoperasian sistem informasi pertukaran Mata Uang maka kesalahan tersebut dicatat dan dilaporkan kepada *head administration* / kepala administrasi), sedangkan pengamatan / pengauditan secara keseluruhan dilakukan sebulan sekali dengan bantuan dari pengembang sistem

informasi pertukaran Mata Uang sebagai bagian dari perjanjian *maintanance* sistem informasi. Pengauditan sistem informasi ini tidak dilakukan oleh pihak ketiga yang *independent,* dan hasil laporan audit diserahkan kepada *head administration* untuk ditindak lanjuti, serta dilaporkan juga kepada kepala cabang. Selain mengaudit sistem informasi maka juga dilakukan pengauditan terhadap kinerja pengamanan aset-aset fisik lainnya.