



KEAMANAN Sistem Informasi



PENERBIT ANDI®



- Mengidentifikasi semua aset dan *resources* yang penting di organisasi
- Menentukan *vulnerability* atau kelemahan sistem, masalah dengan peralatan penunjang sistem, hingga kelemahan sekuriti
- *Assess risk*, berbagai pertimbangan dan langkah dalam prosedur manajemen risiko
- Menentukan tanggung jawab setiap departemen hingga person terkait
- Menyusun kebijakan sekuriti sistem informasi
- Implementasi kebijakan sekuriti sistem informasi dalam sebuah organisasi
- Audit sekuriti sistem informasi

/IBISA/

Daftar Isi

Kata Pengantar.....	vi
Daftar Isi	ix
1. Ancaman Terhadap Keamanan Sistem Informasi	1
1.1 Tujuan Keamanan Terhadap Sistem Informasi.....	1
1.2 Aset.....	2
1.3 Ancaman.....	3
1.4 Informasi.....	4
2. Kebijakan Keamanan Sistem Informasi	7
3. Mengapa Butuh Strategi Keamanan Sistem Informasi?	13
3.1 Keamanan Sistem Informasi.....	13
3.2 ISO 17799	14
3.3 Dampak dari Pemanfaatan Komputer.....	17
3.4 Kebutuhan atas Strategi Keamanan Sistem Informasi	20
4. Risk	21
4.1 Jenis Informasi.....	21
4.2 Risk.....	22
4.3 Analisis Risiko/ <i>Risk Analysis</i>	23
5. Tanggung Jawab Personel	27
5.1 Karyawan	28
5.2 Manajer	29
5.3 Tanggung Jawab Secara Spesifik yang Berkaitan dengan Keamanan Sistem Informasi.....	30
5.3.1 Pemilik Sistem	30
5.3.2 Pemakai.....	30
5.3.3 Pengembang sistem	32
5.3.4 Spesialis Database	33
5.3.5 Spesialis Jaringan Komunikasi	34
5.3.6 Spesialis PABX	35
5.3.7 Organisasi <i>Data Processing</i>	36
5.3.8 Auditor	36

5.3.9	Administrator Sistem Keamanan	37
5.3.10	Personel Administrasi	38
6.	<i>Logical Security dan Kontrol Password</i>.....	39
6.1	Tujuan	39
6.2	Aplikasi <i>Logical Security</i>	40
6.2.1	User-ID	40
6.2.2	Password	41
6.2.3	Level Pengaksesan (<i>Access Level</i>)	45
6.2.4	<i>Closed Menu</i>	46
6.3	Tanggung Jawab Pemberian Kontrol.....	46
7.	<i>Physical Security</i>.....	57
7.1	Tujuan	57
7.2	Sentra Komputer/ <i>Computer centre</i>	58
7.3	Kamar Komputer/ <i>Computer room</i>	58
7.4	Tanda Pengenal	60
7.5	Sistem Alarm.....	60
7.6	Prosedur dalam Keadaan Darurat	61
7.7	Peralatan	61
7.8	<i>Air Conditioning</i>	61
7.9	Tabung Pemadam Kebakaran.....	62
7.10	Alat Pendeteksi Api.....	62
7.11	Pintu Darurat	62
7.12	Laporan-laporan yang Tidak Dipakai Lagi.....	62
7.13	Aset Komputer.....	63
7.14	Media Backup	64
7.15	Kelemahan Keamanan.....	64
8.	Prosedur Perubahan Program	73
8.1	Tujuan	73
8.2	Prosedur	74
8.3	Prinsip Dasar Pengontrolan	76
9.	Pengembangan Sistem.....	79
9.1	Tanggung Jawab	79
9.1.1	<i>Steering Committee</i> /Tim Pengendali	80
9.1.2	<i>User Group</i> /Tim Pemakai	81

9.1.3	<i>Test Group/Tim Uji Coba</i>	82
9.2	Pengembangan Sistem	82-
9.2.1	Awal Proyek.....	83
9.2.2	Studi Kelayakan/ <i>Feasibility study</i>	84
9.2.3	<i>Functional Analysis</i> dan Desain	85
9.2.4	<i>Technical Analysis</i> dan Desain.....	85
9.2.5	Programming.....	86
9.2.6	Melatih Pemakai	86
9.2.7	Uji Coba Sistem	86
9.2.8	Persiapan Data dan <i>Parallel Run</i>	87
9.2.9	Pengalihan dan Akseptasi Sistem.....	87
9.3	Kebijakan Peraturan Akseptasi.....	88
9.4	Prinsip Pengalihan Sistem	88
9.5	Otorisasi Komponen Sistem	89
9.6	Daftar Pertanyaan pada Saat Penerimaan Sistem	90
9.7	Kontrol Setelah Pengalihan dan Akseptasi Sistem	95
9.8	<i>Outsourcing</i>	98
9.9	<i>Distributed System</i>	101
10.	Kontrol Terhadap PC	107
10.1	<i>Personal Computer</i>	107
10.2	Persoalan Kontrol	108
10.3	Peraturan Pengadaan Barang.....	109
10.3.1	Justifikasi/Pertimbangan yang Kuat	109
10.3.2	Standarisasi.....	111
10.3.3	Leveransir/Supplier	111
10.3.4	Pembelian Software	112
10.4	Persoalan Manajemen.....	113
10.4.1	Pengembangan Sistem.....	113
10.4.2	Integritas Sistem Aplikasi	114
10.5	Ancaman Terhadap PC	115
10.6	Peraturan Manajemen	118
10.7	PC vs Mainframe.....	120
10.7.1	<i>Physical Security</i>	121
10.7.2	<i>Software Security</i>	122
10.7.3	Persoalan Administrasi.....	124

11. Keamanan Jaringan, PC, dan LAN.....	127
11.1 Keamanan di dalam Jaringan.....	127
11.2 Ancaman.....	128
11.3 Langkah Pengamanan Jaringan	133
11.4 Internet.....	138
11.5 Keamanan PC dan LAN	139
11.6 <i>Disaster Recovery</i>	144
12. Ancaman dari Dalam.....	147
12.1 Kategori Pelaku.....	148
12.2 Mengapa Ancaman dari Dalam Lebih Parah daripada Ancaman dari Luar?.....	149
13. <i>Disaster Recovery Plan</i>.....	153
13.1 Pengumpulan Fakta	154
13.2 Penentuan Prioritas.....	154
13.3 Evaluasi Alternatif.....	155
13.4 Dokumentasi <i>Disaster Recovery Plan</i>	156
13.5 Uji Coba	158
13.6 <i>Maintain</i> dan <i>Review</i>	159
13.7 Asuransi	159
Kesimpulan.....	161
Singkatan.....	162
Lampiran	165
Daftar Pustaka	179