LAMPIRAN 1

Check List Audit Manajemen Keamanan Informasi

Ini adalah check list yang digunakan untuk melakukan audit kondisi pengelolaan Keamanan Sistem Informasi di Depkominfo saat ini. Check list ini mengacu pada ISO 17799:2005, bertujuan agar penulis dan pembaca mendapat gambaran kondisi keamanan sistem informasi di Depkominfo saat ini. Check list ini dibagi menjadi 6 kategori, yaitu: *Security Policy, Organization of Information Security, Asset Management, Human Resource Security, Communication and Operation Management,* dan *Business Continuity Management.*

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005

Petunjuk: Jawaban adalah **Y** (Ya) atau **T** (Tidak).

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
Security Policy									
1.1	5.1	***Information security policy***							
1.1.1	5.1.1	**Information security policy document**	Apakah ada kebijakan keamanan Informasi, yg disahkan oleh manajemen, dikeluarkan dan dikomunikasikan dengan semestinya kepada seluruh pegawai.	T	T	T	T	T	**T**
			Apakah kebijakan tersebut menyatakan tanggung-jawab manajemen dan mengemukakan pendekatan manajemen terhadap pengelolaan keamanan informasi.	T	T	T	T	T	**T**
1.1.2	5.1.2	**Review of Informational Security Policy**	Apakah Kebijakan Keamanan Informasi ditinjau pada interval-interval yang direncanakan, atau jika perubahan-perubahan yang signifikan terjadi untuk memastikan kesesuaian, kecukupan, dan keefektifan nya yang berkelanjutan.	T	Y	T	T	T	**T**
			Apakah ada pemilik kebijakan Keamanan Informasi, yang menyetujui tanggung-jawab manajemen untuk pengembangan, peninjauan, dan evaluasi kebijakan keamanan tersebut.	T	T	T	Y	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
			Apakah ada prosedur peninjauan untuk setiap Kebijakan Keamanan Informasi yang ditetapkan dan apakah prosedur tersebut berisi syarat-syarat untuk peninjauan manajemen.	T	T	T	T	T	**T**
			Apakah hasil-hasil dari peninjauan manajemen dimasukkan ke dalam laporan.	T	T	T	T	T	**T**
			Apakah persetujuan manajemen diperoleh untuk kebijakan yang ditinjau ulang.	T	T	T	T	T	**T**
Organization of information security									
2.1	6.1	***Internal Organization***							
2.1.1	6.1.1	**Management commitment to information security**	Apakah manajemen membuktikan dukungan yang aktif untuk pengukuran keamanan di dalam organisasi. Ini dapat dilakukan melalui arahan yang jelas, komitmen yang dibuktikan, penugasan yang jelas, pengakuan tanggung-jawab keamanan informasi.	T	Y	T	Y	T	**T**
2.1.2	6.1.2	**Information security coordination**	Apakah aktivitas-aktivitas keamanan informasi dikoordinasikan dengan perwakilan dari berbagai bagian dari organisasi, dengan tugas dan tanggung-jawab yang jelas.	T	T	T	T	T	**T**
2.1.3	6.1.3	**Allocation of**	Apakah tanggung-jawab untuk perlindungan	T	T	T	Y	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
		information security responsibilities	aset-aset individual, dan untuk melakukan proses-proses keamanan spesifik, telah diidentifkasi dan ditetapkan dengan jelas.						
2.1.4	6.1.4	**Authorization process for information processing facilities**	Apakah proses otorisasi manajemen ditetapkan dan diterapkan untuk setiap fasilitas pemrosesan informasi yang baru di dalam organisasi.	T	T	T	Y	T	**T**
2.1.5	6.1.5	**Confidentiality agreements**	Apakah kebutuhan organisasi untuk Kerahasiaan atau *Non-Disclosure Agreement (NDA)* untuk perlindungan informasi ditentukan dengan jelas dan ditinjau secara teratur.	T	T	T	Y	T	**T**
			Apakah kebutuhan ini menyebut syarat untuk melindungi informasi yang rahasia dengan menggunakan syarat-syarat yang menurut hukum dapat dilaksanakan.	T	T	T	T	T	**T**
2.1.6	6.1.6	**Contact with authorities**	Apakah ada prosedur yang menjelaskan kapan, dan oleh siapa: kewenangan yang relevan seperti Aparat hukum, jawatan pemadam kebakaran, dll., harus dihubungi, dan bagaimana insiden tersebut harus dilaporkan.	T	T	T	Y	T	**T**
2.1.7	6.1.7	**Contact with**	Apakah koneksi-koneksi yang sesuai dengan *interest groups* atau forum-forum ke ahli	Y	T	T	Y	Y	**Y**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
		special interest groups	keamanan lain, dan asosiasi profesional dipelihara.						
2.1.8	6.1.8	**Independent review of information security**	Apakah pendekatan organisasi kepada pengelolaan keamanan informasi, dan implementasinya, ditinjau secara independent pada interval-interval yang direncanakan, atau ketika perubahan-perubahan mayor pada implementasi keamanan terjadi.	T	T	T	Y	T	**T**
2.2	6.2	***External Parties***							
2.2.1	6.2.1	**Identification of risks related to external parties**	Apakah resiko-resiko pada informasi organisasi dan fasilitas pemrosesan informasi, dari proses yang melibatkan akses pihak luar, diidentifikasi dan ukuran kontrol yang sesuai diterapkan sebelum pemberian akses.	Y	Y	Y	Y	T	**Y**
2.2.2	6.2.2	**Addressing security when dealing with customers**	Apakah seluruh syarat-syarat keamanan yang teridentifikasi sudah dipenuhi sebelum pemberian akses pelanggan ke informasi atau aset-aset organisasi.	Y	T	Y	Y	T	**Y**
2.2.3	6.2.3	**Addressing Security in third party agreements**	Apakah persetujuan dengan pihak-pihak ketiga, melibatkan pengaksesan, pemrosesan, komunikasi atau pengelolaan informasi organisasi atau fasilitas pemrosesan informasi, atau pengenalan produk atau servis pada fasilitas pengelolaan informasi,	Y	T	T	Y	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
			memenuhi seluruh syarat keamanan yang sesuai.						
Asset Management									
3.1	7.1	***Responsibility for assets***							
3.1.1	7.1.1	**Inventory of assets**	Apakah seluruh aset diidentifikasi dan dalam inventaris atau pencatatan dipelihara dengan seluruh aset yang penting.	Y	T	Y	T	T	**T**
3.1.2	7.1.2	**Ownership of assets**	Apakah tiap aset yang diidentifikasi ada pemiliknya, klasifikasi keamanan yang ditentukan dan disepakati, dan pembatasan akses yang ditinjau secara periodik.	T	T	T	T	T	**T**
3.1.3	7.1.3	**Acceptable use of assets**	Apakah regulasi untuk penggunaan yang akseptabel dari informasi dan aset dihubungkan dengan fasilitas pemrosesan informasi telah diidentifikasi, didokumentasikan, dan diterapkan.	T	T	T	T	T	**T**
3.2	7.2	***Information classification***							
3.2.1	7.2.1	**Classification guidelines**	Apakah informasi diklasifikasikan dalam *term* nilai, syarat-syarat legal, sensitivitas, dan kekritisan nya pada organisasi.	T	T	T	T	T	**T**
3.2.2	7.2.2	**Information labelling and**	Apakah kumpulan prosedur yang sesuai telah ditentukan untuk pelabelan dan penanganan	T	T	T	T	Y	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
		handling	informasi, dalam penyesuaian dengan skema klasifikasi yang diadopsi oleh organisasi.						
Human resources security									
4.1	8.1	***Prior to employment***							
4.1.1	8.1.1	**Roles and responsibilities**	Apakah aturan dan tanggung-jawab keamanan pegawai, kontraktor, dan pengguna pihak ketiga telah ditentukan dan didokumentasikan sesuai dengan kebijakan keamanan informasi organisasi.	Y	T	T	Y	Y	**Y**
			Apakah aturan dan tanggung-jawab ditentukan dan dikomunikasikan dengan jelas kepada calon pegawai semasa proses perekrutan.	T	T	T	Y	T	**T**
4.1.2	8.1.2	**Screening**	Apakah uji verifikasi latar belakang untuk seluruh kandidat pegawai, kontraktor, dan pengguna pihak ketiga telah dilaksanakan sesuai dengan aturan yang relevan.	Y	T	T	T	T	**T**
			Apakah uji tersebut termasuk referensi karakter, konfirmasi dari kualifikasi akademi dan profesional yang diklaim, dan uji identitas independen.	Y	T	T	T	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
4.1.3	8.1.3	**Terms and conditions of employment**	Apakah pegawai, kontraktor, dan pengguna pihak ketiga diminta tandatangan perjanjian yang rahasia dan *non-disclosure* sebagai bagian dari syarat dan ketentuan awal dari kontrak pekerjaan.	Y	T	T	Y	Y	**Y**
			Apakah perjanjian ini melingkupi tanggung-jawab keamanan informasi dari organisasi dan pegawai, kontraktor, dan pengguna pihak ketiga.	Y	T	T	T	T	**T**
4.2	8.2	***During employment***							
4.2.1	8.2.1	**Management responsibilities**	Apakah manajemen membutuhkan pegawai, kontraktor, dan pengguna pihak ketiga untuk menerapkan keamanan sesuai dengan kebijakan dan prosedur yang dibuat organisasi.	T	T	T	Y	T	**T**
4.2.2	8.2.2	**Information security awareness, education and training**	Apakah seluruh pegawai di dalam organisasi, dan jika bersangkutan, kontraktor dan pengguna pihak ketiga, menerima pelatihan kesadaran keamanan yang sesuai dan *update* yang teratur dalam kebijakan dan prosedur organisasi sebagaimana berkenaan dengan fungsi kerja mereka.	T	T	T	T	T	**T**
4.2.3	8.2.3	**Disciplinary process**	Apakah ada proses disipliner resmi untuk pegawai yang melakukan pelanggaran keamanan.	Y	T	T	T	Y	**Y**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
4.3	8.3	***Termination or change of employment***							
4.3.1	8.3.1	**Termination responsibilities**	Apakah tanggung-jawab untuk pelaksanaan pemberhentian pekerjaan, atau penggantian pekerjaan, telah dijelaskan dan ditetapkan dengan jelas.	Y	T	T	Y	Y	**Y**
4.3.2	8.3.2	**Return of assets**	Apakah ada proses yang memastikan seluruh pegawai, kontraktor, dan pengguna pihak ketiga menyerahkan seluruh aset organisasi yang mereka miliki atas penghentian pekerjaan, kontrak, dan perjanjian mereka.	Y	T	T	Y	Y	**Y**
4.3.3	8.3.3	**Removal of access rights**	Apakah hak akses dari seluruh pegawai, kontraktor, dan pengguna pihak ketiga, pada informasi dan fasilitas pemrosesan informasi, akan dihapus atas penghentian pekerjaan, kontrak atau perjanjian, atau akan disesuaikan atas perubahan.	Y	T	T	Y	T	**Y**
Communications and Operations Management									
5.1	10.1	***Operational Procedures and responsibilities***							
5.1.1	10.1.1	**Documented Operating procedures**	Apakah prosedur pengoperasian didokumentasikan, dipelihara dan tersedia untuk seluruh pengguna ketika dibutuhkan.	Y	T	T	T	T	**T**
			Apakah prosedur seperti itu diperlakukan sebagai dokumen formal, dan oleh sebab itu	T	T	T	Y	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
			setiap perubahan yang dibuat memerlukan autorisasi manajemen.						
5.1.2	10.1.2	**Change management**	Apakah seluruh perubahan pada fasilitas pemrosesan informasi dan sistem dikontrol.	T	T	T	T	Y	**T**
5.1.3	10.1.3	**Segregation of duties**	Apakah tugas dan area tanggung-jawab dipisah, agar mengurangi kemungkinan modifikasi yang tidak terautorisasi atau penyalahgunaan dari informasi atau layanan.	T	T	T	Y	Y	**T**
5.1.4	10.1.4	**Separation of development, test and operational facilities**	Apakah fasilitas pengembangan dan percobaan diisolir dari fasilitas operasional. Sebagai contoh, perangkat lunak pengembangan dan produksi harus dijalankan di komputer yang berbeda. Jika perlu, jaringan pengembangan dan produksi harus dibuat terpisah satu sama lain.	T	T	T	Y	Y	**T**
5.2	10.2	***Third party service delivery management***							
5.2.1	10.2.1	**Service delivery**	Apakah langkah-langkah dilakukan untuk memastikan bahwa kontrol keamanan, definisi layanan, dan level *delivery*, termasuk dalam perjanjian *service delivery* pihak ketiga, diterapkan, dioperasikan, dan dipelihara oleh pihak ketiga.	Y	T	Y	T	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
5.2.2	10.2.2	**Monitoring and review of third party services**	Apakah layanan, laporan, dan catatan yang disediakan oleh pihak ketiga dimonitor dan ditinjau secara teratur.	Y	T	Y	T	Y	**Y**
			Apakah audit dilakukan pada layanan, laporan, dan catatan pihak ketiga, pada interval yang teratur.	T	T	T	T	T	**T**
5.2.3	10.2.3	**Managing changes to third party services**	Apakah perubahan ketetapan layanan, termasuk pemeliharaan dan peningkatan kebijakan, prosedur, dan kontrol keamanan informasi yang ada, dikelola.	T	T	T	T	T	**T**
			Apakah perubahan ini memperhitungkan sistem bisnis, proses yang terlibat, dan perkiraan ulang resiko secara kritis.	T	T	T	T	T	**T**
5.3	10.3	***System planning and acceptance***							
5.3.1	10.3.1	**Capacity Management**	Apakah kebutuhan kapasitas dimonitor dan proyeksi kebutuhan kapasitas ke depan dibuat, untuk memastikan daya dan penyimpanan pemrosesan yang memadai tersedia. Cth: Monitor *space* hard disk, RAM, dan CPU pada server-server yang kritikal.	T	T	T	Y	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
5.3.2	10.3.2	**System acceptance**	Apakah kriteria penerimaan sistem dibangun untuk sistem informasi baru, *upgrades*, dan versi-versi baru.	T	T	T	T	Y	**T**
			Apakah pengujian yang layak telah dilakukan sebelum penerimaan.	Y	T	T	Y	T	**T**
5.4	10.4	***Protection against malicious and mobile code***							
5.4.1	10.4.1	**Controls against malicious code**	Apakah deteksi, pencegahan, dan kontrol pemulihan, untuk melindungi terhadap *malicious code* dan menyediakan pengguna, telah dikembangkan dan diterapkan.	T	T	T	T	Y	**T**
5.4.2	10.4.2	**Controls against mobile code**	Apakah hanya *mobile code* yang terautorisasi yang digunakan.	T	T	T	T	T	**T**
			Apakah konfigurasi tersebut memastikan bahwa *mobile code* yang terautorisasi bekerja sesuai dengan kebijakan keamanan.	T	T	T	T	T	**T**
			Apakah eksekusi dari *mobile code* yang tidak terautorisasi dicegah.	T	T	T	T	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
			Ket: *Mobile code* adalah perangkat lunak yang memindahkan dari satu komputer ke komputer lain dan mengeksekusi secara otomatis. Dia melakukan fungsi yang spesifik dengan sedikit atau tidak ada intervensi pengguna. *Mobile code* diasosiasikan dengan sejumlah layanan *middleware*.						
5.5	10.5	***Backup***							
5.5.1	10.5.1	**Information backup**	Apakah backup dari informasi dan perangkat lunak diambil dan diuji secara teratur sesuai dengan kebijakan backup yang disepakati.	Y	T	T	T	T	**T**
			Apakah seluruh informasi dan yang perangkat lunak yang penting dapat dipulihkan sesudah bencana atau kerusakan media.	Y	T	T	Y	T	**T**
5.6	10.6	***Network Security Management***							
5.6.1	10.6.1	**Network Controls**	Apakah jaringan dikelola dan dikontrol dengan memadai, untuk melindungi dari ancaman, dan untuk menjaga keamanan untuk sistem dan aplikasi yang menggunakan jaringan tersebut, termasuk informasi yang melintas.	Y	T	T	Y	Y	**Y**
			Apakah kontrol diimplementasikan untuk memastikan keamanan dari informasi pada	Y	T	T	Y	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
			jaringan, dan proteksi layanan yang terhubung dari ancaman, seperti akses yang tidak terautorisasi.						
5.6.2	10.6.2	**Security of network services**	Apakah fitur-fitur keamanan, level-level layanan, dan syarat-syarat manajemen, dari seluruh layanan jaringan, diidentifikasi dan dimasukkan dalam setiap perjanjian layanan jaringan.	Y	T	T	Y	T	**T**
			Apakah kemampuan penyedia layanan jaringan, untuk mengelola layanan yang disepakati dengan cara yang aman, ditentukan dan dimonitor secara teratur, dan disepakati hak untuk mengauditnya.	Y	T	T	Y	T	**T**
5.7	10.7	***Media handling***							
5.7.1	10.7.1	**Management of removable media**	Apakah ada prosedur untuk pengeloaan *removable media,* seperti tape, disk, kaset, *memory cards,* dan laporan.	T	T	T	T	T	**T**
			Apakah seluruh prosedur dan level autorisasi ditentukan dan didokumentasikan dengan jelas.	T	T	T	T	T	**T**
5.7.2	10.7.2	**Disposal of Media**	Apakah media yang tidak dibutuhkan lagi dibuang dengan aman, sebagaimana prosedur formal.	T	T	T	T	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
5.7.3	10.7.3	**Information handling procedures**	Apakah ada prosedur untuk menangani penyimpanan informasi.	T	T	T	T	Y	**T**
			Apakah prosedur ini menujukan issu, seperti proteksi informasi, dari penyingkapan yang tidak terautorisasi atau penyalahgunaan.	T	T	T	T	T	**T**
5.7.4	10.7.4	**Security of system documentation**	Apakah dokumentasi sistem diproteksi terhadap akses yang tidak terautorisasi.	T	T	T	Y	Y	**T**
5.8	10.8	***Exchange of Information***							
5.8.1	10.8.1	**Information exchange policies and procedures**	Apakah ada kebijakan pertukaran formal, prosedur, dan kontrol pada tempatnya untuk memastikan proteksi pada informasi.	T	T	T	T	T	**T**
			Apakah prosedur dan kontrol tersebut melingkupi penggunaan fasilitas komunikasi eletronik untuk pertukaran informasi.	T	T	T	T	T	**T**
5.8.2	10.8.2	**Exchange agreements**	Apakah kesepakatan yang dibuat berkenaan dengan pertukaran informasi dan perangkat lunak antara organisasi dengan pihak luar.	T	T	T	Y	T	**T**
			Apakah muatan keamanan dari kesepakatan mencerminkan sensitifitas dari informasi bisnis yang terlibat.	T	T	T	Y	T	**T**
5.8.3	10.8.3	**Physical Media**	Apakah media yang berisi informasi	Y	T	T	Y	Y	**Y**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
		in transit	diproteksi terhadap akses yang tidak terautentikasi, penyalahgunaan atau perubahan selama transportasi melewati perbatas fisik organisasi.						
5.8.4	10.8.4	**Electronic Messaging**	Apakah informasi yang terlibat dalam *electronic messaging* diproteksi dengan baik. (*Electronic messaging* berisi tapi tidak dibatasi pada Email, Tukar menukar Data Elektronik, *Instant Messaging*).	Y	T	T	Y	Y	**Y**
5.8.5	10.8.5	**Business information systems**	Apakah kebijakan dan prosedur dikembangkan dan dilaksanakan untuk melindungi informasi yang berhubungan dengan interkoneksi sistem informasi bisnis.	T	T	T	Y	T	**T**
5.9	10.9	***Electronic Commerce Services***							
5.9.1	10.9.1	**Electronic Commerce**	Apakah informasi yang terlibat dalam *electronic commerce* yang melalui jaringan publik diproteksi dari aktivitas penipuan *(fraudulent)*, perselisihan kontrak, dan berbagai akses, atau modifikasi yang tidak terautorisasi.	Y	T	T	T	T	**T**
			Apakah kontrol keamanan seperti aplikasi kontrol kriptografi dipertimbangkan.	T	T	T	T	T	T
			Apakah pengaturan *electronic commerce* antara	T	T	T	T	T	T

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
			partner-partner *trading* berisi kesepakatan yang didokumentasikan, yang mengikat kedua pihak pada *terms of trading* yang disepakati, termasuk rincian dari issu-issu keamanan.						
5.9.2	10.9.2	**On-Line Transactions**	Apakah informasi yang terlibat dalam transaksi *online* diproteksi untuk mencegah transmisi yang tidak komplit, kesalahan *routing*, pengubahan pesan yang tidak terautorisasi, penyingkapan *(disclosure)* yang tidak terautorisasi, duplikasi atau *replay* pesan yang tidak terautorisasi.	Y	T	T	T	T	T
5.9.3	10.9.3	**Publicly available information**	Apakah integritas dari informasi yang tersedia di depan umum terproteksi terhadap berbagai modifikasi yang tidak terautorisasi.	Y	T	T	Y	Y	Y
5.10	10.10	***Monitoring***							
5.10.1	10.10.1	**Audit logging**	Apakah catatan (log) audit yang merekaman aktivitas pengguna, eksepsi, dan kejadian keamanan informasi dibuat dan disimpan selama periode yang disepakati untuk membantu investigasi ke depan dan pengawasan kontrol akses.	T	T	T	Y	T	**T**
			Apakah langkah-langkah proteksi pribadi yang tepat dipertimbangkan dalam pemeliharaan catatan log audit.	T	T	T	T	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
5.10.2	10.10.2	**Monitoring system use**	Apakah prosedur dikembangkan dan diterapkan untuk pengawasan penggunaan sistem untuk fasilitas pemrosesan informasi.	T	T	T	Y	Y	**T**
			Apakah hasil dari pengawasan aktivitas ditinjau secara teratur.	T	T	T	Y	T	**T**
			Apakah tingkat pengawasan dibutuhkan untuk fasilitas pemrosesan informasi tersendiri ditentukan dengan pengukuran resiko.	T	T	T	T	T	**T**
5.10.3	10.10.3	**Protection of log information**	Apakah fasilitas logging dan informasi log diproteksi dengan baik terhadap akses yang merusak dan tidak terautorisasi.	Y	T	T	Y	T	**T**
5.10.4	10.10.4	**Administrator and operator logs**	Apakah aktivitas-aktivitas administrator sistem dan operator sistem di-log.	Y	T	T	Y	T	**T**
			Apakah aktivitas-aktivitas yang di-log tersebut ditinjau secara teratur.	T	T	T	Y	T	**T**
5.10.5	10.10.5	**Fault logging**	Apakah kesalahan *(faults)* dianalisa pencatatannya dan diambil tindakan yang tepat.	T	T	T	T	T	**T**
			Apakah level *logging* yang dibutuhkan untuk sistem secara individual ditentukan dengan pengukuran resiko, mempertimbangkan penurunan performa.	T	T	T	T	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
5.10.6	10.10.6	**Clock synchronisation**	Apakah jam sistem dan seluruh sistem pemrosesan informasi di dalam organisasi atau domain keamanan disinkronisasi dengan sumber waktu yang akurat yang disepakati. (Pengaturan jam komputer yang benar penting untuk memastikan keakuratan log audit)	T	T	T	T	T	**T**
Business Continuity Management									
6.1.	14.1	***Information security aspects of business continuity management***							
6.1.1	14.1.1	**Including information security in the business continuity management process**	Apakah ada proses yang dikelola dengan benar yang menunjukkan syarat-syarat keamanan informasi untuk mengembangkan dan mengelola kelanjutan bisnis di seluruh organisasi.	T	T	T	T	T	**T**
			Apakah proses ini menangkap resiko-resiko yang dihadapi organisasi, identifikasi aset-aset bisnis yang kritikal, memperhitungkan implementasi dari kontrol-kontrol pencegahan tambahan, dan mendokumentasikan rencana kelanjutan bisnis yang menunjukkan syarat-syarat keamanan tersebut.	T	T	T	T	T	**T**
6.1.2	14.1.2	**Business continuity and**	Apakah kejadian-kejadian yang mengakibatkan terhentinya proses bisnis	T	T	T	T	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
		risk assessment	diidentifikasikan beserta dengan kemungkinan dan dampak gangguan-gangguan dan konsekuensinya dengan keamanan informasi.						
6.1.3	14.1.3	**Developing and implementing continuity plans including information security**	Apakah perencanaan-perencanaan telah dikembangkan untuk memelihara dan memulihkan operasi-operasi bisinis, memastikan ketersediaan informasi di dalam level yang dibutuhkan dalam kurun waktu yang dibutuhkan setelah gangguan atau kegagalan pada proses bisnis.	T	T	T	T	T	**T**
			Apakah perencanaan tersebut mempertimbangkan identifikasi dan perjanjian tanggung-jawab, identifikasi kehilangan yang bisa diterima, implementasi prosedur pemulihan dan restorasi, dokumentasi dari prosedur dan pengujian yang teratur.	T	T	T	T	T	**T**
6.1.4	14.1.4	**Business continuity planning framework**	Apakah ada kerangka kerja tunggal untuk rencana kelanjutan bisnis.	T	T	T	T	T	**T**
			Apakah kerangka kerja tersebut dipelihara untuk memastikan bahwa seluruh perencanaan adalah konsisten dan mengidentifikasikan prioritas untuk pengujian dan pemeliharaan.	T	T	T	T	T	**T**

Check List Audit Manajemen Keamanan Informasi ISO/IEC 17799:2005									
Referensi		**Area Audit, Objektif, dan Pertanyaan**		**Jawaban**					
Checklist	**Standard**	**Bagian**	**Pertanyaan Audit**	**Resp. 1**	**Resp. 2**	**Resp. 3**	**Resp. 4**	**Resp. 5**	**Rata-rata**
			Apakah rencana kelanjutan bisnis menunjukkan syarat-syarat keamanan informasi yang teridentifikasi.	T	T	T	T	T	**T**
6.1.5	14.1.5	**Testing, maintaining and re-assessing business continuity plans**	Apakah rencana-rencana kelanjutan bisnis telah diuji secara teratur untuk memastikan bahwa mereka *up to date* dan efektif.	T	T	T	T	T	**T**
			Apakah pengujian rencana kelanjutan bisnis memastikan bahwa seluruh anggota tim pemulihan dan staf lain yang relevan menyadari rencana-rencana tersebut dan tanggung-jawab mereka untuk kelanjutan bisnis dan keamanan informasi dan mengetahui peran mereka dan ketika perencanaan ditimbulkan.	T	T	T	T	T	**T**

LAMPIRAN 2

DOKUMEN MANAJEMEN KEAMANAN SISTEM INFORMASI

Berikut ini adalah dokumen Manajemen Keamanan Sistem Informasi yang berisi kebijakan-kebijakan yang terkait dengan permasalahan-permasalahan Keamanan Sistem Informasi yang dianalisa pada Bab 5.

[DRAFT] Kebijakan Keamanan Informasi

PERNYATAAN KEBIJAKAN KEAMANAN INFORMASI	Kebijakan No. 001	
Juli 2009	Versi 1.0	Revisi No.

OBJEKTIF

Objektif dari Keamanan Informasi adalah untuk memastikan kelangsungan bisnis Depkominfo dan meminimalkan resiko dari kerusakan dengan pencegahan insiden-insiden keamanan dan mengurangi dampaknya yang potensial.

CAKUPAN

Prosedur ini digunakan pada lingkungan Depkominfo

KEBIJAKAN

- Tujuan kebijakan tersebut adalah untuk melindungi aset-aset yang berhubungan dengan informasi dari Depkominfo terhadap seluruh ancaman internal, eksternal, disengaja atau tidak disengaja.
- Menteri Kominfo sebagai *Chief Executive Officer* harus menyetujui kebijakan keamanan informasi.
- Kebijakan Keamanan tersebut harus memastikan bahwa:
  - Informasi akan dilindungi terhadap segala akses yang tidak terautorisasi;
  - *Confidentiality* dari informasi akan dijamin;
  - *Integrity* dari informasi akan dipelihara;
  - *Availability* dari informasi untuk proses-proses bisnis akan dipelihara;
  - Syarat-syarat ***Legislative*** dan *regulatory* akan dipenuhi;
  - *Business continuity plans* akan dikembangkan, dipelihara, dan diuji;
  - Pelatihan Keamanan Informasi akan diberikan pada seluruh pegawai;
  - Seluruh pelanggaran keamanan informasi yang aktual maupun yang dicurigai akan dilaporkan kepada **Kepala Subbidang Pengamanan (Pusteka) dan Kepala Subbidang Pengamanan Data (Pusdat)** dan akan diinvestigasi dengan tuntas.
- Ada prosedur-prosedur untuk mendukung kebijakan, termasuk langkah-langkah pengendalian virus, password, dan *continuity plans.*
- Kebutuhan-kebutuhan bisnis akan ketersediaan informasi dan sistem akan dipenuhi.
- **Kepala Subbidang Pengamanan dan Kepala Subbidang Pengamanan Data** bertanggung-jawab untuk pemeliharaan kebijakan tersebut dan penyediaan dukungan dan advokasi selama implementasinya.
- Seluruh pimpinan bertanggung-jawab secara langsung untuk implementasi kebijakan tersebut dan memastikan **penyesuaian staf dalam bagian-bagian yang berhubungan.**

Tandatangan _____ Tanggal _____

Jabatan _____

Kebijakan ini akan ditinjau tiap tahun oleh Kepala Subbidang Pengamanan dan Kepala Subbidang Pengamanan Data

[DRAFT] Kebijakan Keamanan Informasi

ELEMEN-ELEMEN KEBIJAKAN KEAMANAN	Kebijakan No. 002	
Juli 2009	Versi 1.0	Revisi No.

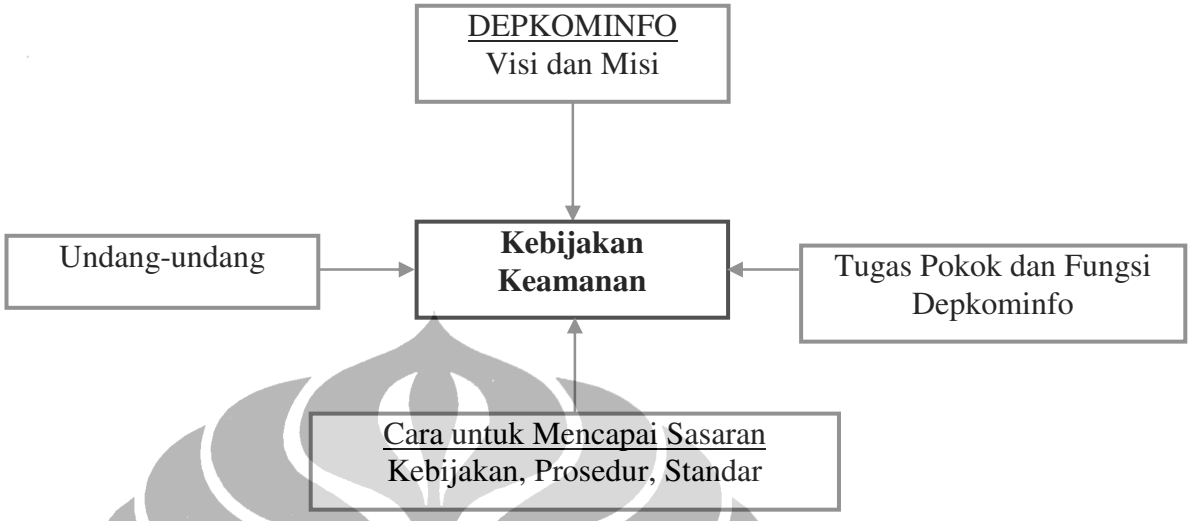

Diagram ini menggambarkan kebijakan keamanan sebagai sebuah dokumen yang menerangkan visi, misi, dan nilai-nilai dari Depkominfo. Kebijakan Keamanan tersebut merefreksikan nilai-nilai dari organisasi. Sesuai dengan itu, sejumlah model mungkin menarik untuk digunakan tergantung pada garis bisnis dan objektif organisasi. Selain itu, pembatasan yang menurut hukum tertentu harus dipertimbangkan ketika mengembangkan kebijakan-kebijakan keamanan, seperti ketentuan-ketentuan dari aturan proteksi data, aturan akses informasi, aturan pada proteksi informasi personal dan dokumen-dokumen elektronik, dan lain-lain. Penentuan tugas dan tanggung-jawab dari anggota staf menunjukkan satu dari aspek-aspek yang paling penting dalam tercapainya seluruh pegawai bekerja menuju tujuan bersama.

PANDUAN KEBIJAKAN KEAMANAN INFORMASI	Kebijakan No. 003	
Juli 2009	Versi 1.0	Revisi No.

1. PENDAHULUAN

SASARAN DARI KEBIJAKAN KEAMANAN

Depkominfo bergantung pada informasi dan sistem informasi. Sasaran dari kebijakan keamanan adalah menetapkan sasaran-sasaran untuk organisasi sehubungan dengan proteksi dari aset-aset informasinya. Kebijakan keamanan menyediakan dasar untuk implementasi kontrol-kontrol keamanan yang mengurangi resiko-resiko dan vulnerabilitas sistem. Dengan penjelasan tanggung-jawab dari pengguna dan langkah-langkah yang harus mereka ambil untuk melindungi informasi dan sistem. Depkominfo menghindari kehilangan yang serius atau *disclosure* yang tidak terautorisasi. Selain itu, nama baik organisasi sebagian bergantung pada cara bagaimana memproteksi informasi dan sistem informasi nya. Akhirnya, kebijakan keamanan dapat berguna sebagai bukti dalam proses pengadilan, dalam negosiasi kontrak klien, selama proses penawaran akuisisi, dan untuk relasi-relasi bisnis secara umum. Manajemen Depkominfo telah dimulai dan berlanjut untuk menyangga upaya keamanan informasi berkat pengembangan dalam kebijakan-kebijakan dan prosedur-prosedur.

KERANGKA KERJA MANAJEMEN KEAMANAN

Seluruh kebijakan dan prosedur yang dimasukkan dalam dokumen ini disetujui, didukung, dan dipertahankan oleh manajemen senior dari Depkominfo. Sebagai respek pada kebijakan keamanan adalah seluruh kepentingan pada organisasi, informasinya dan informasi yang dipercayakan kepadanya harus diproteksi sesuai dengan nilai kritikal dan *sensitive nature* dari informasi ini. Langkah-langkah keamanan harus diambil, tanpa memperhatikan media penyimpanan dimana informasi disimpan, sistem yang digunakan untuk pemrosesan informasi, atau metoda-metoda yang digunakan untuk transfer informasi. Informasi harus diproteksi sesuai dengan klasifikasi keamanannya, tanpa memperhatikan fase dari daur hidup informasi dimana dia ditemukan.

CAKUPAN

Para Pegawai

Keamanan informasi adalah sebuah upaya tim. Itu membutuhkan partisipasi dan dukungan dari seluruh anggota organisasi yang bekerja dengan sistem informasi. Jadi, tiap pegawai harus mengikuti syarat-syarat dari kebijakan keamanan informasi dan dokumentasi yang mengikut. Para pegawai yang secara sengaja atau karena lalai melanggar kebijakan keamanan informasi akan dikenakan tindakan disipliner atau pemecatan.

Sistem-sistem

Kebijakan ini berlaku pada seluruh komputer, jaringan, aplikasi, dan sistem operasi yang dimiliki atau dioperasikan oleh Depkominfo. Kebijakan ini mencakup hanya informasi yang ditangani oleh komputer dan jaringan.

PANDUAN KEBIJAKAN KEAMANAN INFORMASI	Kebijakan No. 003	
Juli 2009	Versi 1.0	Revisi No.

ATURAN-ATURAN DAN TANGGUNG-JAWAB

Bagian-bagian yang Mengelola Keamanan Informasi

- Bagian yang menangani Keamanan Informasi bertanggung-jawab untuk membangun dan memelihara kebijakan keamanan informasi, standard, petunjuk, dan prosedur organisasi.
- Bagian yang menangani Audit Internal harus memastikan penyesuaian teknologi informasi dengan kebijakan-kebijakan, prosedur-prosedur, dan setiap perundang-undangan yang dapat dipakai.
- Investigasi sistem *hacking* dan insiden-insiden keamanan informasi lainnya adalah tanggung-jawab dari bagian yang menangani Keamanan Fisik.
- Aksi disipliner dalam respon terhadap pelanggaran regulasi-regulasi keamanan informasi adalah tanggung-jawab pelaksana pimpinan lokal yang bersama-sama dengan Bagian Kepegawaian.

Kategori-kategori Tanggung-jawab

Sesuai dengan koordinasi upaya-upaya keamanan, Depkominfo membagi tanggung-jawab dari anggotanya ke dalam tiga kategori.

1. Tanggung-jawab Pengguna

Para pengguna wajib bersungguh-sungguh membiasakan diri mereka dengan seluruh informasi kebijakan-kebijakan, prosedur-prosedur, standar-standar keamanan, dan perundang-undangan yang dapat dipakai.

2. Tanggung-jawab Pemilik

- Para pemilik aset-aset informasi secara umum adalah para eksekutif, para pimpinan, atau para perwakilan dari Depkominfo yang harus memperoleh, mengembangkan, dan memelihara aplikasi-aplikasi operasional (*decision support systems*) yang mendukung pembuatan keputusan dan aktivitas-aktivitas organisasi lainnya.
- Tiap aplikasi operasional harus memiliki seorang pemilik yang ditunjuk.
- Para pemilik mengindikasi klasifikasi tersebut yang terbaik menggambarkan *sensitive nature,* nilai kritikal dan *availability* dari tiap jenis informasi. Klasifikasi tersebut akan, bergantian, menentukan level akses pengguna.

3. Tanggung-jawab Administrator Informasi

- Para administrator adalah staf yang ditugaskan dengan penyimpanan informasi organisasi atau informasi yang dipercayakan pada organisasi.
- Personil bagian Teknologi Informasi, para administrator sistem, dan para pengguna yang menangani informasi pada komputer mereka masing-masing seluruhnya memegang jabatan sebagai administrator.
- Tiap jenis sistem informasi operasional harus memiliki setidaknya satu administrator yang terautorisasi. Para administrator bertanggung-jawab

untuk penyimpanan informasi, penerapan sistem kontrol akses (untuk mencegah penyingkapan yang tidak terautorisasi) dan secara berkala menjalakan *backup* (untuk memastikan informasi yang kritikal tidak hilang).

- Para administrator juga diharuskan untuk mengembangkan, menerapkan, dan merevisi langkah-langkah keamanan yang ditentukan oleh para pemilik informasi.

2. DEFINISI DAN SINGKATAN

IT : Information technology
PC : Personal Computer

Malicious software: Program atau bagian dari program yang ditujukan untuk mengacaukan, mengubah, atau menghancurkan seluruh atau sebagian dari logic dari elemen-elemen penting pada operasi dari sistem pemrosesan informasi. Program-program ini dapat dibagi dalam 4 kelas: virus komputer, worm, trojan horse, dan logic bom.

3. SENSITIVITAS DAN KLASIFIKASI INFORMASI

EMPAT KLASIFIKASI INFORMASI

- Klasifikasi informasi merupakan elemen penting dari manajemen resiko, sebagaimana itu menentukan kebutuhan, prioritas, dan tingkat proteksi yang diwajibkan untuk tiap tipe informasi.
- Depkominfo mengadopsi struktur klasifikasi informasi yang melihat informasi tersusun berdasarkan kategori. Struktur ini mendefinisikan level yang sesuai dari proteksi untuk kategori yang diberikan dan menginformasikan orang yang bertanggung-jawab dari tiap langkah-langkah khusus atau perlakuan yang diharuskan.
- Seluruh informasi harus terintegrasi ke dalam satu dari empat kategori berikut:
  - Confidential
  - Private
  - Internal use only
  - Public
- Untuk memastikan proteksi informasi, seluruh pengguna harus membiasakan diri mereka dengan definisi-definisi dari tiap kategori sebagaimana langkah-langkah yag diharuskan.

PELABELAN INFORMASI

- Depkominfo mengembangkan prosedur-prosedur yang sesuai untuk pelabelan dan penanganan informasi sesuai dengan struktur klasifikasi yang telah dipakai.
- Informasi sensitif, dari permulaan hingga penghancuran, harus mengandung penandaan klasifikasi informasi yang sesuai.
- Label-label identifikasi harus mengandung klasifikasi tersebut, tanggal kadaluarsa klasifikasi, instruksi penggunaan dan penanganan, dan lokasi, jika diperlukan.
- Label-label harus terlihat pada *footers* dari dokumen-dokumen organisasi.
- Karena kebanyakan dokumen masuk ke dalam kategori "Internal use only", tidak perlu meletakkan label pada jenis informasi ini karena akan diklasifikasikan sebagai *default*.

4. KEAMANAN ORGANISASI

PENYINGKAPAN *(DISCLOSURE)* KE PIHAK KETIGA

- Informasi yang berlabel selain dari pada "Public" harus diproteksi dari penyingkapan ke pihak ketiga.
- Akses pihak ketiga ke informasi milik organisasi bisa diijinkan jika dia telah menunjukkan bahwa informasi ini diperlukan untuk memperbolehkan pihak ketiga memperoleh hak yang telah diberkan organisasi. Bagaimanapun, perjanjian *non-disclosure* dengan Depkominfo harus ditandatangi sebelumnya dan penyingkapan harus diautorisasi dengan jelas oleh pemilik informasi.
- Segala kehilangan atau penyingkapan yang tidak terautorisasi atau yang dicurigai dari informasi yang sensitive harus dilaporkan segera ke pemilik informasi dan bagian Keamanan Informasi.

PERMINTAAN PIHAK KETIGA UNTUK INFORMASI

- Jika pegawai tidak terautorisasi oleh pemilik informasi untuk menyingkap informasi secara umum, seluruh permintaan untuk informasi berkenaan dengan Depkominfo harus dilaporkan ke bagian Hubungan Masyarakat.
- Permintaan untuk kuisiner-kuisioner, laporan-laporan keuangan, dokumen-dokumen kebijakan internal, prosedur-prosedur, survei-survei, dan wawancara-wawancara dengan personil dilindungi oleh kebijakan ini.
- Kebijakan ini tidak berlaku untuk informasi mengenai produk-produk dan layanan-layanan Depkominfo. Pihak ketiga yang ingin mengirim informasi yang sensitive ke salah satu pegawai yang bertindak sebagai bagian Depkominfo harus sebelumnya menandatangani surat pernyataan melepaskan tuntutan Depkominfo dari segala tanggung-jawab.

PENGGANDAAN INFORMASI YANG TIDAK TERAUTORISASI

- Para pengguna dilarang menggandakan, tanpa justifikasi dan autorisasi yang sah, informasi dan perangkat lunak milik organisasi.
- Orang-orang yang bertanggung-jawab untuk *forwarding* yang tidak terautorisasi dari informasi yang digandakan ke pihak ketiga akan dikenai tindakan disipliner.
- Pembuatan *backup* salinan, bagaimanapun, diautorisasi.

PENYINGKAPAN PIHAK LUAR DARI INFORMASI KEAMANAN

Informasi terkait langkah-langkah keamanan untuk sistem pemrosesan informasi dan jaringan adalah rahasia dan harus tidak disingkapkan ke pengguna yang tidak terautorisasi, jika sebelumnya tidak diijinkan oleh pimpinan keamanan informasi. Sebagai contoh, dilarang keras untuk memberitahukan telepon rumah pegawai kepada kompetitor.

5. ADMINISTRATIVE SECURITY CONTROLS

PENGGUNAAN SUMBER DAYA TEKNOLOGI DARI ORGANISASI

- Seluruh pegawai yang ingin menggunakan sistem pemrosesan informasi Depkominfo harus menandatangani pernyataan ketaatan. Dalam menandatangi pernyataan ini, para pengguna menunjukkan bahwa mereka mengerti dan menerima untuk taat pada kebijakan-kebijakan dan prosedur-prosedur dari Depkominfo ketika mereka berhubungan dengan penggunaan komputer dan jaringan, termasuk instruksi-instruksi yang termuat dalam kebijakan terbaru.
- Sistem informasi Depkominfo digunakan semata-mata untuk urusan pekerjaan.
- Kadang penggunaan pribadi diijinkan, jika sebentar dan tanpa mengganggu produktifitas.
- Dilarang memainkan games selama jam kerja, karena ini berdampak negatif pada produktifitas dan, sebagai hasil, keuntungan. Setiap orang yang diketahui memainkan games akan menghadapi tindakan disipliner.
- Bentuk hiburan ini diperbolehkan sepanjang jam makan dan istirahat pegawai. Penggunaan sistem informasi organisasi untuk mengirim surat berantai atau penghasutan, atau mentransmisi atau mengunduh materi yang tidak menyenangkan adalah dilarang.

WEWENANG PENGAWASAN

- Manajemen menyimpan wewenang untuk memonitor dan menginspeksi setiap waktu sistem informasi milik organisasi.
- Inspeksi ini dapat mengambil tempat dengan atau tanpa persetujuan dan kehadiran pegawai yang terlibat.

- Sistem informasi mungkin dikenakan kepada inspeksi demikian termasuk log aktifitas para pengguna, file-file pada *hard drive* dan email. Bagaimanapun, dokumen-dokumen tercetak, laci-laci meja, dan area-area penyimpanan juga dikenakan inspeksi.
- Inspeksi harus dilakukan hanya setelah diperoleh persetujuan dari bagian legal dan keamanan.
- Manajemen menyimpan wewenang untuk menyita materi yang ofensif atau informasi ilegal.

KEPEMILIKAN EKSKLUSIF DARI MATERIAL YANG DIKEMBANGKAN

- Depkominfo memiliki hak-hak eksklusif terhadap paten, hak cipta, penemuan atau apapun properti intelektual lain yang dikembangkan oleh pegawai-pegawainya.
- Seluruh program dan dokumen yang diproduksi dan dipersiapkan oleh pegawai untuk keuntungan Depkominfo adalah properti dari Depkominfo.

AKSES INTERNET

- Seluruh pegawai Depkominfo memiliki akses Internet pada *workstation* masing-masing. Akses ini dapat dicabut kapan saja, bagaimanapun, atas kebijaksanaan manajemen.
- Akses Internet dimonitor untuk memastikan penggunaan yang wajar dan memenuhi kebijakan-kebijakan keamanan.
- Dilarang untuk mewakili organisasi pada *newsgroups* atau dalam forum publik lainnya jika sebelumnya tidak diautorisasi oleh manajemen.
- Segala informasi yang diterima melalui Internet harus diperhatikan dengan was-was hingga dikonfirmasi sebaliknya oleh sumber-sumber yang dipercaya.
- Dilarang meletakkan material organisasi pada sistem pemrosesan informasi yang dapat diakses publik jika tidak diautorisasi oleh pemilik aset dan bagian keamanan informasi.
- Informasi sensitif seperti password dan nomor kartu kredit seharusnya tidak dikirim melalui Internet jika tidak dienkripsi.

SURAT ELEKTRONIK *(ELECTRONIC MAIL)*

- Depkominfo menyediakan alamat email untuk seluruh pegawai dan layanan email untuk memfasilitasi performa kerja mereka.
- Seluruh komunikasi bisnis harus dikirim dan diterima menggunakan alamat email ini.
- Akun email pribadi (Yahoo, Gmail, Hotmail, dsb) tidak dapat digunakan untuk bisnis organisasi.
- Seluruh personil harus menggunakan sebuah *signature* yang standar yang memuat nama awal dan akhir, posisi, alamat bisnis, dan nomor telepon.

- Pesan-pesan yang penting seharusnya tidak disimpan di dalam Inbox email.

BACKUP DAN PEMULIHAN DATA

- Informasi pada sistem individu seharusnya di-backup secara teratur pada *compact disc* atau media penyimpanan lainnya.
- Untuk multi-pengguna dan sistem komunikasi, administrator sistem bertanggung-jawab untuk melakukan backup berkala.
- Jika diperlukan, bagian Teknologi Informasi harus menyediakan bantuan teknis untuk instalasi dari perangkat keras atau lunak backup.
- Seluruh salinan backup dari informasi yang kritikal atau sensitif harus disimpan dalam suatu area yang disetujui dengan akses yang dikontrol.
- Salinan-salinan ini harus dijaga semata-mata untuk tujuan pemulihan sistem setelah infeksi virus komputer, kerusakan *hard drive*, atau masalah-masalah komputer lainnya.
- Perencanaan keadaan darurat harus dikembangkan untuk seluruh aplikasi yang menangani informasi operasional yang kritikal. Pemilik informasi harus memastikan bahwa perencanaan tersebut dikembangkan dengan cukup, sering diperbaharui, dan ditinjau secara periodik.

MANAJEMEN PERUBAHAN

- Komputer-komputer organisasi dan sistem-sitem komunikasi untuk aktivitas-aktivitas operasional harus didukung oleh proses manajemen perubahan yang terdokumentasi yang memastikan hanya perubahan-perubahan yang terautorisasi yang dilakukan.
- Prosedur manajemen perubahan diterapkan sewaktu-waktu perubahan penting dibuat untuk sistem operasi, perangkat, *links*, atau prosedur-prosedur.
- Kebijakan ini berlaku pada PC-PC yang menjalankan sistem operasi dan pada sistem multi-pengguna yang lebih besar.

STANDAR PENGEMBANGAN SISTEM

- Pengembangan perangkat lunak operasional atau perawatan oleh staf internal harus mengikuti kebijakan dari bagian Teknologi Informasi dan standar, prosedur, dan ketentuan-ketentuan pengembangan sistem.
- Ketentuan-ketentuan ini termasuk pengujian, pelatihan, dan dokumentasi.

MANAJEMEN LISENSI-LISENSI

- Manajemen harus merundingkan persetujuan-persetujuan yang sesuai dengan penyedia perangkat lunak dengan memperhatikan kebutuhan untuk lisensi tambahan.
- Layanan persediaan akan membeli seluruh perangkat lunak yang diperlukan.

6. KONTROL-KONTROL KEAMANAN TEKNIS

IDENTIFIKASI DAN AUTENTIKASI PENGGUNA

User ID dan Password

- Depkominfo mengharuskan seluruh pegawai yang mengakses sistem informasi nya untuk memiliki User ID tunggal dan password yang tersendiri.
- User ID harus digunakan untuk membatasi hak khusus akses sistem sesuai dengan fungsi, tanggung-jawab, dan aktivitas tiap pengguna.
- Seluruh pegawai bertanggung-jawab untuk perlindungan user ID dan password mereka.

Pemilihan Password

Para pengguna sistem informasi harus memilih password yang susah ditebak dan yang tidak berisi informasi yang berhubungan dengan pekerjaan dan kehidupan pribadi mereka. Sebagai contoh, nomor identitas pribadi (tanggal lahir, PIN, Surat Ijin Mengemudi, nomor asuransi kesehatan), nomor telepon, nama suami/istri, alamat surat, sesuai dengan nama, tempat-tempat yang diketahui umum, atau istilah-istilah teknis seharusnya tidak digunakan.

Berikut adalah beberapa tips untuk membuat password:

- Kombinasi beberapa kata bersamaan.
- Kombinasi tanda baca atau nomor dengan sebuah kata (huruf besar atau kecil)
- Mengubah sebuah kata yang umum dengan metode yang spesifik
- Membuat singkatan (inisial yang membentuk kata)
- Dengan sengaja salah mengeja sebuah kata.
- Deliberately misspell a word.

Kesamaan Password

Para pengguna seharusnya tidak berulang-kali membuat password yang identik atau pada dasarnya sama dengan password sebelumnya.

Pembatasan Password

- Password harus memuat setidaknya 8 digit, dan diganti pada interval 90 hari atau kurang.
- Sistem manajemen password mewajibkan para pengguna untuk mengkombinasikan huruf dengan nomor dan tidak memperbolehkan penggunaan ulang sebuah password dalam rentang waktu tertentu.

Penyimpanan Password

- Password seharusnya tidak disimpan dalam bentuk yang bisa dibaca dalam *sequential files*, perangkat lunak *macros*, komputer tanpa sistem akses

kontrol atau tempat apapun dimana orang yang tidak terautorisasi dapat menemukannya.

- Password seharusnya tidak ditulis dan diletakkan di tempat yang mudah dilihat, seperti monitor komputer atau meja kerja.

Password Sharing

- Ketika informasi perlu dibagikan, para pegawai harus melakukannya dengan menggunakan email, database, direktori publik yang terletak pada server jaringan lokal, disket, dan media pertukaran lainnya.
- Password seharusnya tidak pernah dibagi atau disingkapkan.
- Para administrator sistem dan staf teknis seharusnya tidak pernah meminta para pegawai untuk memberitahukan password pribadi mereka. Satu-satunya pengecualian adalah dalam kasus password sementara yang akan diganti ketika pengguna mengakses sistem untuk pertama kalinya.
- Jika para pengguna mencurigai seseorang menggunakan user ID dan password mereka, adalah merupakan tanggung-jawab mereka untuk segera mengadvokasi administrator sistem.

MALICIOUS SOFTWARE

Perangkat Lunak Pendeteksi Virus

- Para pengguna sistem seharusnya tidak membatalkan proses memperbarui *virus definition* otomatis.
- Seluruh file sitem seharusnya discan oleh perangkat lunak pendeteksi virus.
- Scan harus dijalankan sebelum pembukaan file-file data baru dan sebelum eksekusi perangkat lunak baru.

Pembersihan Virus-virus

- Pada sinyal pertama dari kemungkinan virus komputer, para pegawai harus segera berhenti menggunakan sistem yang terkena dan memanggil *technical support.*
- Seluruh disket dan media penyimpanan magnetik lainnya yang digunakan di komputer yang terinfeksi seharusnya tidak digunakan pada komputer lain manapun hingga virus telah berhasil dihapuskan.
- Komputer yang terinfeksi harus dikarantina (diisolir dari jaringan internal).
- Para pengguna diharuskan tidak mencoba menghapus sendiri virus-virus tersebut.
- Staf-staf yang berkualifikasi atau konsultan akan menghapus virus-virus tersebut dan memastikan kerusakan data yang minimal, dan *downtime* yang minimal.

PANDUAN KEBIJAKAN KEAMANAN INFORMASI	Kebijakan No. 003	
Juli 2009	Versi 1.0	Revisi No.

KEAMANAN JARINGAN

Koneksi Jaringan Internal

- Seluruh komputer yang menyimpan informasi yang sensitif dan secara permanen atau sebentar terhubung ke jaringan komputer internal organisasi harus memiliki sistem kontrol akses yang disetujui oleh bagian Keamanan Informasi.
- Seluruh jenis sistem pemrosesan informasi harus diperlengkapi dengan password screensaver yang mengunci setelah periode tertentu tidak ada aktivitas. Layar tersebut akan diaktivasi ulang ketika password yang benar dimasukkan.
- Sistem multi-pengguna harus menggunakan mekanisme penutupan *session* yang secara otomatis menutup *session* pengguna setelah periode tertentu tidak ada aktivitas.

Koneksi Jaringan Eksternal

- Seluruh koneksi eksternal ke sistem informasi dari Depkominfo harus diproteksi dengan sistem kontrol akses password dinamis yang disetujui. Password dinamis berubah dengan tiap pengguna, mengubah pencurian mereka yang tidak berguna.
- Para pegawai seharusnya tidak membangun koneksi dengan jaringan eksternal (Penyedia Jasa Internet) menggunakan sistem milik organisasi tanpa sebelumnya persetujuan dari bagian Keamanan Informasi.

Perubahan Jaringan

- Kecuali dalam situasi darurat, seluruh perubahan pada jaringan komputer dari Depkominfo harus dicatat dalam *maintenance request* dan disetujui oleh bagian Teknologi Informasi.
- Seluruh perubahan pada jaringan internal harus dilakukan oleh personil yang diautorisasi oleh bagian Teknologi Informasi.
- Proses ini mengurangi resiko penyingkapan yang tidak terautorisasi dan perubahan yang dibuat dengan kurang hati-hati selama gangguan tanpa pengetahuan dari bagian Teknologi Informasi.
- Proses-proses ini berlaku tidak hanya pada para pegawai Depkominfo, tapi juga para penyedia jasa.

Teleworking

- Pegawai tertentu diautorisasi, berasarkan kebijakan manajemen, untuk bekerja dari rumah.
- Pengawasan yang segera dari para pegawai yang ingin untuk *telework* harus memperoleh *permission* berdasarkan *checklist* yang sesuai.
- *Permission* untuk melanjutkan *teleworking* bergantung sebagian pada penyesuaian dengan sejumlah tertentu dari kebijakan dan standar keamanan informasi.

- Pemeriksaan berkala dari email oleh para pegawai di perjalanan tidak dianggap sebagai *teleworking*, tetapi memerlukan respes yang sama dengan regulasi-regulasi keamanan.

7. PENYESUAIAN

Depkominfo secara berkala melakukan audit keamanan untuk memastikan kesesuaian dengan kebijakan, prosedur, dan perundangan-undangan yang dapat dipakai.

PENYESUAIAN DENGAN KEBIJAKAN DAN PROSEDUR
Seluruh pegawai harus patuh dengan kebijakan keamanan informasi dan dokumen-dokumen yang berhubungan. Pegawai yang, dengan lalai atau sengaja, melanggar kebijakan keamanan akan dikenakan tindakan disipliner atau pemecatan.

PENYESUAIAN DENGAN PERUNDANG-UNDANGAN DAN REGULASI
Seluruh kebijakan keamanan informasi harus tunduk pada perundang-undangan yang dapat dipakai, seperti aturan mengenai proteksi data, akses pada informasi, proteksi informasi pribadi dan dokumen-dokumen elektronik, dsb.

8. LANGKAH-LANGKAH DISIPLINER

- Tersangka pelanggaran-pelanggaran keamanan informasi (hacking sistem, infeksi virus) yang dapat membahayakan integritas dari sistem informasi harus segera dilaporkan ke bagian Keamanan Informasi atau ke tim Manajemen Darurat.
- Pelanggaran atau kerusakan yang terbukti sesuai dengan kebijakan keamanan informasi memerlukan kelanjutan yang serius untuk para pelanggar. Langkah-langkah disipliner berbeda sesuai dengan tingkat pelanggaran, dan dapat berakibat pada pemecatan.

[DRAFT] Kebijakan Keamanan Informasi

PERAN DAN TANGGUNG-JAWAB TERKAIT DENGAN ASET	Kebijakan No. 004	
Juli 2009	Versi 1.0	Revisi No.

DEFINISI PERAN DAN TANGGUNG-JAWAB TERKAIT DENGAN ASET

RINGKASAN PERAN DAN TANGGUNG-JAWAB	
Peran	**Tanggung-jawab**
Pemilik Biasanya eksekutif atau kepala dari bagian-bagian, pemilik bertanggung-jawab untuk manajemen dan proteksi informasi. Mereka dapat membuat semua keputusan penting mengenai informasi yang mereka control supaya menjaga integritas dan kerahasiaannya. **Para Pemilik biasanya pegawai tetap bagian dari organisasi.**	• Memahami resiko-resiko utama yang terkait dengan seluruh penggunaan internal dari jenis tertentu dari informasi. • Menentukan sensitivitas dan tingkat kritikal dari informasi tersebut, dan menentukan klasifikasi yang sesuai. • Menentukan metode kontrol tambahan yang diperlukan untuk proteksi informasi tersebut. • Menyetujui permintaan pengguna untuk mengakses informasi tersebut. • Meninjau daftar kontrol akses pengguna untuk menentukan apakah hak akses harus dicabut.
Administrator Administrator asset biasanya adalah anggota dari bagian Keamanan Informasi dan mungkin memegang posisi lain sebagai administrator system atau operator kontrol data. Mereka memegang informasi tersebut, mengelola system pemrosesan informasi, dan mengawasi akses pada informasi. **Administrator lebih baik adalah pegawai tetap.**	• Menyimpan dan secara fisik menjaga informasi tersebut. • Mengikuti instruksi pemilik untuk pemrosesan dan penanganan informasi tersebut. • Secara teratur memberika kepada pemilik daftar orang-orang yang telah mengakses informasi tersebut. • Menyarankan teknologi dan prosedur baru kepada pemilik. • Memelihara kehandalan dari perangkat akses informasi. • Menerapkan perintah yang ditetapkan pemilik. • Memasang mekanisme keamanan. • Membuat *backup* secara teratur dan pemulihan data dari salinan *backup* ketika diperlukan.
Pengguna Pengguna adalah anggota pegawai Depkominfo atau pihak ketiga yang mengakses dan menggunakan data dari Depkominfo semata-mata untuk tujuan bisnis (atau sebagai yang dimandatkan oleh Depkominfo). **Para pihak ketiga dan sub-kontraktor harus menandatangani perjanjian rahasia untuk mendapatkan akses terhadap informasi.**	• Meminta kepada pemilik akses terhadap informasi dan sistem. • Tidak menggunakan system dan informasi tanpa autorisasi. • Menggunakan perangkat akses yang aman yang disediakan oleh administrator. • Patuh pada kontrol yang ditempatkan oleh pemilik dan manajemen. • Melaporkan kesalahan dan keganjilan informasi kepada pemilik nya. • Melaporkan vulnerabilitas dan pelanggaran ke bagian Keamanan Informasi.

PERAN DAN TANGGUNG-JAWAB TERKAIT DENGAN ASET	Kebijakan No. 004	
Juli 2009	Versi 1.0	Revisi No.

DIAGRAM PERAN DAN TANGGUNG-JAWAB TERKAIT DENGAN ASET

PENJELASAN TANGUNG-JAWAB DAN ASET					
PENGGUNA					
Nama					
Supervisor					
Unit Kerja					
Jabatan					
Penjelasan Tanggung-jawab					
[Penjelasan]					
No. Aset	**Penjelasan**	**Klasifikasi**	**Pemrosesan Terautorisais**	**Akses**	**Access Dicabut**
				yyyy-mm-dd	yyyy-mm-dd

[DRAFT] Kebijakan Keamanan Informasi

PANDUAN KLASIFIKASI ASET	Kebijakan No. 005	
Juli 2009	Versi 1.0	Revisi No.

LEVEL KLASIFIKASI

Definisi	
Klasifikasi Empat Level	
Secret (Highly Restricted)	Informasi yang paling sensitive, yang ditujukan semata-mata untuk penggunaan internal, ditetapkan klasifikasi ini. Penyingkapan yang tidak terautorisasi dari jenis informasi ini dapat berdampak serius dan tidak baik pada organisasi, shareholder nya, partner, atau para pelanggan.
Confidential	Klasifikasi ini ditetapkan untuk informasi yang kurang sensitif, tapi masih ditujukan untuk penggunaan internal saja. Penyingkapan yang tidak terautorisasi dari jenis informasi ini dapat berakibat tidak baik pada organisasi, shareholder nya, partner, atau para pelanggan.
Private	Klasifikasi ini disediakan untuk informasi yang digunakan di dalam organisasi, dan penyingkapan yang tidak terautorisasi dapat berakibat serius dan tidak baik pada organisasi dan para pegawainya.
Unclassified	Klasifikasi ini mencakup informasi yang tidak sesuai dengan klasifikasi yang lainnya. Meskipun penyingkapan yang tidak terautorisasi pada jenis informasi ini adalah melanggar kebijakan, seharusnya tidak berdampak serius atau tidak bauk pada organisasi, shareholder nya, partner, atau para pelanggan.
Klasifikasi Tiga Level	
Confidential	Informasi yang kurang sensitif, meskipun demikian ditujukan untuk penggunaan internal, adalah diklasifikasikan juga. Penyingkapan nya yang tidak terautorisasi dapat berakibat tidak baik pada organisasi, shareholder nya, partner, atau para pelanggan.
Internal Use Only	Informasi dalam kategori ini seharusnya hanya dibuka kepada pihak ketiga yang telah menandatangani sebuah perjanjian kerahasiaan. Penyingkapannya seharusnya tidak menyebabkan kerugian yang serius pada organisasi. Informasi tersebut tersedia untuk seluruh pegawai melalui Intranet organisasi. Klasifikasi ini diterapkan kepada seluruh informasi yang tidak terklasifikasi secara default, dan melingkungi direktori-direktori telepon, dokumen-dokumen pelatihan, template-template, dan jadwal-jadwal.
Public	Informasi yang oleh bagian Hubungan Masyarakat telah disetujui secara eksplisit untuk didistrubusikan ke public, seperti *press releases.*

PANDUAN KLASIFIKASI ASET	Kebijakan No. 005	
Juli 2009	Versi 1.0	Revisi No.

Proses yang Diperlukan		**Klasifikasi Empat Level**				**Klasifikasi Tiga Level**		
Pemrosesan	**Langkah-langkah Keamanan**	**Secret**	**Confidential**	**Private**	**Unclassified**	**Confidential**	**Internal Use**	**Public**
Media Penyimpanan	Enkripsi atau kontrol akses yang jelas	X	X	X		X	X	
	Enkripsi (optional)				X			
	Enkripsi tidak direkomendasi							X
Penyalinan	Mendapat ijin pemilik adalah direkomendasikan	X	X	X		X		
	Tidak ada pembatasan				X		X	X
Pengiriman Fax	Perangkat penerima yang diproteksi oleh password	X	X	X		X		
	Tidak ada pembatasan				X		X	X
Transmisi melalui jaringan publik	Enkripsi	X	X	X		X		
	Enkripsi (optional)				X		X	
	Enkripsi tidak direkomendasi							X
Pengrusakan	Penyobekan atau pembuangan di tempat yang aman untuk tujuan ini	X	X	X		X		
	Keranjang sampah				X		X	X
Penyingkapan ke pihak ketiga	Ijin pemilik dan perjanjian *nondisclosure*	X	X	X		X		
	Perjanjian *Nondisclosure*				X		X	
	Tidak ada pembatas							X
Pelabelan media elektronik ketika diperlukan	Pelabelan Internal dan External	X	X	X		X		
	Tanggal dan klasifikasi penyingkapan							X
	Tidak diperlukan pelabelan				X		X	
Pelabelan dokumen jika dibutuhkan	Pada tiap halaman (jika tidak dijilid) dan pada sampul depan dan belakang dan halaman judul dari dokumen yang dijilid	X	X	X		X		
	Tanggal dan klasifikasi penyingkapan							X
	Tidak diperlukan pelabelan				X		X	

PANDUAN KLASIFIKASI ASET	Kebijakan No. 005	
Juli 2009	Versi 1.0	Revisi No.

Pemaketan surat internal dan eksternal	Ditujukan untuk penerima yang spesifik dan ditempatkan di dalam dua amplop, dengan label klasifikasi hanya di dalam amplop yg di dalam	X	X	X		X		
	Satu amplop tanpa jenis pelabelan yang spesifik				X		X	X
Pemberian hak akses	Hanya pemilik Aset	X	X	X		X		
	Pimpinan Setempat				X		X	
	Tidak ada pembatasan							X
Jejak Audit	Penerima, jumlah salinan yang dibuat, lokasi, alamat, penghancuran, saksi.	X						
	Hanya diperlukan jika pribadi		X	X		X		
	Tidak direkomendasikan				X		X	X

[DRAFT] Kebijakan Keamanan Informasi

PELATIHAN STAF KEAMANAN INFORMASI	Kebijakan No. 006	
Juli 2009	Versi 1.0	Revisi No.

Instruksi dan Pelatihan Dasar
Seluruh pegawai harus menerima pelatihan dan instruksi yang sesuai berkaitan dengan keamanan informasi : kebijakan-kebijakan, prosedur-prosedur, syarat-syarat keamanan, tanggung-jawab hukum, langkah-langkah kontrol, penggunaan fasilitas-fasilitas pemrosesan informasi, respon terhadap insiden-insiden dan malfungsi keamanan, penggunaan email dan Internet, dll. Beberapa bagian dari program pelatihan dapat diberikan oleh instruktur-instruktur dari luar.

Pembaharuan File Pegawai
Rincian dari seluruh pelatihan keamanan informasi yang diterima harus disimpan dalam file personil dari pegawai yang telah menerima pelatihan.

Analisa Kebutuhan
Kebutuhan-kebutuhan pelatihan dengan mudah diidentifikasi jika analisa kebutuhan pelatihan individu dilakukan. Analisa ini seharusnya dilengkapi sewaktu-waktu pelatihan tertentu dibutuhkan. Ketika keahlian, ketrampilan, dan kemampuan yang diharuskan untuk sebuah pekerjaan telah dibuat dan dimasukkan ke dalam *job description*, pemenuhan pegawai dengan syarat-syarat ini dapat dievaluasi dan kebutuhan pelatihan diidentifikasi.

Pelatihan Spesifik untuk Peran Spesifik
Pegawai dengan tugas keamanan informasi yang spesifik mungkin membutuhkan pelatihan teknikal. Deskripsi kerja dan kontrak pekerjaan dari posisi tertentu menguraikan tanggung-jawab keamanan informasi spesifik. Berikut adalah daftar posisi yang dapat membutuhkan pelatihan teknis. Daftar ini disesuaikan dengan organisasi.

Direktur Informasi	Personil Keamanan
Penasehat Keamanan Informasi	Pencari dan Pelatih sumber daya manusia
Anggota dari forum manajemen keamanan informasi	Pimpinan (secara umum)
Kepala Teknologi Informasi	Staf Keuangan
Kepala Jaringan	Sekertaris Eksekutif/personil legal
Staf support TI dan staf asisten teknis	Auditor system internal
Webmaster	Tim kelanjutan bisnis/respon keadaan darurat

[DRAFT] Kebijakan Keamanan Informasi

PELATIHAN STAF KEAMANAN INFORMASI	Kebijakan No. 007	
Juli 2009	Versi 1.0	Revisi No.

INFORMASI UMUM

Diagram di bawah menggambarkan bagaimana pesan elektronik di dalam organisasi dapat mengakibatkan masalah. Ini menunjukkan dasar pembenaran peletakan kebijakan-kebijakan di tempat pengelolaan penggunaan email, dan secara teratur membuat para pegawai peka pada kebiasaan yang sesuai ketika menggunakannya.