

Grand Design Sistem Informasi

Komisi Pemilihan Umum (KPU)

Buku V: Keamanan (Security)

DAFTAR ISI

DAFTAR ISI	II
1 PENDAHULUAN	1
2 DEFINISI SECURITY	3
2.1 KLASIFIKASI KEAMANAN SISTEM INFORMASI	3
2.2 ASPEK KEAMANAN.....	4
2.2.1 <i>Privacy / confidentiality</i>	4
2.2.2 <i>Integrity</i>	5
2.2.3 <i>Authentication</i>	6
2.2.4 <i>Availability</i>	6
2.2.5 <i>Non-repudiation</i>	7
2.2.6 <i>Access control</i>	7
2.3 PENGGUNAAN TEKNOLOGI KRIPTOGRAFI UNTUK PENGAMANAN	7
2.3.1 <i>Private-Key Cryptosystem</i>	8
2.3.2 <i>Public-key Cryptosystem</i>	9
2.4 TEKNOLOGI TAMBAHAN DALAM PENGAMANAN	9
2.4.1 <i>Kebijakan dan Prosedur Keamanan (Security Policies and Procedures)</i>	10
2.4.2 <i>Keamanan Aplikasi</i>	10
2.4.3 <i>Mengevaluasi Desain Jaringan KPU</i>	11
2.4.4 <i>Implementasi Firewall</i>	11
2.4.5 <i>Implementasi Intrusion Detection System (IDS)</i>	12
2.4.6 <i>Implementasi Network Management</i>	12
2.4.7 <i>Pemasangan Anti virus</i>	12
2.4.8 <i>Desain dan Implementasi Backup System & Dissaster Recovery Plan</i>	12
2.4.9 <i>Desain dan Implementasi Audit Trail</i>	13
3 DESAIN DAN IMPLEMENTASI PENGAMANAN SISTEM INFORMASI KPU	14
3.1 DEFINISI DALAM PENGAMANAN SISTEM INFORMASI KPU.....	14
3.1.1 <i>Pengguna</i>	14
3.1.2 <i>Sistem</i>	14
3.1.3 <i>Aplikasi</i>	14
3.1.4 <i>Contingency Planning</i>	15
3.2 SISTEM INFORMASI MONITORING PEMILU	15
3.2.1 <i>Pengguna</i>	16
3.2.2 <i>Sistem</i>	16
3.2.3 <i>Aplikasi</i>	16
3.2.4 <i>Contingency Planning</i>	16
3.3 SISTEM INFORMASI OPERASIONAL	16
3.3.1 <i>SIOGARA (Sistem Informasi Organisasi Penyelenggara)</i>	17
3.3.1.1 <i>Pengguna</i>	17
3.3.1.2 <i>Sistem</i>	17
3.3.1.3 <i>Aplikasi</i>	17
3.3.1.4 <i>Contingency Planning</i>	17
3.3.2 <i>SIDUKLIH (sistem Informasi Penduduk dan Pemilih)</i>	17
3.3.2.1 <i>Pengguna</i>	17
3.3.2.2 <i>Sistem</i>	18
3.3.2.3 <i>Aplikasi</i>	18

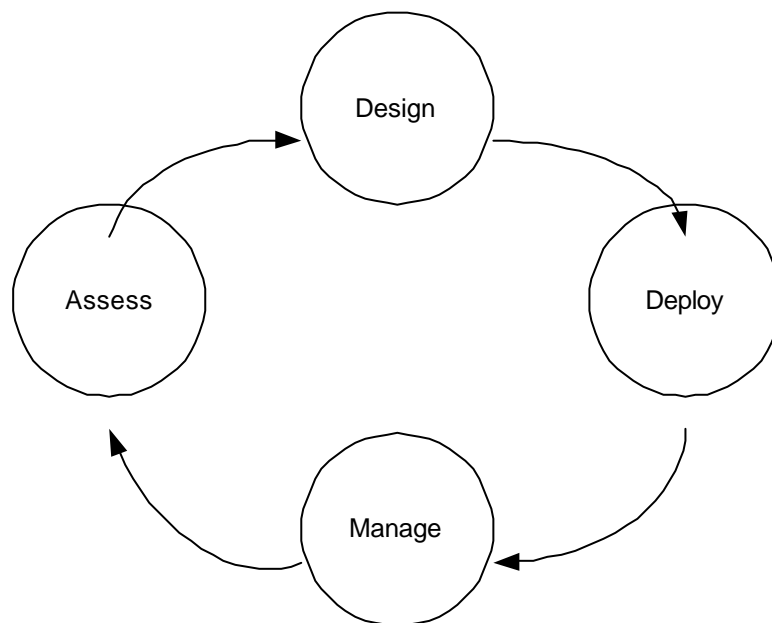
3.3.2.4 Contingency PLanning.....	18
3.3.3 SIPARPOL (<i>Sistem Informasi Partai Politik</i>).....	18
3.3.3.1 Pengguna.....	18
3.3.3.2 Sistem	18
3.3.3.3 Aplikasi.....	18
3.3.3.4 Contingency Planning.....	19
3.3.4 SIPERLU (<i>Sistem Informasi Perlengkapan Dan Logistik Pemilu</i>).....	19
3.3.4.1 Pengguna.....	19
3.3.4.2 Sistem	19
3.3.4.3 Aplikasi.....	19
3.3.4.4 Contingency Planning.....	19
3.3.5 SITUNG (<i>Sistem Informasi Penghitungan Suara</i>).....	19
3.3.5.1 Pengguna.....	19
3.3.5.2 Sistem	19
3.3.5.3 Aplikasi.....	20
3.3.5.4 Contingency Planning.....	20
3.3.6 SITAPLIH (<i>Sistem Informasi Penetapan Terpilih</i>).....	20
3.3.6.1 Pengguna.....	20
3.3.6.2 Sistem	20
3.3.6.3 Aplikasi.....	20
3.3.6.4 Contingency Planning.....	20
3.3.7 SIMALU (<i>Sistem Informasi Manajemen Pemilu</i>)	21
3.3.7.1 Pengguna.....	21
3.3.7.2 Sistem	21
3.3.7.3 Aplikasi.....	21
3.3.8.4 Contingency Planning.....	21
3.3.8 SIPANTAS (<i>Sistem Informasi Pemantauan Pemungutan Suara</i>).....	21
3.3.8.1 Pengguna.....	21
3.3.8.2 Sistem	21
3.3.8.3 Aplikasi.....	21
3.3.8.4 Contingency Planning.....	22
3.3.9 SIPORSILU (<i>Sistem Pelaporan Hasil Pemilu</i>).....	22
3.3.9.1 Pengguna.....	22
3.3.9.2 Sistem	22
3.3.9.3 Aplikasi.....	22
3.3.9.4 Contingency Planning.....	22
3.4 SISTEM INFORMASI ADMINISTRASI.....	22
3.4.1 SIPEG (<i>Sistem Informasi Kepegawaian</i>)	22
3.4.1.1 Pengguna.....	22
3.4.1.2 Sistem	22
3.4.1.3 Aplikasi.....	23
3.4.1.4 Contingency Plannning.....	23
3.4.2 SIPER (<i>Sistim Informasi Perlengkapan</i>).....	23
3.4.2.1 Pengguna.....	23
3.4.2.2 Sistem	23
3.4.2.3 Aplikasi.....	23
3.4.2.4 Contingency Planning.....	23
3.4.3 SIKEU (<i>Sistem Informasi Keuangan</i>).....	23
3.4.3.1 Pengguna.....	23
3.4.3.2 Sistem	23
3.4.3.3 Aplikasi.....	23

3.4.3.4 Contingency Planning.....	24
3.4.4 SIHUKUM (<i>Sistem Informasi Hukum</i>).....	24
3.4.4.1 Pengguna.....	24
3.4.4.2 Sistem	24
3.4.4.3 Aplikasi.....	24
3.4.4.4 Contingency Planning.....	24
3.4.5 Web Based IS.....	24
3.4.5.1 Pengguna.....	24
3.4.5.2 Sistem	24
3.4.5.3 Aplikasi.....	24
3.4.5.4 Contingency Planning.....	24
3.5 SISTEM INFORMASI PERKANTORAN	25
3.5.1 Pengguna.....	25
3.5.2 Sistem	25
3.5.3 Aplikasi.....	25
3.5.4 Contingency Planning.....	25
4 SDM SECURITY.....	26
4.1 USULAN PROGRAM KERJA SDM.....	26
4.1.1 Security Awareness.....	26
4.1.2 Security audit dan maintenance secara berkala.....	27
4.1.3 Pembuatan policy dan procedures.....	27
5 CONTINGENCY SISTEM OPERASI KPU	28
5.1 USULAN KERJA CONTINGENCY PLANNING.....	28
5.1.1 Definisi Sistem Contingency.....	28
5.1.2 Contingency Sites.....	28
5.1.3 Struktur Manajemen Sistem IT Contingency.....	28
5.1.4 Guide Disaster Planning.....	28
5.1.5 Evaluasi Inventory	29
5.1.6 Arsitektur Sistem Contingency.....	29

1 Pendahuluan

Aspek keamanan (*security*) merupakan salah satu aspek yang sering dipertanyakan dalam implementasi sebuah sistem informasi. Apalagi sistem yang akan dikembangkan di KPU memiliki data-data yang sangat sensitif. Untuk itu masalah keamanan perlu mendapat perhatian yang khusus. Buku ini tidak membahas aspek keamanan secara rinci, namun dapat memberikan kerangka implementasi dari sistem informasi KPU. Sudah banyak buku lain¹ yang membahas keamanan secara rinci.

Keamanan merupakan sebuah proses, bukan sebuah produk akhir. (*Security is a process, not an end product*) Hal ini ditegaskan oleh pakar security Bruce Schneier. Maksud dari pernyataan ini adalah tidak mungkin kita membuat sebuah sistem yang 100% aman untuk selama-lamanya. Setelah berjalan untuk suatu waktu akan ditemukan lubang keamanan yang dapat dieksploitasi. Selain ditemukan adanya lubang keamanan pada sistem yang lama, sistem informasi sering mendapat perbaikan (*upgrade*) dengan menambah perangkat dan teknologi baru. Misalnya adanya teknologi wireless (seperti handphone GSM, CDMA, komputer dengan perangkat yang mengerti protokol IEEE 802.11b) telah memungkinkan untuk mengakses sistem informasi melalui perangkat wireless (handphone, PDA²). Penambahan perangkat baru ini dapat menimbulkan lubang baru yang tidak diprediksi sebelumnya. Untuk itu pengamanan sistem informasi harus dilakukan secara terus menerus.



Gambar 1.1. Security Life Cycle

¹ Contoh buku tentang keamanan dalam bahasa Indonesia adalah buku karangan Budi Rahardjo, "Keamanan Sistem Informasi Berbasis Internet," yang dapat diperoleh dari Internet. Lihat <http://budi.insan.co.id>

² PDA = Personal Digital Assistant, perangkat komputer dalam ukuran kecil yang dapat dibawa kemana-mana.

Keamanan berbanding terbalik dengan kenyamanan (*convenience*). Jika kita ingin membuat sebuah sistem informasi yang sangat aman, maka dia akan sulit digunakan dan bahkan menjadikannya tidak berfungsi. Sebagai contoh, jika kita ingin mengamankan sebuah kumpulan data dalam bentuk elektronik maka kumpulan data tersebut dapat saya simpan dalam sebuah computer notebook (atau laptop) yang kemudian saya simpan di dalam peti besi. Peti besi ini dapat disimpan di ruangan yang dijaga secara fisik oleh Polisi. Data-data tersebut mungkin aman, akan tetapi dapat dipastikan bahwa untuk mengakses data tersebut sangat tidak nyaman. Untuk meningkatkan kenyamanan, data dapat disimpan dalam komputer yang terhubung dengan LAN (Local Area Network). Kenyamanan meningkat karena data-data dapat diakses dari workstation lain yang terhubung dengan LAN tersebut. Akan tetapi nilai keamanannya menurun karena pengguna lain di LAN yang sama memiliki potensi untuk mengakses data tersebut. Pengguna lain ini belum tentu boleh mengakses data tersebut. Untuk meningkatkan kenyamanan, maka data-data dapat dipasang pada sebuah server yang terhubung dengan Internet sehingga data-data tersebut dapat diakses darimana saja. (Tentunya dengan menggunakan password.) Untuk yang terakhir ini, potensi lubang keamanan menjadi lebih besar. Dari uraian di atas dapat kita lihat bahwa keamanan berbanding terbalik dengan kenyamanan. Pemilihan keamanan (atau kenyamanan) menjadi bergantung kepada pengguna.

Dalam bab-bab dokumen ini akan dibahas perincian dari segi keamanan Sistem Informasi KPU yang akan meliputi data yang dipergunakan oleh KPU, pengguna dari setiap aplikasi, aplikasi-aplikasi yang akan digunakan, jaringan dan juga hardware. Termasuk dalam perincian definisi-definis security yang berhubungan dengan keamanan suatu sistem. Kemudian, dari definisi-definis tersebut akan lebih diperinci untuk setiap aspek dari Sistem Informasi KPU. Antara lain adalah level dari security baik dari segi fisik dan non-fisik, perincian mengenai backup data dan Contingency Planning untuk setiap aplikasi. Selanjutnya, juga akan dibahas SDM yang diperlukan guna menjaga keamanan dari sistem.

2 DEFINISI SECURITY

Melihat uraian pada bagian sebelumnya, definisi dari keamanan menjadi tidak baku. Garfinkel dan Spafford mendefinisikan *computer security* sebagai berikut:

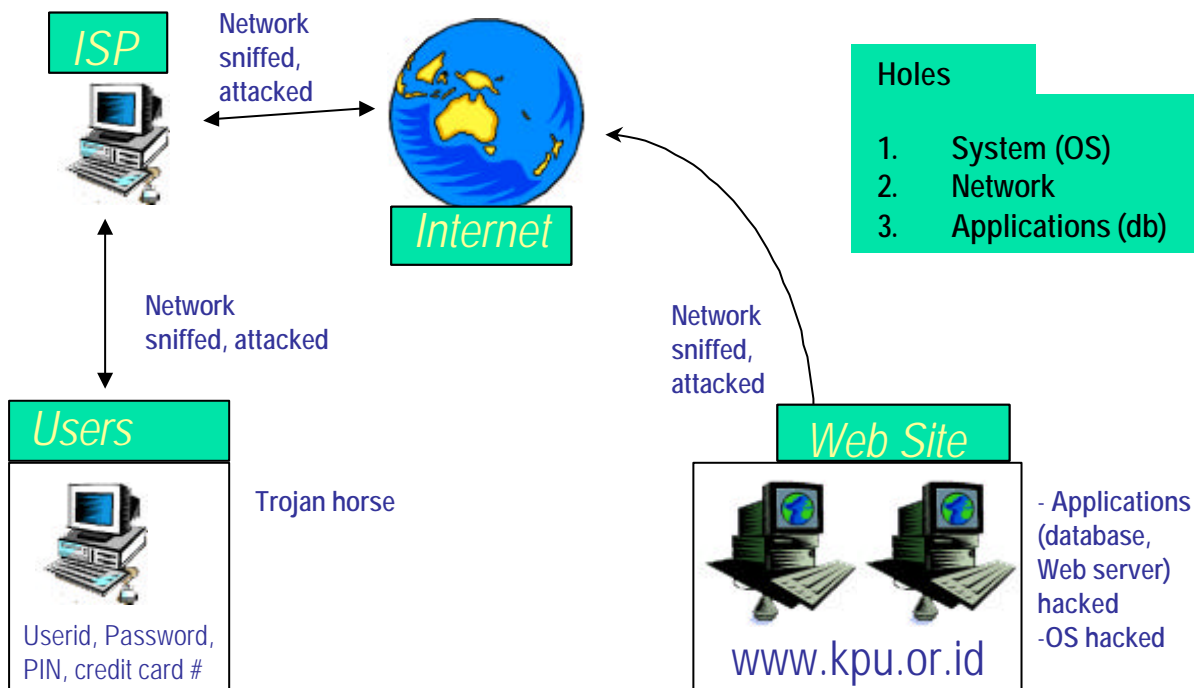
"A computer is secure if you can depend on it and its software to behave as you expect"

Definisi di atas dapat diperluas untuk jaringan (*network*), aplikasi, dan sistem. Definisi tersebut juga memberikan kelonggaran atas apa yang disebut aman (*secure*). Aman menurut seseorang belum tentu aman untuk orang lain. Hal lain yang perlu mendapat perhatian adalah *security* bergantung kepada *expectation* dan nantinya terkait dengan resiko yang dapat diterima (mau diambil) oleh pengguna dan pengelola sistem informasi itu sendiri.

2.1 KLASIFIKASI KEAMANAN SISTEM INFORMASI

Dilihat dari fungsinya dalam sebuah sistem informasi, keamanan dapat dibagi menjadi tiga kelompok:

- **Network security:** fokus kepada media pembawa informasi/data, seperti jaringan komputer;
- **Computer security:** fokus kepada komputer (server, workstation, terminal), termasuk di dalamnya masalah yang berhubungan dengan operating system; dan
- **Application security:** fokus kepada program aplikasi (software) dan database.



Gambar 2.1. Hubungan antara keamanan jaringan, komputer, dan aplikasi

Gambar 5.1 menunjukkan hubungan antara ketiga komponen tersebut beserta kemungkinan serangan (*attack*). Sisi "users" (pengguna) merupakan pengguna yang ingin mengakses informasi. Dia menggunakan ISP untuk mengakses Internet. Penyedia informasi ("web site") bisa berupa situs hasil pemilu di KPU.

Contoh serangan terhadap jaringan (network) meliputi penyadapan data atau pengiriman data yang berlebihan (*flooding*). Serangan ini dapat terjadi di sisi jaringan mana saja, baik di sisi pengguna maupun di sisi penyedia informasi sebagaimana dapat dilihat pada gambar 5.1 tersebut. Penyadapan data merupakan serangan terhadap aspek *confidentiality*, sementara network flooding merupakan serangan terhadap aspek *availability*.

Contoh serangan terhadap komputer adalah adanya *virus* dan *trojan horse* di sisi pengguna yang dapat menghapus data-data, mengirimkan data yang rahasia, atau menghabiskan *resources* (memory, harddisk, CPU cycle) milik pengguna tersebut. Virus ini dapat masuk melalui email atau melalui situs web.

Contoh serangan terhadap aplikasi adalah adanya setup database yang kurang benar sehingga *record* yang terdapat pada database tersebut dapat diubah-ubah. Hal ini akan berbahaya jika data-data (*record*) tersebut merupakan informasi yang sangat vital (seperti misalnya data kepegawaian atau data hasil pemilu). Pengembangan aplikasi juga harus memperhatikan masalah validasi dari data. Dikarenakan SIKPU akan banyak menggunakan web sebagai basis dari aplikasinya, maka keamanan sistem web akan menjadi suatu hal yang perlu diperhatikan. (Pembahasan yang lebih lengkap mengenai keamanan sistem web ada pada berbagai buku referensi seperti misalnya buku karangan Lincoln D. Stein yang berjudul "Web Security: A step-by-step reference guide", Addison-Wesley.)

2.2 ASPEK KEAMANAN

Keamanan sebuah sistem informasi memiliki beberapa aspek keamanan, yaitu:

1. Privacy / confidentiality
2. Integrity
3. Authentication
4. Availability
5. Non-repudiation
6. Access control

Tidak kesemua aspek tersebut harus diimplementasikan pada sebuah sistem informasi. Umumnya implementasi sebuah SI menggunakan beberapa bagian dari aspek tersebut.

2.2.1 Privacy / confidentiality

Aspek ini berhubungan dengan kerahasiaan data-data. Banyak data yang harus dirahasiakan seperti nama, tempat tanggal lahir, agama, hobby, penyakit yang pernah diderita, data pelanggan, dan sebagainya. Untuk KPU data-data yang dirahasiakan antara lain adalah data-data kepegawaian (untuk keperluan internal, kenaikan pangkat, dan sejenisnya), dan data-data pemilih dalam pemilihan umum. Data-data ini hanya boleh diakses oleh orang yang berhak. Implementasi sistem informasi harus dapat menjamin aspek privacy atau confidentiality ini.

Serangan terhadap aspek ini antara lain adalah penyadapan data atau *interception* (misalnya dengan menggunakan program sniffer yang menyadap data di jaringan LAN atau Internet), virus (misalnya virus *SirCam* yang mengirimkan data-data dari

harddisk kita ke orang lain tanpa sepengetahuan kita), trojan horse (misalnya software Back Orifice atau Subseven yang dapat mengendalikan komputer *victim* dari jarak jauh) atau password yang dituliskan pada secarik kertas sehingga dapat digunakan oleh orang lain.

Banyak aplikasi di jaringan yang masih menggunakan plain (clear) text ketika mengirimkan userid dan password. Sebagai contoh aplikasi telnet (untuk mengakses server dan router dari jarak jauh), FTP (untuk transfer file), dan POP (untuk membaca atau mendownload email) masih menggunakan pasangan userid dan password yang dapat disadap. Aplikasi-aplikasi ini sebaiknya digantikan dengan aplikasi yang menggunakan enkripsi. Sebagai contoh, telnet dapat digantikan dengan SSH (secure shell), sementara FTP dapat digantikan dengan scp (secure copy). Implementasi dari aplikasi ini dapat diperoleh dari Internet.

Serangan juga dapat dilakukan secara fisik dengan cara mencuri notebook yang berisi data-data penting. Seharusnya data-data penting di notebook dienkripsi sehingga bila notebook dicuri atau hilang, maka data-data tersebut tidak dapat dibaca orang dengan mudah. Namun pada kenyataannya hal ini jarang dilakukan.

Pengamanan terhadap aspek kerahasiaan ini dapat dilakukan dengan berbagai cara. Salah satu cara adalah dengan menggunakan teknologi kriptografi untuk mengacak data-data, menggunakan jaringan yang terpisah (*dedicated line*), segmentasi jaringan, penggunaan firewall, dan dengan menggunakan *switch device* sebagai pengganti hub di LAN. Penggunaan *secure email*, seperti dengan menggunakan program PGP³ (*Pretty Good Privacy*), juga merupakan usaha untuk mengamankan kerahasiaan data. Masih banyak lagi teknik-teknik pengamanan yang dapat digunakan yang pada prinsipnya adalah mempersulit orang yang tidak berhak untuk menyadap data. Namun lagi-lagi pengamanan dengan menggunakan enkripsi sering tidak dilakukan karena menambah pekerjaan bagi pengguna dan tidak nyaman.

2.2.2 Integrity

Integrity (keutuhan) mengatakan bahwa data atau informasi tidak boleh berubah (*tampered, altered, modified*) tanpa izin dari pemilik. Bagi KPU, keutuhan data ini menjadi penting misalnya pada pelaksanaan pemilu. Data-data hasil pemilu tidak boleh diubah oleh orang yang tidak berhak.

Serangan terhadap aspek *integrity* adalah adanya virus, trojan horse, *man in the middle attack*, atau masuknya orang yang tidak berhak ke sistem informasi. Tanpa ada pengamanan data-data dapat diubah sehingga tidak utuh lagi. Jika hal ini terjadi maka keabsahan data dapat dipertanyakan.

Pengamanan terhadap aspek ini adalah dengan menggunakan (*digital*) *signature*, *checksum*, *hash algorithm*, dan teknik-teknik lain. Pada intinya sistem pengamanan akan memberikan tanda apabila data sudah berubah. Karena seringkali serangan terhadap aspek ini dilakukan dengan menggunakan virus,

³ Informasi mengenai PGP dapat diperoleh dari <http://www.pgp.com> dan <http://www.pgpi.com>. Yang terakhir ini adalah untuk PGP versi Internasional.

maka penggunaan anti virus menjadi salah satu mekanisme pengamanan yang harus dilakukan.

2.2.3 Authentication

Aspek *authentication* digunakan untuk meyakinkan keaslian data, sumber data, orang yang mengakses data, dan server yang digunakan. Aplikasinya di KPU dapat beragam. Pengiriman data dari sebuah sumber harus dapat dicek kebenaran (keaslian) sumber tersebut. Orang yang akan mengakses database KPU (atau masuk ke ruangan server / Network Operation Center) harus menunjukkan identitasnya dan membuktikan bahwa dia adalah orang yang berhak mengakses database atau sistem tersebut. Hal ini dapat diimplementasikan dengan menggunakan tanda pengenalan, password, digital signature, dan biometrics.

Untuk pelayanan kepada masyarakat, situs web KPU harus dilengkapi dengan tanda bukti (certificate) bahwa dia adalah situs resmi dari KPU. Dengan adanya tanda bukti ini maka pengguna dapat merasa aman bahwa dia memang mengakses situs KPU.

Serangan terhadap mekanisme authentication antara lain adalah pemalsuan password, tanda pengenalan, atau identitas lainnya. Sebagai contoh situs web “kilkbca.com”⁴ merupakan pemalsuan (penyaruhan) situs “klikbca.com”. Situs palsu ini mengauthenticate bahwa dia adalah situs dari Internet Banking BCA. Serangan lain adalah dengan menggunakan alamat komputer palsu (dikenal dengan istilah spoofing) atau bahkan dengan menggunakan alamat email palsu.

Pengamanan dapat dilakukan dengan menggunakan tanda pengenalan, password, digital signature, dan biometrics.

2.2.4 Availability

Aspek availability (ketersediaan) menjamin bahwa data dan informasi harus dapat tersedia ketika dibutuhkan. Suatu sistem informasi akan tidak bermanfaat jika dia tidak dapat memberikan data ketika dibutuhkan. Bayangkan apabila SIKPU berhenti di tengah jalan ketika sedang memproses pemilu. Dampak negatifnya sangat luar biasa.

Serangan terhadap aspek ketersediaan dikenal dengan istilah Denial of Service (DoS) attack. Contoh dari DoS attack adalah membuat sistem atau server menjadi hang atau crash, jaringan dibanjiri oleh sampah (*network flooding, exhaust network*), atau aplikasi dibuat menjadi tidak berfungsi. Banyak software yang dapat diambil dari Internet yang dapat melakukan DoS attack tersebut. Bahkan saat ini metoda penyerangan telah meningkat dengan mendistribusikan “agen penyerang” ke beberapa (banyak) komputer sehingga ada istilah yang disebut *Distributed DoS* (DDoS) attack. Pada DDoS attack, target diserang oleh ratusan komputer pada saat yang bersamaan. Seringkali pemilik komputer yang digunakan untuk menyerang tidak tahu bahwa komputernya digunakan untuk menyerang orang lain.

⁴ Perhatikan bahwa huruf “i” dan “l” tertukar pada kata “klik” yang berubah menjadi “kilk”.

Serangan ini tidak saja dilakukan secara logika akan tetap juga dapat dilakukan secara fisik, misalnya dengan merusak server, mencuri server, menghancurkan lokasi server, atau memutuskan jaringan. Bencana alam (natural disaster) seperti banjir juga dapat mengakibatkan hilangnya ketersediaan sistem informasi sehingga dapat dikategorikan ke dalam kelompok ini. Demikian pula ketidaksengajaan (menghapus file penting dengan tidak sengaja), salah menggunakan program dapat juga dimasukkan dalam kelompok ini.

Pengamanan dari aspek ketersediaan bervariasi dari pendeteksian adanya serangan (melalui *Intrusion Detection System* atau IDS), backup, *audit trail*, *disaster recovery*, sampai kepada pembuatan mirror dari sistem di tempat lain.

2.2.5 Non-repudiation

Aspek *non-repudiation* mengatakan bahwa seseorang tidak dapat menyangkal apabila dia telah melakukan sebuah transaksi. Aplikasi untuk KPU di pemilihan umum antara lain adalah apabila seseorang yang telah menggunakan hak suaranya (vote) tidak dapat menyangkal bahwa dia sudah menggunakan hak suaranya. Atau seseorang yang mengirimkan email yang dilengkapi dengan tanda tangan digitalnya tidak dapat menyangkal bahwa dia telah mengirimkan email tersebut.

Implementasi dari non-repudiation adalah dengan menggunakan digital signature dan digital certificates. Pengguna menandatangani kegiatannya secara digital sehingga tidak dapat menampik bahwa dia telah melakukan kegiatan tersebut. Dalam implementasinya ada pihak ketiga yang menjadi saksi tentang keabsahan tanda tangan digital tersebut.

2.2.6 Access control

Aspek ini membatasi atau mengatur siapa boleh melakukan apa. Biasanya akses ke suatu data atau sistem memiliki tingkat (level, jenjang). Sebagai contoh seorang pengguna biasa di sistem informasi KPU hanya boleh mengakses informasi yang umum dan terbatas. Sementara itu pimpinan KPU dapat mengakses informasi yang lebih detail. Administrator memiliki akses untuk mengubah data. (Lihat pada bagian aplikasi untuk mengetahui lebih lengkap mengenai siapa yang dapat mengakses data apa saja.)

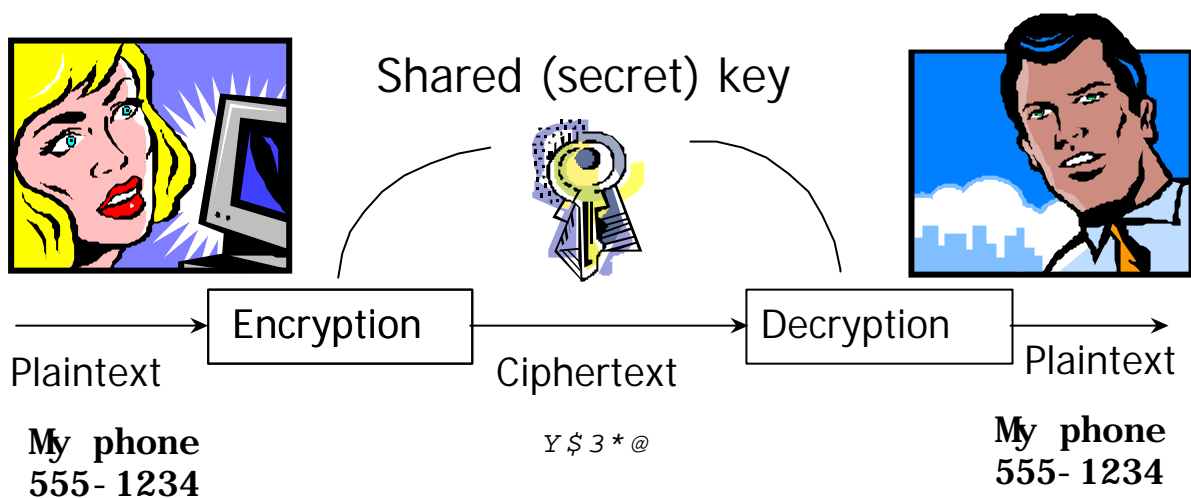
Implementasi access control biasanya menggunakan password atau dengan menggunakan token lainnya. Sebagai contoh untuk masuk ke ruang server KPU bisa digunakan badge/ID tag yang dilengkapi dengan magnetic atau smartcard. Untuk sistem keamanan yang lebih tinggi dimungkinkan penggunaan biometrik (tangan, sidik jari jempol, mata) untuk access control.

2.3 PENGGUNAAN TEKNOLOGI KRIPTOGRAFI UNTUK PENGAMANAN

Teknologi kriptografi pada berbagai kasus dapat digunakan untuk meningkatkan keamanan sistem informasi. Teknik pengacakan data (enkripsi) dapat digunakan untuk mengacak data sehingga sulit dibaca oleh pihak yang tidak berhak. Hanya pihak yang dituju yang dapat membuka data (dekripsi) dengan menggunakan kuncinya.

Pada saat ini ada dua sistem kriptografi yang umum dipakai, yaitu *private-key cryptosystem* (atau dikenal juga dengan nama *symmetric cryptosystem*) dan *public-key cryptosystem* (dikenal juga dengan nama *asymmetric cryptosystem*). Pada *private-key cryptosystem*, sistem menggunakan satu kunci untuk mengunci (*encrypt*) dan membuka (*decrypt*) data. Sementara itu pada *public-key cryptosystem* digunakan dua kunci, yaitu kunci privat dan kunci publik untuk melakukan proses enkripsi dan dekripsi. Secara visual keterangan kedua sistem ini dapat dilihat pada gambar 2.3.1 dan 2.3.2 dan dibahas pada bagian berikut.

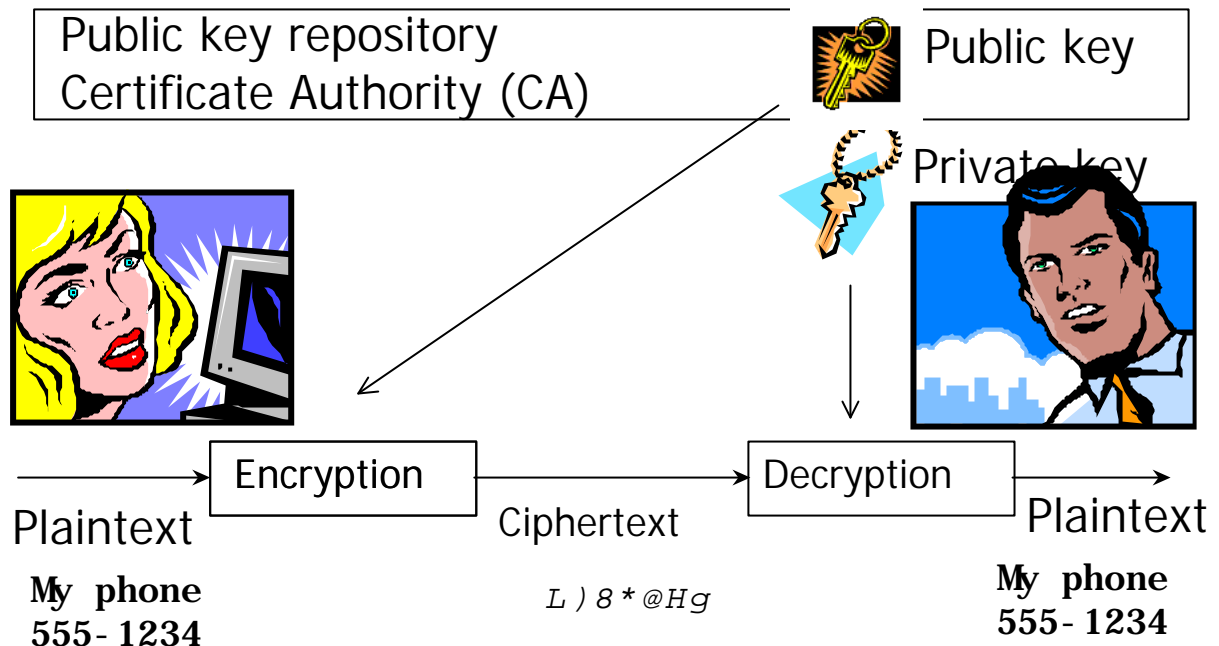
2.3.1 Private-Key Cryptosystem



Gambar 2.2. Private-key cryptosystem.

Pada gambar 2.2 ditunjukkan bahwa sebuah kunci (shared key) digunakan untuk mengunci dan membuka pesan. Sistem kriptografi kunci privat sudah banyak digunakan dengan algoritma yang cepat. Namun dia memiliki beberapa kekurangan, antara lain adalah kesulitan dalam mengelola dan mendistribusikan kunci. Sebagai contoh, bagaimana mengkomunikasikan kunci yang akan digunakan? Jika kunci tersebut dikirimkan melalui saluran yang sama maka akan percuma sebab kita mengambil asumsi saluran tidak aman. Jika saluran sudah aman, untuk apa dienkripsi lagi? Untuk setiap pasangan pengguna harus digunakan kunci yang berbeda. Akibatnya jumlah kunci yang harus digunakan akan membengkak secara eksponensial, yaitu $(n)(n-1)$ dimana n adalah jumlah pengguna. Bayangkan jika n memiliki nilai jutaan, sebagaimana jumlah pengguna Internet di dunia. Algoritma yang mengimplementasikan sistem kriptografi kunci privat antar lain adalah DES dan IDEA.

2.3.2 Public-key Cryptosystem



Gambar 2.3. Public-key cryptosystem

Gambar 2.3 menunjukkan konfigurasi dari sebuah public-key cryptosystem. Setiap pengguna memiliki dua buah kunci, kunci privat dan kunci publik. Kunci privat hanya diketahui oleh pengguna itu sendiri, sementara kunci publik boleh diketahui oleh semua orang. Kunci publik ini dapat disimpan dalam sebuah database (public key repository) dan dapat disertifikasi oleh sebuah lembaga certificate authority (CA). Sebuah pesan yang dikunci oleh kunci publik (public key) hanya dapat dibuka oleh kunci privat (private key). Sebaliknya, pesan yang dikunci oleh kunci privat hanya dapat dibuka oleh kunci publik. Yang terakhir ini merupakan fungsi dari tanda tangan digital (digital signature).

Sistem krypto dengan kunci publik memiliki tingkat keamanan yang tinggi. Namun untuk melakukan enkripsi (dan dekripsi) diperlukan komputasi yang sangat lebih sulit dibandingkan dengan sistem krypto kunci privat. Akibatnya sistem ini membutuhkan waktu yang lebih lama untuk melakukan proses enkripsi (dan dekripsi). Algoritma yang mengimplementasikan sistem krypto kunci privat antara lain adalah RSA dan ECC (Elgamal).

2.4 TEKNOLOGI TAMBAHAN DALAM PENGAMANAN

Pengamanan Sistem Informasi KPU harus dapat memberikan jaminan terhadap aspek keamanan (privacy / confidentiality, integrity, authentication, availability, non-repudiation, dan access control). Pilihan implementasi bergantung kepada tingkat keamanan yang diinginkan, budget, dan ketersediaan teknologi. Pada bagian berikut akan dibahas beberapa usulan implementasi dari pengamanan sistem informasi KPU. Perlu diingat bahwa usulan di bawah ini masih bergantung kepada budget dan ketersediaan teknologi (yang berubah dengan sangat cepat).

Sebagian besar dari desain yang dijabarkan pada bagian ini bertitik berat pada sistem internal KPU, bukan pada sistem untuk Pemilu. Masalah keamanan sistem Pemilu akan mendapat pembahasan yang lebih mendalam pada bagian lain.

2.4.1 Kebijakan dan Prosedur Keamanan (Security Policies and Procedures)

Computer crimes are committed by people, not machines. Strong policies and procedures attack this human element and reinforce other security measures. (Richard W. Baker, "Network Security")

"Security policy and procedures" (kebijakan dan prosedur yang terkait dengan keamanan) merupakan komponen penting sebab dia yang menjadi perantara antara sistem keamanan dengan manusia pengguna sistem informasi tersebut. Ini merupakan langkah awal dari sebuah arsitektur sistem informasi jika dilihat dari sudut pandang *security*.

Kebijakan dan prosedur keamanan dari SIKPU ini harus sejalan dengan asas atau kebijakan yang mengatur aktivitas KPU. Kebijakan dan prosedur keamanan ini harus didukung oleh management agar dia dapat menjadi efektif. Kebijakan dan prosedur keamanan ini dibuat dengan mempertimbangkan kemudahan (kenyamanan) melakukan kegiatan, karena biasanya semakin tinggi tingkat keamanan semakin tidak nyaman untuk melakukan kegiatan.

Kebijakan dan prosedur keamanan ini harus ada dan dimengerti oleh semua pengguna dan pengelola sistem informasi KPU. Sebagai contoh, apa saja hak dari pengguna sistem informasi ini? Apakah kegiatan pegawai di KPU boleh disadap jika yang bersangkutan diduga melakukan tindak kejahatan? Apa hak dan kewajiban pengelola sistem informasi? Apa yang harus dilakukan oleh pengelola bila ada pengguna lain yang melakukan probing atau port scanning terhadap situs web KPU? Bagaimana jika pengguna SIKPU menerima *junk mail* atau *spam*⁵? Atau bagaimana jika justru pengguna SIKPU yang melakukan *spamming*? Kesemua ini harus terjawab dalam security policies and procedures. Dokumentasi dari kebijakan dan prosedur keamanan sebaiknya tidak terlalu tebal sehingga membingungkan pengguna. Sosialisasi dan penerapan dari kebijakan dan prosedur keamanan ini dapat dilakukan melalui pelatihan.

Inti dari kebijakan dan prosedur keamanan adalah:

- Membuat setiap pengguna bertanggung jawab (*accountable*) terhadap perilakunya (*actions, behaviors*).
- Mendesain sistem sedemikian rupa sehingga untuk melakukan kejahatan (*crime, fraudulent act*) dibutuhkan lebih dari satu orang.

2.4.2 Keamanan Aplikasi

Sebelum melakukan implementasi aplikasi-aplikasi SIKPU (baik untuk keperluan Pemilu maupun untuk kegiatan kesekretariatan), perlu dilakukan kegiatan untuk

⁵ Spamming atau pengiriman junk mail adalah mengirimkan email kepada orang yang tidak dikenal dan tidak mengharapkan menerima email dari anda. Spamming biasanya berisi tentang tawaran barang atau jasa.

mengklasifikasikan data atau informasi. Hasil dari proses klasifikasi ini dapat diimplementasikan ke dalam program aplikasi, misalnya untuk mekanisme *authentication* dan *access control*. Klasifikasi dari data dan/atau informasi ini dapat dibagi menjadi empat (4) kelas seperti dijabarkan pada tabel berikut.

Klasifikasi	Definisi
Public	Informasi yang secara eksplisit dinyatakan untuk publik. Informasi ini dapat dikomunikasikan melalui terbitan konvensional (majalah, surat kabar, newsletter) dan/atau WWW
Internal	Informasi yang tidak/belum boleh diketahui oleh umum tapi sudah diketahui di dalam (internal). Informasi ini dapat dijadikan publik apabila sudah mendapat persetujuan. Informasi ini juga dapat tetap menjadi internal.
Confidential	Informasi yang bilamana bocor dapat memberikan dampak negatif yang berat terhadap institusi, pekerjaannya, dan pihak-pihak yang terkait. Informasi ini dapat diketahui oleh pekerja internal namun tidak diperuntukan untuk publik.
Restricted	Informasi yang bilamana bocor dapat memberikan dampak negatif yang sangat kritis terhadap masalah finansial, hukum (legal), regulatory, atau reputasi dari institusi, pekerjaannya, dan pihak yang terkait. Informasi ini hanya diketahui oleh orang-orang tertentu saja.

Program aplikasi yang dikembangkan harus memiliki fasilitas *audit trail*, misal dalam bentuk logfile, sehingga ketika ada masalah dapat diketahui penyebabnya.

Khusus untuk aplikasi perhitungan suara, **source code dari aplikasi ini harus tersedia untuk proses review**. Banyak pihak yang takut adanya trojan horse atau logic bomb yang ditanamkan dalam software ini. Misalnya, ditakutkan ada kode yang memenangkan partai tertentu atau kode yang dapat dijalankan oleh oknum. Untuk menghindari hal ini, maka source code dari aplikasi ini harus tersedia.

2.4.3 Mengevaluasi Desain Jaringan KPU

Tahap awal dalam implementasi jaringan KPU adalah melakukan evaluasi terhadap desain, baik untuk intranet maupun hubungan ke Internet. Dalam kerangka SIKPU ini diprediksi adanya kebutuhan akses dari institusi lain dan KPU daerah. Untuk itu desain dari jaringan KPU ini harus dilakukan secara teliti dengan memperhatikan faktor keamanan. Peningkatan faktor keamanan dapat dilakukan dengan cara melakukan segmentasi dan menggunakan perangkat yang memiliki tingkat keamanan yang lebih tinggi (misal menggunakan switch sebagai pengganti hub biasa).

2.4.4 Implementasi Firewall

Sebetulnya kegiatan ini merupakan turunan atau hasil dari kegiatan sebelumnya, desain jaringan KPU yang terhubung ke Internet. Namun kami memperkirakan bahwa penggunaan firewall merupakan sebuah keharusan.

Firewall merupakan pengaman yang memisahkan jaringan internal KPU dengan jaringan Internet. Jika dianalogikan dengan rumah, maka firewall merupakan pagar

yang melindungi rumah. Tamu harus melalui pagar (firewall) dulu sebelum masuk ke rumah. Ada beberapa jenis firewall. Pemilihan firewall yang tepat membutuhkan pengkajian yang lebih mendalam. Sistem Informasi KPU harus memiliki firewall untuk memisahkan jaringan internal dengan Internet.

2.4.5 Implementasi Intrusion Detection System (IDS)

Sama halnya dengan firewall, Intrusion Detection System (IDS) merupakan konsekuensi dari desain jaringan KPU. Namun, kami memperkirakan bahwa penggunaan IDS ini merupakan sebuah keharusan (mandatory).

IDS mendeteksi adanya intrusion (tamu yang tidak diundang). Jika dianalogikan dengan rumah, maka IDS mirip dengan sistem alarm. Perlu diingat bahwa IDS akan memberikan tanda **setelah** intruder masuk.

Ada dua jenis IDS, yaitu network-based IDS dan host-based IDS. Network-based IDS mengamati jaringan untuk mendeteksi adanya kelainan (anomali). Sebagai contoh, network flooding atau port scanning, usaha pengiriman virus melalui email akan terdeteksi oleh IDS ini. Sementara host-based IDS dipasang pada host untuk mendeteksi kelainan pada host tersebut (misalnya ada proses yang semestinya tidak jalan akan tetapi sekarang sedang jalan, adanya virus di workstation).

2.4.6 Implementasi Network Management

Penggunaan jaringan membutuhkan perangkat untuk mengelola. Istilah yang sering digunakan adalah Network Management. Pengelola dapat memantau penggunaan jaringan untuk mendeteksi adanya masalah (jaringan tidak bekerja, lambat, dan seterusnya).

Implementasi dari network management dapat bervariasi. Standar yang sering digunakan saat ini adalah SNMP (Simple Network Management Protokol).

2.4.7 Pemasangan Anti virus

Mengingat bahwa banyak lubang keamanan dikirimkan melalui email, maka penggunaan anti virus yang up-to-date merupakan sebuah keharusan. Anti virus ini harus dipasang pada setiap workstation dan server yang ada di jaringan sistem informasi KPU. Perlu diperhatikan bahwa penggunaan program anti-virus bajakan tidak diperkenankan di SIKPU.

2.4.8 Desain dan Implementasi Backup System & Disaster Recovery Plan

Untuk menghindari hal-hal yang tidak diinginkan seperti hilangnya data, SIKPU harus memiliki backup system. Backup system yang sederhana atau paling minimal berupa backup data ke media tape, CD, dan optical. Namun juga sebaiknya dicadangkan server (standby) dan disk yang dapat digunakan dengan segera apabila server mengalami masalah. Selain on-site backup, perlu diimplementasikan off-site backup yaitu backup data yang diletakkan di tempat lain (bahkan di tempat yang secara fisik berjauhan). Di Jakarta ada beberapa data

center yang dapat digunakan untuk disaster recovery sites. Sementara itu tempat di luar kota Jakarta perlu dicari.

Selain backup data, harus dipersiapkan juga backup dari listrik (catu daya). Sistem yang penting harus dilengkapi dengan UPS. Untuk sistem yang harus bekerja dalam jangka waktu yang lama, perlu disediakan fasilitas diesel karena umumnya UPS tidak dapat bertahan lama. Servis yang penting juga harus dibuatkan mirrornya di tempat lain. Sebagai contoh, sistem yang digunakan untuk penghitungan data pemilihan umum termasuk kategori yang harus bekerja (*available*) selama pemilihan umum berlangsung.

Pengamanan lain yang harus dipersiapkan adalah perangkat anti petir. Seringkali jaringan telepon dan LAN terkena serangan petir. Akibatnya tidak saja perangkat jaringan yang kena, akan tetapi server dan workstation dapat juga kena.

2.4.9 Desain dan Implementasi Audit Trail

Setiap kegiatan yang berdampak kepada SIKPU harus dicatat dalam berkas log. Kegiatan yang normal (seperti update software) dan juga usaha untuk pengrusakan (akses yang tidak berhak) akan tercatat dalam log. Audit trail ini dapat digunakan untuk memperbaiki sistem jika ada kesalahan atau masalah.

Pada implementasinya data-data yang digunakan untuk audit trail bisa berukuran besar. Untuk itu perlu dipersiapkan sistem dengan storage yang besar dan mesin pengolah data yang memiliki kemampuan untuk mengolah data dengan cepat. Implementasi dari network management dapat bervariasi. Standar yang sering digunakan saat ini adalah SNMP (Simple Network Management Protokol). Dokumentasi dari security policies and procedures sebaiknya tidak terlalu tebal sehingga membingungkan pengguna. Sosialisasi dan penerapan dari security policies & procedures ini dapat dilakukan melalui pelatihan.

3 Desain dan Implementasi Pengamanan Sistem Informasi KPU

Berdasarkan pembahasan dalam bab 2 mengenai berbagai aspek keamanan yang harus dipertimbangkan, bab ini akan membahas implementasi pengamanan dalam Sistem Informasi KPU. Khususnya, bab 3 ini adalah perincian dalam aspek pengguna, sistem, aplikasi dan contingency planning. Namun pembahasan contingency planning akan lebih diperinci di bab 5.

3.1 DEFINISI DALAM PENGAMANAN SISTEM INFORMASI KPU

3.1.1 Pengguna

Dalam pengamanan SI KPU, pengguna tiap aplikasi dibataskan, yaitu hanya personel-personel tertentu yang dapat mengakses aplikasi tersebut. Penentuan personel-personel dilakukan berdasarkan fungsi dari tiap aplikasi. Dari sini maka dapat ditentukan juga jumlah pengguna aplikasi-aplikasi dalam SI KPU.

3.1.2 Sistem

Pengamanan sistem dikategorikan menjadi:

1. Security Level, yaitu pengamanan sistem secara fisik dan non-fisik.
Tingkatan Security Level sistem yang digunakan adalah:
 - i. High, yaitu pengamanan secara fisik dan logik
 - ii. Medium, yaitu pengamanan secara logik saja, contohnya dengan logging
 - iii. Low, yaitu tanpa pengamanan
2. Availability, yaitu jumlah waktu minimal dimana sistem harus bekerja dengan baik
 - i. High, sistem harus selalu up
 - ii. Medium, sistem harus selalu up, maksimal waktu down 1 jam
 - iii. Low, sistem tidak harus selalu up, maksimal waktu down 24 jam
3. Pengamanan dengan teknologi tambahan, seperti firewall, audit trail, sesuai dengan pembahasan di bab 2.4.

3.1.3 Aplikasi

Pengamanan aplikasi adalah pengamanan yang harus diikutsertakan dalam design tiap aplikasi agar aspek-aspek keamanan, seperti integrity data (lihat bab 2.2), dapat terjaga dengan baik.

Kategori sifat data yang dipergunakan adalah:

1. Public, masyarakat umum di luar KPU juga dapat mengakses data
2. Internal, data hanya untuk lingkungan KPU
3. Confidential, data tersedia hanya untuk sekelompok orang tertentu
4. Restricted, data hanya dapat diakses oleh beberapa orang saja (1-4)

Data-data yang terdapat dalam aplikasi SI KPU diamankan dengan menyediakan backup dan mendefinisikan sifat dari data tersebut berdasarkan pengguna dari tiap aplikasi.

Masing-masing kebutuhan backup data-data tiap aplikasi disesuaikan dengan tingkat urgensi. Tipe-tipe backup:

1. Tiap hari (akhir hari)
2. Tiap Minggu
3. Tiap Bulan
4. Full Backup, incremental backup

3.1.4 Contingency Planning

Dalam suatu Sistem Informasi, harus ada pengamanan dalam bentuk prosedur pengembalian sistem apabila terjadi suatu bencana besar, seperti kebakaran atau listrik mati. Khususnya, Sistem Informasi KPU bersifat sangat genting karena pengoperasiannya menyangkut stabilitas negara. Maka dari itu, harus dipersiapkan suatu contingency planning, dimana data-data dalam aplikasi harus tetap terjaga integritasnya bila terjadi suatu musibah besar yang dapat menyebabkan matinya sistem dan hilangnya data.

Dalam contingency planning, pengamanan dapat dilakukan dalam berbagai aspek:

1. Aplikasi, yang berupa backup aplikasi, backup data, redundant storage
2. Sistem, yang dapat berupa software untuk bantu disaster recovery, emergency power
3. Service, yang dapat berupa backup site atau offsite resources
4. Network, yang dapat berupa redundant server, redundant link (alternate path), emergency power, offsite resources

Maka dari itu, harus diinventarisir sistem mana yang perlu redundant, perlu emergency power karena harus selalu on, dan juga sistem mana yang tidak perlu suatu prosedur yang rumit.

Untuk itu, kategori-kategori yang dipakai dalam rancangan Sistem Informasi KPU adalah sebagai berikut:

1. High, yaitu sistem harus tersedia contingency planning di segala aspek berupa redundant server, redundant storage dan redundant link (network). Aplikasi-aplikasi yang termasuk dalam level contingency ini harus selalu up maka juga harus tersedia emergency power.
2. Medium, sama seperti high tetapi cukup dengan hanya tersedianya emergency power sewaktu-waktu saja.
3. Low, yaitu tidak perlu redundant server, redundant storage atau redundant link. Emergency power hanya cukup untuk shut down agar sistem dapat dimatikan secara lancar.

3.2 SISTEM INFORMASI MONITORING PEMILU

Sistem Informasi Monitoring terdiri dari:

1. Sistem Informasi Monitoring Pemilu:
 - a. Sistem Monitoring Kegiatan Pendataan
 - b. Sistem Monitoring Kegiatan Persiapan Pemilu

- c. Sistem Monitoring Kegiatan Pelaksanaan Pemilu
- d. Sistem Monitoring Kegiatan Penghitungan Suara
- 2. Sistem Informasi Monitoring Administrasi:
 - a. Sistem Informasi Monitoring Keuangan
 - b. Sistem Informasi Monitoring Perlengkapan
 - c. Sistem Informasi Monitoring Kepegawaian

Untuk setiap Sistem Informasi Monitoring, spesifikasi pengamanan tiap aplikasi monitoring adalah sebagai berikut:

3.2.1 Pengguna

Sistem Informasi Monitoring Pemilu merupakan aplikasi-aplikasi yang tersedia bagi anggota KPU, Sekum dan Wasekum untuk mendapatkan informasi mengenai kegiatan pemilu. Pengguna sistem ini hanya dapat melihat informasi dan tidak dapat merubah apapun (read only).

3.2.2 Sistem

1. Security Level System adalah Medium, karena aplikasi-aplikasi tersebut hanya menyediakan informasi bagi pengguna-penggunanya.
2. Availability: Low/High. Sifat dari aplikasi-aplikasi tersebut untuk memonitor kegiatan pemilu dan hanya menyediakan laporan-laporan dalam periode yang telah ditentukan, maka availability cukup low sebelum periode penyelenggaraan pemilu dan high pada saat periode tersebut.
3. Tidak perlu adanya tambahan teknologi seperti audit trail karena aplikasi-aplikasi ini tidak menyimpan data.

3.2.3 Aplikasi

Data-data bersifat internal dan tidak perlu di backup karena data-data hanya dapat dilihat dan tidak dirubah, juga dalam aplikasi-aplikasi ini data diambil dari suatu database dalam aplikasi lain.

3.2.4 Contingency Planning

Sifat dari informasi yang terdapat dalam aplikasi-aplikasi ini, memerlukan adanya suatu contingency planning dengan level high. Yaitu suatu rencana untuk menyediakan adanya redundant server, storage dan link, juga suatu emergency power khususnya pada masa periode penyelenggaraan Pemilu dimana availability aplikasi harus High.

3.3 SISTEM INFORMASI OPERASIONAL

Pengaman Sistem Informasi Operasional KPU tergantung daripada fungsi aplikasi yang dipakai. Sistem Informasi Operasional KPU terdiri dari:

1. SIOGARA
2. SIDUKLIH
3. SIPARPOL
4. SIPERLU

5. SITUNG
6. SITAPLIH
7. SIMALU
8. SIPANTAS
9. SIPORSILU

Berikut ini adalah rincian dari spesifikasi pengamanan yang harus diimplementasi di setiap aplikasi. Pengamanan-pengamanan ini dilakukan khususnya pada saat aplikasi dipergunakan.

3.3.1 SIOGARA (Sistem Informasi Organisasi Penyelenggara)

3.3.1.1 Pengguna

Sistem ini akan dipergunakan oleh Biro Perencanaan, Biro Perlengkapan, Biro Perhubungan, Biro Humas, Biro Hukum, Biro Lahtadalin, Biro Keuangan dan Biro Pengamanan. Untuk itu diperlukan adanya User ID Password, dimana hanya staff Biro-biro tersebut yang boleh mengakses aplikasi ini. Jumlah pengguna adalah jumlah staff dalam Biro-biro tersebut.

3.3.1.2 Sistem

1. Security Level: Medium. Secara fisik komputer yang terdapat aplikasi ini tidak perlu diletakkan dalam ruangan tersendiri. Tetapi, akan ada suatu access control, dimana hanya staff yang mempunyai user ID password yang dapat menggunakan aplikasi ini.
2. Availability: Low.
3. Teknologi tambahan: logging system. Adanya batasan dalam pengguna sistem ini memerlukan suatu logging sistem.

3.3.1.3 Aplikasi

Harus ada integrity data, dimana diajaga agar data tidak ada kekeliruan data dalam aplikasi ini. Data-data SIOGARA termasuk dalam kategori Confidential. Ini berarti, data-data tersebut hanya dapat diakses oleh biro-biro yang bersangkutan dan tidak oleh biro-biro lain atau anggota KPU di luar Biro. Backup data harus dilakukan setiap hari.

3.3.1.4 Contingency Planning

Untuk aplikasi ini, cukup dengan level medium karena sifat data dalam aplikasi ini penting dalam penyelenggaraan pemilu.

3.3.2 SIDUKLIH (sistem Informasi Penduduk dan Pemilih)

3.3.2.1 Pengguna

Sistem ini digunakan oleh Biro Perencanaan, Biro Humas dan Biro Lahtadalin. Untuk itu diperlukan adanya User ID Password, dimana hanya staff Biro-biro tersebut yang boleh mengakses aplikasi ini. Jumlah pengguna adalah jumlah staff dalam Biro-biro tersebut.

3.3.2.2 Sistem

1. Security Level: High. Keutuhan data yang akurat harus terjaga, maka pengamanan fisik dan non-fisik dari sistem ini harus terjaga.
2. Availability: Medium.
3. Perlu adanya audit trail dan logging system.

3.3.2.3 Aplikasi

Integritas data harus terjaga, maka perlu adanya enkripsi data dalam aplikasi ini. Pada akhirnya data dalam SIDUKLIH bersifar public. Karena pentingnya data-data dalam aplikasi ini, backup data harus dilakukan setiap hari.

Untuk modul yang menetapkan jumlah kursi, harus ada tambahan access control, karena hanya pengguna tertentu yang boleh mengakses modul ini.

3.3.2.4 Contingency PLanning

Sifat dari data-data dalam aplikasi ini sangat penting dan harus dijaga, maka level yang harus dipakai dalam contingency planning aplikasi ini adalah dengan level Medium. Availability aplikasi dengan level medium ini tidak perlu disediakan adanya emergency power setiap saat, cukup dalam sewaktu-waktu saja, khususnya pada saat pemilu diselenggarakan.

3.3.3 SIPARPOL (Sistem Informasi Partai Politik)

3.3.3.1 Pengguna

Pengguna sistem ini adalah Biro Perencanaan, Biro Humas, Biro Hukum, Biro Lahtadalin dan Biro Pengamanan. Untuk itu diperlukan adanya User ID Password, dimana hanya staff Biro-biro tersebut yang boleh mengakses aplikasi ini. Jumlah pengguna adalah jumlah staff dalam Biro-biro tersebut.

3.3.3.2 Sistem

1. Security Level: High. Keutuhan data yang akurat harus terjaga, maka pengamanan fisik dan non-fisik dari sistem ini harus terjaga.
2. Availability: Medium.
3. Perlu adanya audit trail dan logging system.

3.3.3.3 Aplikasi

Integritas data harus terjaga, maka perlu adanya enkripsi data dalam aplikasi ini. Sama seperti SIDUKLIH pada akhirnya data dalam SIPARPOL bersifar public. Karena pentingnya data-data dalam aplikasi ini, backup data harus dilakukan setiap hari.

Untuk modul yang melakukan evaluasi data calon, harus ada tambahan enkripsi dan access control. Sifat data-data dalam modul ini confidential karena itu hanya pengguna tertentu yang boleh mengakses modul ini.

3.3.3.4 Contingency Planning

Sama seperti SIDUKLIH, aplikasi ini dapat diamankan dengan Contingency level medium.

3.3.4 SIPERLU (Sistem Informasi Perlengkapan Dan Logistik Pemilu)

3.3.4.1 Pengguna

Pengguna sistem ini adalah Biro Perencanaan, Biro Pengawasan, Biro Perlengkapan, Biro Perhubungan, Biro Humas, Biro Lahtadalin, Biro Keuangan dan Biro Pengamanan. Untuk itu diperlukan adanya User ID Password, dimana hanya staff Biro-biro tersebut yang boleh mengakses aplikasi ini. Jumlah pengguna adalah jumlah staff dalam Biro-biro tersebut.

3.3.4.2 Sistem

1. Security Level: High. Keutuhan data yang akurat harus terjaga, maka pengamanan fisik dan non-fisik dari sistem ini harus terjaga.
2. Availability: Medium.
3. Perlu adanya audit trail dan logging system.

3.3.4.3 Aplikasi

Backup data dalam aplikasi ini dapat dilakukan secara minimal setiap minggu. Sifat data confidential untuk Biro Perencanaan, Biro Perlengkapan dan Biro Perhubungan. Integritas data dapat dijaga dengan menggunakan enkripsi.

3.3.4.4 Contingency Planning

Level dari contingency planning aplikasi ini cukup dengan level medium.

3.3.5 SITUNG (Sistem Informasi Penghitungan Suara)

3.3.5.1 Pengguna

Jumlah pengguna aplikasi ini sangat tinggi karena sifat data hasil penghitungan suara yang tinggi. Biro-biro yang dapat mengakses aplikasi ini adalah Biro Perencanaan, Biro Humas dan Biro Lahtadalin.

3.3.5.2 Sistem

1. Security Level: High. Keutuhan data yang akurat harus terjaga, maka pengamanan fisik dan non-fisik dari sistem ini harus terjaga.
2. Availability: High, terutama pada saat pemilu berlangsung
3. Perlu adanya proteksi terhadap serangan dari luar berupa firewall dan intrusion detection device.

3.3.5.3 Aplikasi

Harus ada klasifikasi data, pada akhirnya data bersifat publik, tapi sebelum dapat dilihat publik harus diverifikasi terlebih dahulu untuk mencegah adanya pemalsuan atau kesalahan dalam data penghitungan suara. Dalam proses verifikasi ini, data masih bersifat internal tetapi partai politik boleh lihat. Setelah proses verifikasi selesai, maka batch data dapat diumumkan ke public. Backup data harus dilakukan minimal satu hari sekali.

Tambahan fungsi dalam aplikasi ini yang harus dipertimbangkan adalah adanya suatu kemampuan agar pihak atas (eksekutif) bisa mengganti data apabila ada koreksi yang harus dilakukan. Tetapi harus diingan adanya konsekuensi-konsekuensi bila fungsi ini tersedia, seperti perlu adanya tambahan pengamanan dan juga perlu pertimbangan mengenai siapa yang boleh mengganti data penghitungan suara tersebut.

3.3.5.4 Contingency Planning

Aplikasi ini adalah aplikasi yang sangat penting pada saat pemilu dilaksanakan. Maka dari itu, contingency planning untuk SITUNG harus dengan level High.

3.3.6 SITAPLIH (Sistem Informasi Penetapan Terpilih)

3.3.6.1 Pengguna

Aplikasi ini digunakan oleh Biro Perencanaan, Biro Humas, Biro Hukum dan Biro Lahtadalin.

3.3.6.2 Sistem

1. Security Level: High. Keutuhan data yang akurat harus terjaga, maka pengamanan fisik dan non-fisik dari sistem ini harus terjaga.
2. Availability: Medium.
3. Perlu adanya audit trail dan logging system.

3.3.6.3 Aplikasi

Pada mulanya data bersifat confidential sampai seluruh proses penentuan terpilih. Sesudah proses tersebut selesai, maka hasil penetapan terpilih akan menjadi public.

3.3.6.4 Contingency Planning

Setelah penghitungan suara selesai dilakukan maka peneteapan terpilih adalah aktifitas yang penting. Level contingency planning yang cocok bagi aplikasi ini adalah High setelah pemilu berakhir.

3.3.7 SIMALU (Sistem Informasi Manajemen Pemilu)

3.3.7.1 Pengguna

Pengguna sistem ini adalah Biro Perencanaan, Biro Pengawasan, Biro Perlengkapan, Biro Perhubungan, Biro Humas, Biro Lahtadalin, Biro Keuangan dan Biro Pengamanan. Untuk itu diperlukan adanya User ID Password, dimana hanya staff Biro-biro tersebut yang boleh mengakses aplikasi ini. Jumlah pengguna adalah jumlah staff dalam Biro-biro tersebut.

3.3.7.2 Sistem

1. Security Level: Low.
2. Availability: Low
3. Perlu adanya access control menggunakan logging system.

3.3.7.3 Aplikasi

Data-data bersifat internal, hanya biro-biro yang bersangkutan yang dapat mengakses aplikasi ini. Backup data harus dilakukan setiap minggu.

3.3.8.4 Contingency Planning

Sifat dari data-data dalam aplikasi ini penting dalam penyelenggaraan pemilu, maka contingency planning yang harus digunakan adalah level medium.

3.3.8 SIPANTAS (Sistem Informasi Pemantauan Pemungutan Suara)

3.3.8.1 Pengguna

Pengguna sistem ini adalah Biro Perencanaan, Biro Perlengkapan, Biro Perhubungan, Biro Humas, Biro Lahtadalin dan Biro Pengamanan. Biro-biro tersebut adalah yang berhak menangani masalah-masalah yang timbul dalam proses pemilu. Namun, idealnya sistem ini dapat dilakukan online agar publik juga bisa mengakses aplikasi ini untuk melaporkan kejadian-kejadian aneh yang mungkin terjadi selama pemilu berlangsung.

3.3.8.2 Sistem

1. Security Level: Low.
2. Availability: Medium
3. Perlu adanya access control menggunakan logging system bagi biro-biro yang bertugas menangani masalah-masalah pemilu.

3.3.8.3 Aplikasi

Data-data yang di-input oleh pengguna bersifat internal. Maka perlu adanya pengamanan dalam proses pemasukan data tersebut.

3.3.8.4 Contingency Planning

Contingency planning aplikasi ini harus dalam level high, khususnya pada saat penyelenggaraan pemilu.

3.3.9 SIPORSILU (Sistem Pelaporan Hasil Pemilu)

3.3.9.1 Pengguna

Biro-biro yang menggunakan aplikasi ini adalah Biro Perencanaan, Biro Pengawasan, Biro Perlengkapan, Biro Perhubungan, Biro Humas, Biro Lahtadalin, Biro Keuangan dan Biro Pengaman.

3.3.9.2 Sistem

1. Security Level: Low.
2. Availability: Low, tetapi bila tiba saatnya laporan-laporan harus dikumpulkan, availability aplikasi ini harus High.
3. Tidak diperlukan adanya teknologi tambahan

3.3.9.3 Aplikasi

Data-data dalam aplikasi ini bersifat internal. Backup data cukup dilakukan satu minggu sekali.

3.3.9.4 Contingency Planning

Contingency planning aplikasi ini cukup dengan medium.

3.4 SISTEM INFORMASI ADMINISTRASI

Dalam pelaksanaan Pemilu, Sistem Informasi Administrasi terdiri dari:

1. SIPEG
2. SIPER
3. SIKEU
4. SIHUKUM
5. Web Based IS

3.4.1 SIPEG (Sistem Informasi Kepegawaian)

3.4.1.1 Pengguna

Sistem ini digunakan oleh Biro Pengawasan dan Biro Umum.

3.4.1.2 Sistem

1. Security Level: High, pengguna sistem ini terbatas, maka perlu adanya suatu access control dan keamanan fisik dari sistem ini harus juga terjaga.

2. Availability: Low,
3. Perlu adanya enkripsi untuk mengamankan informasi di dalam aplikasi ini.

3.4.1.3 Aplikasi

Aplikasi ini mengandung informasi yang bersifat confidential, hanya kedua biro yang bersangkutan yang boleh mengakses informasi tersebut.

3.4.1.4 Contingency Plannning

Karena data-data dalam aplikasi ini sangat penting tetapi tingkat urgensi dari data rendah, maka coniingency planning cukup dengan level medium.

3.4.2 SIPER (Sistim Informasi Perlengkapan)

3.4.2.1 Pengguna

Sistem ini digunakan oleh seluruh Biro dalam KPU.

3.4.2.2 Sistem

1. Security Level: Low.
2. Availability: Medium
3. Tidak diperlukan teknologi tambahan.

3.4.2.3 Aplikasi

Aplikasi ini mengandung data-data yang bersifat internal.

3.4.2.4 Contingency Planning

Aplikasi ini sangat penting pada penyelenggaraan pemilu, maka contingency planning harus dengan level medium.

3.4.3 SIKEU (Sistem Informasi Keuangan)

3.4.3.1 Pengguna

Sistem ini digunakan oleh seluruh Biro dalam KPU kecuali biro Hukum dan Biro Pengamanan.

3.4.3.2 Sistem

1. Security Level: High, karena informasi dalam sistem ini harus diamankan dari pihak-pihak yang tidak boleh merubah informasi-informasi tersebut.
2. Availability: Medium, karena masalah keuangan adalah masalah yang sensitif
3. Tidak diperlukan teknologi tambahan.

3.4.3.3 Aplikasi

Aplikasi ini mengandung data-data yang bersifat internal.

3.4.3.4 Contingency Planning

Sifat data-data dalam SIKEU sangat penting dalam menjaga kesuksesan penyelenggaraan pemilu. Maka level contingency planning aplikasi ini harus dalam level high.

3.4.4 SIHUKUM (Sistem Informasi Hukum)

3.4.4.1 Pengguna

Sistem ini digunakan oleh seluruh Biro dalam KPU.

3.4.4.2 Sistem

1. Security Level: Low.
2. Availability: Medium
3. Tidak diperlukan teknologi tambahan.

3.4.4.3 Aplikasi

Aplikasi ini mengandung data-data yang bersifat internal.

3.4.4.4 Contingency Planning

Level contingency planning aplikasi ini cukup dengan level medium.

3.4.5 Web Based IS

3.4.5.1 Pengguna

Sistem ini digunakan oleh seluruh anggota KPU dan juga oleh masyarakat di luar KPU.

3.4.5.2 Sistem

1. Security Level: Low.
2. Availability: Low/High. Pada saat pelaksanaan pemilu informasi mengenai jumlah suara harus tersedia setiap saat, maka pada saat ini availability Web Based IS harus High. Tetapi sebelum periode itu availability cukup dengan low.
3. Tidak diperlukan teknologi tambahan.

3.4.5.3 Aplikasi

Aplikasi ini mengandung data-data yang bersifat publik.

3.4.5.4 Contingency Planning

Web Based IS cukup diamankan dengan contingency planning level medium.

3.5 SISTEM INFORMASI PERKANTORAN

Sistem Informasi Perkantoran KPU terdiri dari:

1. E-mail system
2. SIAR (Sistem Informasi Kearsipan)
3. Group/collaborative works system
4. Bulletin board

Spesifikasi pengaman sistem-sistem tersebut adalah sebagai berikut.

3.5.1 Pengguna

Pengguna sistem-sistem tersebut adalah seluruh anggota KPU dalam pelaksanaan penyelenggaraan Pemilu.

3.5.2 Sistem

1. Security Level: Low.
2. Availability: Medium. Karena sistem-sistem tersebut diperlukan dalam segala masalah perkantoran, termasuk dalam berkomunikasi, maka availability harus dijaga dengan baik.
3. Tidak diperlukan teknologi tambahan.

3.5.3 Aplikasi

Data-data dalam sistem-sistem tersebut bersifat internal.

3.5.4 Contingency Planning

Untuk semua Sistem Informasi Perkantoran contingency planning dengan level medium.

4 SDM SECURITY

Ada banyak permasalahan seputar aspek keamanan. Sumber daya manusia (SDM) merupakan komponen utama dari aspek keamanan karena pengguna sistem informasi adalah manusia. Sayang sekali aspek keamanan seringkali tidak menjadi perhatian dari manusia pengguna sistem informasi.

"Computers do not committ computer crime. People do. An effective seurity system must begin with the human problem".

*"You can't lock the gates yourself so you have to train more gatekeepers".
(Richard W. Baker, "Network Security")*

Ada dua sisi dari SDM, yaitu pengguna dan pengelola sistem informasi. Kedua sisi SDM sini harus menyadari akan masalah keamanan. Pengguna harus sadar akan masalah keamanan (memiliki *security awareness*). Sebagai contoh pengguna tidak boleh memberikan password akses ke sistem ke orang lain. Atau pengguna harus mengamankan komputer / workstation miliknya dari serangan virus dengan memasang anti virus terbaru. Seringkali pengguna merupakan aspek terlemah dari sistem keamanan. Sisi SDM pengelola sistem informasi seringkali mengalami permasalahan karena kurangnya SDM yang paham akan masalah keamanan.

Untuk itu harus ada satu departemen yang khusus bertanggung jawab dalam segala masalah IS. Khususnya harus ada satu orang Chief Security officer yang bertanggung jawab atas data-data, jaringan and internet.

Job description dari Chief Security Officer:

1. Bertanggung jawab atas masalah keamanan baik dalam aspek logis maupun data atau informasi di KPU
2. Merancang dan melakukan program-program untuk security training, seperti membuat slogan-slogan atau video yang mendidik tentang isu-isu keamanan
3. Membuat peraturan-peraturan (policy), seperti pengguna tidak boleh membawa disket bila masuk ke dalam ruangan komputer yang terdapat aplikasi-aplikasi penting, bila pengguna membutuhkan software harus melalui departemen IT, dst.

4.1 USULAN PROGRAM KERJA SDM

4.1.1 Security Awareness

Security awareness tidak dapat tumbuh dengan begitu saja. Dia harus diprogramkan secara aktif. Untuk itu perlu adanya program untuk memberikan wawasan (awareness) tentang masalah keamanan kepada seluruh pengguna dan pengelola sistem informasi KPU. Terlebih kepada pengelola sistem informasi KPU, masalah security harus dimengerti. Program security awareness dapat dilakukan dengan mengikuti pelatihan atau training.

Banyak hal yang dapat diberikan pada pelatihan ini, seperti misalnya bagaimana menggunakan dan memilih password, bahwa pengguna bertanggung jawab atas account dan passwordnya, bahwa pengguna harus logoff dari terminal atau workstation agar tidak digunakan oleh orang lain, bahwa pengguna mengerti kebijakan dari tempat dimana dia bekerja.

4.1.2 Security audit dan maintenance secara berkala

Sebagaimana telah dikemukakan di beberapa bagian dari buku ini, tingkat keamanan harus dievaluasi secara berkala. Evaluasi atau audit ini sebaiknya dilakukan oleh pihak ketiga (bukan oleh KPU) untuk menjaga objektivitas.

4.1.3 Pembuatan policy dan procedures

Pembuatan policy dan procedures bukanlah pekerjaan yang mudah. Untuk itu perlu dibuat sebuah kegiatan khusus untuk membuat (develop) policy and procedures, seperti misalnya AUP (Acceptable Uses Policy). Termasuk didalam kegiatan ini adalah pembuatan mekanisme *incident handling* dan kelompok (siapa-siapa) yang bertanggungjawab terhadap masalah keamanan.

5 Contingency Sistem Operasi KPU

Terdapat beberapa aspek pengamanan dari contingency planning Sistem Informasi KPU yang berada di luar scope dari project ini dan disarankan untuk diadakannya penyelidikan lebih lanjut. Penyelidikan-penyelidikan tersebut diperlukan guna merancang contingency planning yang cocok dengan Sistem Informasi yang dirancang dan memperkirakan dana yang diperlukan untuk contingency planning Sistem Informasi KPU tersebut.

Berikut ini adalah perincian dari usulan kerja yang harus dilakukan dalam contingency planning Sistem Informasi KPU

5.1 USULAN KERJA CONTINGENCY PLANNING

5.1.1 Definisi Sistem Contingency

Harus ada suatu pendefinisian dari komponen-komponen sistem, seperti definisi Hardware, kapan hardware tersebut on dan dalam situasi apa, definisi Line, kapan line tersebut on dan dalam situasi apa, dan seterusnya.

5.1.2 Contingency Sites

Dalam pengamanan sistem terhadap kejadian-kejadian darurat harus tersedia juga lokasi alternatif bila lokasi utama terganggu, seperti kebakaran atau listrik padam. Dalam Sistem Informasi KPU, lokasi alternatif yang tersedia harus minimal tiga lokasi yang berbeda. Tiga lokasi ini diperlukan karena stabilitas negara berada dalam bahaya apabila lokasi utama Sistem Informasi KPU terganggu.

Kriteria dari tiga lokasi contingency sites ini adalah sebagai berikut:

1. Sistem lengkap harus tersedia di kota luar Jakarta yang tersedia secara umum
2. Di Jakarta, sebagai kota pusat sistem ini, juga harus tersedia lokasi alternatif selain lokasi pusat KPU. Khususnya lokasi ini bisa diberikan kepada pihak swasta jadi bersifat private dan dapat terjaga keamanannya.
3. Tambahan lokasi di Jakarta yang berbeda dengan lokasi yang disebutkan di nomer sebelumnya.

5.1.3 Struktur Manajemen Sistem IT Contingency

Dalam pengamanan sistem, harus ada suatu unit yang bertanggungjawab dalam menangani insiden-insiden yang membahayakan. KPU harus mendefinisikan unit manajemen Sistem IT ini karena tergantung pada organisasi KPU. Untuk itu, harus ditentukan apakah manajemen sistem IT ini diserahkan pada keamanan atau pada grup IT.

STRUKTUR ORGANISASI SISTEM IT CONTINGENCY JUGA HARUS JELAS, SEPERTI UNTUK JABATAN DIREKTUR APA TANGGUNG JAWABNYA DAN SKILL SET YANG HARUS DIMILIKINYA.

5.1.4 Guide Disaster Planning

Untuk mengantisipasi bencana-bencana yang dapat sewaktu-waktu terjadi, perlu disusun suatu dokumen panduan. Dokumen tersebut adalah suatu pedoman dalam pengoperasian Sistem Informasi apabila terjadi suatu situasi darurat.

5.1.5 Evaluasi Inventory

Perlu diadakan suatu evaluasi inventaris dimana logistik dari sistem ini terjaga. Juga diperlukan program-program apabila terjadi sesuatu terhadap perlengkapan dari sistem ini. Contohnya, apabila hard disk hilang harus ditentukan berapa lama yang dibutuhkan agar bisa dikembalikan.

5.1.6 Arsitektur Sistem Contingency

Dalam penentuan arsitektur Sistem Contingency, KPU harus tetap mengikuti perkembangan teknologi. Arsitektur ini tergantung daripada kebutuhan dan sistem yang digunakan oleh KPU, seperti dana yang tersedia untuk rancangan sistem Contingency ini. Termasuk dalam arsitektur ini juga adalah penentuan waktu kapan sistem harus dipindahkan ke lokasi dua atau lokasi tiga, dan siapa yang bertanggungjawab untuk mengambil aba-aba untuk pindah.