14 KEAMANAN

14.1 PERSYRATAAN UMUM

14.1.1 TUJUAN

Untuk mengetahui persyaratan atau keperluan untuk keamanan di departemen operasi dan untuk terminal dan peralatan komunikasi yang ditempatkan di luar departemen tersebut.

14.1.2 CAKUPAN

Bagian ini mendeskripsikan secara umum faktor-faktor yang perlu dipertimbangkan pada waktu menyusun atau membangun sistem keamanan untuk departemen operasi.

Dua aspek pokok keamanan yang perlu ditangani adalah:

— Proteksi atau perlindungan investasi perusahaan yang berupa peralatan, sistem, data, dan staf dari kerusakan, kehilangan atau kerusakan yang diakibatkan oleh kecelakaan atau desain.

Area-area tertentu akan dibahas secara lebih rinci dalam:

— Keamanan Fisik (14.2);

— Keamanan Data (14.3);

— Kemanan Sistem (14.4).

Ketrangan lebih lanjut mengenai semua aspek keamanan diberikan dalam terbitan NCC yang berjudul *Management Handbook of Computer Security.*

14.1.3 TANGGUNG JAWAB

Manajer Operasi akhirnya akan bertanggung jawab atas keamanan secara keseluruhan di departemennya. Rincian pengimple mentasian dan pemeliharaan sistem keamanan bisa didelegasikan, dan spesifikasi pekerjaan harus menentukan tugas-tugas, tanggung jawab, dan kewenangan secara jelas.

Keamanan harus merupakan aktivitas yang terorganisir, bukan suatu hobi. Oleh karena itu:

— Perencanaan keamanan harus dimulai bersama-sama dengan instalasi dan/atau desain sistem, tidak boleh ditambahkan (dipasang) kemudian;

— Kita harus minta saran kepada para spesialis (layanan pemadam kebakaran, perusahaan asuransi);

— Kesadaran atau pengetahuan akan keamanan harus ditanamkan kepada semua anggota staf dengan cara mengadakan pelatihan dan dengan melakukan pengecekan terhadap mereka secara random untuk mengetahui pengetahuan mereka tentang semua prosedur keamanan.

14.1.4 PRINSIP-PRINSIP KEAMANAN

1. Besarnya Keamanan

Keamanan yang sempurna tidak pernah mungkin. Karena beberapa alasan, keamanan yang berlebihan tidak layak, sebab:

— Biayannya akan begitu mahal;
— Pemrosesan akan menjadi lambat;
— Tidak akan sebanding dengan hasil produksi.

2. Tujuan

Oleh karena itu, tujuan keamanan adalah untuk mencapai keseimbangan yang wajar antara resiko dan biaya.

Pencegahan tidak bisa berjalan sendiri - sebaiknya kita tidak hanya menurunkan probabilitas kejadian (yang merusak keamanan) namun juga harus meminimisasi dampak-dampaknya sampai ke tingkat yang bisa diterima.

Keamanan harus ditujukan/dimaksudkan untuk:

— Pencegahan;
— Pendeteksian;
— Penekanan
— Pemulihan.

3. Langkah-langkah

Kita perlu:

— Menentukan area-area yang perlu perlindungan dengan cara memeriksa atau menyelidiki probabilitas dan konsekuensi dari kejadian tertentu (14.1.5);
— Mengatur atau menyusun tingkatan keamanan yang tepat, dan memastikan bahwa semua aktivitas departemen memenuhi persyaratan;
— Menyusun prosedur pemulihan yang efektif dan rinci.

Bahaya atau bencana	Gangguan pada pemrosesan	Kerusakan fisik	Kerusakan sistem	Kerugian atau kerusakan total
Kebakaran	2	1	1	1
Banjir	2	1	1	
Layanan:				
Kegagalan atau kerusakan AC	3	1	1	
Kegagalan power	3	1	1	
Fluktuasi power	1	1	1	
Kegagalan mesin	3		1	
Kesalahan:				
Pengoperasian		2	1	1
Data	1		1	
Sistem	2		2	
Sabotase	2	2	1	1
Pencurian	1	1	1	
Perusakan	2		1	
Bom	3			
Ledakan	3	2	1	1

Gambar 14.1 Dampak dari berbagai bencana pada sistem: contoh

4. Cakupan

Keamanan harus mencakup:

— Hardware, yang mahal harganya dan berbiaya mahal untuk menggantinya;

— Data, yang apabila hilang atau rusak, ia tidak akan dapat digunakan;

— Sistem, untuk memastikan bahwa ia tidak mempunyai peluang kena kerusakan atau bencana;

— Orang-orang, untuk memenuhi keamanan bagi mereka dan dari mereka.

Sistem keamanan harus didistribusikan secara merata ke semua aspek tersebut. Kuatnya rantai merupakan kuatnya hubungan terlemahnya.

Kita harus melakukan pertimbangan khusus untuk mencegah penyalahgunaan sistem selama ia digunakan untuk cadangan atau selagi ia diperbaiki.

14.1.5 DAMPAK KEJADIAN

Kita harus mendaftar bahaya-bahaya potensial yang mungkin terjadi dan juga dampak dari kejadiannya. Isi daftar tersebut akan bervariasi menurut kondisi lokal masing-masing, namun pada dasarnya sama seperti Gambar 14.1.

Dampak-dampaknya diklasifikasikan menurut sifatnya:

1. Mungkin
2. Bisa terjadi
3. Pasti

14.2 KEAMANAN FISIK

14.2.1 TUJUAN

Untuk mendeskripsikan keperluan keamanan atau perlindungan dari bahaya fisik dalam departemen operasi.

14.2.1 CAKUPAN

Bagian ini membahas bahaya-bahaya utama dan yang lebih potensial, dan memberikan pedoman tentang ukuran untuk mencegah, mendeteksi, menekan, dan memulihkan diri bila kena bahaya itu, dan memberikan pedoman tentang asuransi yang fungsinya untuk meminimisasi dampak finansial.

14.2.3 FAKTOR KEAMANAN

Komputer:

— Bernilai tinggi dan berbiaya besar. Keamanan sangat penting untuk melindungi investasi perusahaan;

— Berperan banyak dalam aktivitas harian perusahaan. Keamanan diperlukan untuk memelihara layanan;

— Seringkali digunakan pada sore hari, malam hari atau akhir pekan, dimana pada waktu ini kondisi keamanan bervariasi dan sulit dijaga;

— Menarik perhatian banyak pengunjung yang datang untuk mengantarkan input, mengumpulkan output, memelihara peralatan, atau mereka yang sekedar melihat. Aksesnya harus dikontrol;

— Kadang-kadang tidak populer, atau tidak bisa diandalkan, dan dapat menjadi target pengrusakan oleh orang yang tak puas atau tidak senang, yang menyadari peran pentingnya alat itu dalam organisasi.

14.2.4 KEBAKARAN

1. Pencegahan

Kebakaran merupakan bencana paling merusak dalam departemen operasi. Tindakan pencegahan yang harus diambil mencakup:

— Lokasi ruang komputer harus berjauhan dari area-area yang beresiko, misalnya ruang boiler, kantin, atau area yang berfasilitas peralatan pemasak makanan;

— Konstruksinya harus dari bahan antu api atau tahan api, atau setidaknya dilapisi dan bahan anti api;

— Furniture dan perlengkapannya dari logam;

— Pintunya yang dari bahan anti api bisa menutup sendiri bila terkena semburan api;

— Berkonsultasi dengan biro pemadam kebakaran lokal untuk meminta bantuan dan saran pada waktu tahap desain;

— Diberlakuka larangan meroko, makan, minum di dalam ruang komputer;

— Pada sebelah pintu masuk yang ditulisi 'Dilarang Merokok' harus dilengkapi asbak atau kotak sampah;

— Pembersihan barang-barang tidak penting yang sensitif terhadap api, seperti kartu, stasionari, scrap, kotak kosong, dari ruang komputer;

— Memastikan bahwa lanta bawah dan atap tidak mengandung bahan-bahan yang mudah tersulut, atau mengecek kondisi ini di area-area lain di atas ruang komputer;

— Memastikan bahwa hanya disk dan pita yang diperlukan untuk pekerjaan saat itu yang ada. Yang lainnya harus dikembalikan ke perpustakaan atau perpustakaan media;

— Membuat duplikat catatan-catatan yang bernilai dan yang tidak bisa diganti untuk disimpan di lokasi yang aman; ini untuk membantu pemulihan apabila benar-benar terjadi kebakaran;

— Larangan untuk menggunakan peralatan yang membahayakan, seperti kipas angin, pemanas, atau radio. (Radio dapat juga menjadi sumber interferensi frekuensi radio).

2. Pendeteksian

Peralatan deteksi harus diinstal di dalam semua ruangan, di dalam sistem AC, dan di atas langit-langit dan di bawah lantai.

Sistem tersebut harus dirancang supaya bisa:

— Membunyikan peringatan dalam instalasi atau di tempat lain;
— Menghubungkan secara langsung ke biro pemadam kebakaran;
— Mematikan sistem AC;
— Mengoperasikan sistem pemadam kebakaran.

Tiga hal pertama di atas harus bersifat otomatis. Untuk meminimisasi kerusakan yang disebabkan oleh alarm yang salah dan untuk melindungi personel, sistem pemadam kebakaran harus bisa dioperasikan secara manual oleh orang-orang tertentu selama pada jam kerja, dan harus bisa beroperasi secara otomatis ketika saat itu ruang komputer tidak orang nya. Disini harus ada indikasi yang jelas tentang apakah sistem tersebut dioperasikan secara manual ataukah dikon trol secara otomatis, dan dalam sistem ini harus ada prosedur untuk menghidupkan dan mematikannya.

3. Penekanan

Alat pemadam kebakaran yang bisa dipegang tangan cukuplah untuk area tersebut, dan ia harus ditempatkan di tempat yang strategis. Ia menjadi garis pertahanan pertama. Jika alat seperti ini tidak memadai, maka harus digunakan sistem otomatis (14.2.4.2).

Pemadam kebakaran karbondioksida dan BCF disarankan untuk digunakan oleh Komite Fire Office (Kantor Pemadam Kebakaran), meskipun alat ini mempunyai beberapa kelemahan:

— Supply-nya bersifat one-off (sekali pakai)
— Tak ada pengurangan panas apabila menggunakan BCF, oleh karenanya ada resiko flashback (balik);
— Apabila menggunakan CO2, temperaturnya akan turun, dan ini akan berdampak tidak baik bagi peralatan;
— Ada beberapa risiko terhadap personel - CO2 menghasilkan asap tebal yang menghambat pandangan. Sistem CO2 otomatis hanya boleh digunakan ketika ruangan tidak orang.

Bila kondisinya memungkinkan, pematian komputer secara terkontrol disarankan; ini untuk meminimisasi kerusakan terhadap peralatan dan untuk memudahkan pemulihan sistem dan data selanjutnya.

Blanket (selimut) pemadam api efektif untuk memadamkan nyala api, namun karena adanya resiko kontaminasi debu, maka selimut pemadam tersebut tidak boleh digunakan pada peralatan yang sensitif seperti unit tape atau disk. Ia terutama sangat berguna untuk memadamkan kebakaran di dapur tempat beradanya fasilitas masak (2.5.5.6).

4. Keselamatan

Tindakan pencegahan kebakaran harus diperagakan dalam semua area dan semua personel harus mengetahui keperluannya.

Alarm harus bisa didengar dan/atau dilihat secara jelas di seluruh instalasi, khususnya ketika peralatan tersebut sedang bekerja.

Peralatan yang bertegangan tinggi harus ditandai bahwa ia bertegangan tinggi secara jelas.

Lampu darurat harus diinstal agar bisa hidup pada waktu terjadi kegagalan power.

Pintu keluar darurat harus berjumlah cukup, harus terbuka ke luar, dan tidak boleh dikunci selama jam kerja. Pintu- pintu itu harus mudah dicapai dan ditandai secara jelas. Koridor dan lantai harus dijaga tetap bersih.

Instruksi yang jelas dan singkat bisa dikeluarkan untuk memberitahu semua staf yang perlu dihubungi dan hal-hal yang harus dikerjakan oleh mereka ketika terjadi kebakaran, yakni bagaimana:

— Mengoperasikan peralatan pemadam kebakaran;
— Menutup kokmputer dan layanan;
— Menyelamatkan informasi yang penting;
— Melakukan pertolongan pertama.

5. Pengecekan

Kita harus melakukan pengecekan secara teratur dan sering untuk memastikan bahwa:

— Jalur atau jalan darurat menuju bangunan atau gedung tidak terhalang, sehingga kendaraan pemadam kebakaran bisa masuk;
— Peralatan pendeteksi api dan asap bisa beroperasi;
— Alarm bisa bekerja atau bisa didengar atau bisa dilihat;

— Lampu darurat berfungsi;
— Silinder gasnya penuh dan penggantinya telah tersedia;
— Alat pemadam kebakaran ditempatkan pada tempat yang strategis dan dalam kondisi yang baik, dan petunjuknya bisa dibaca dengan jelas;
— Tangga, koridor keluar, dan pintu keluar darurat bebas dari halangan.

14.2.5 BANJIR

1. Pencegahan

Banjir tidak sebahaya kebakaran, dimana ia dapat dicegah dengan melakukan beberapa tindakan pencegahan sederhana dan umum:

— Ruang komputer, penyimpanan media, dan sebagainya, tidak boleh ditempatkan dalam basement (lantai bawah) jika areanya berpeluang kena banjir;
— Pipa atau saluran air tidak boleh dilewatkan di atas, di bawah, atau bersedekatan dengan ruang komputer;
— Kita harus meminta saran tentang penentuan lokasi sistem yang mengandung percikan (splinker-system) dalam kaitannya dengan peralatan elektris;
— Apabila ada potensi terjadi banjir, kita harus menginstal sistem pemompaaan yang bisa menyedot air keluar. Lantai ruang komputer, gedung, dan ruang power harus bisa dikeringkan dan atau dipompa.

2. Pemulihan

Latihan penanganan banjir harus menerapkan instruksi seperti:

— Jika peralatan terendam atau basah, ia harus dibiarkan selama tiga hari, dan kemudian kita jalankan lagi;
— Jika tape dan disk basah atau terendam selama kurang dari dua jam, mereka tidak akan rusak. Jika mereka tetap basah dalam waktu yang lama, maka mereka akan mengalami kerusakan yang serius;
— Kita harus mencari bantuan atau meminta saran dari ahli perekayasaan.

14.2.6 PENCURIAN DAN SABOTASE

1. Pencurian

Tindakan pencegahan harus dilakukan untuk menghindari pencurian:

— Peralatan - khususnya barang-barang yang kecil;
— Alat-alat;

— Bahan - misalnya, pita guntingan/sisa dan kertas tisu;
— Barang-barang kecil - misalnya, pena dan kertas;
— Software (14.4.6);
— Data rahasia/penting;
— Mesin waktu.

2. Sabotase

Kerusakan akibat kejahatan pada instalasi komputer semakin membahayakan. Pengrusakan ini bisa berupa dari operator yang tidak puas yang membuat kerusakan sampai demonstrasi yang terorganisir yang merusak bank data dan pengrusakan tanpa motivasi dengan cara kekerasan oleh teroris, bahkan dengan menggunakan bom.

3. Pencegahan

Tindakan yang bisa diambil untuk meminimisasi ancaman pencurian dan sabotase tersebut mencakup:

— Jika mungkin, komputer sebaiknya ditempatkan dalam gedung yang terpisah, dimana ia bisa lebih mudah dijaga;
— Gedung/bangunan (atau instalasi jika menempati sebagian tempat perusahaan yang biasa) harus kuat secara fisik untuk mencegah entri yang secara paksa. Jumlah pintunya kalu bisa sedikit mungkin, dan pintu-pintu itu harus tidak bisa diterobos atau diperkuat dengan jeruji. Ruang aula, lobang udara, dan balkon tempat melihat pemandangan biasanya mudah ditembus dan mereka ini memerlukan perhatian khusus;
— Akses ke ruang komputer hanya terbatas untuk personel yang berwenang. (Dalam kaitannya dengan hubungan staf, aturan ini bisa fleksibel, namun jika orang-orang yang berkunjung ke ruang komputer telah selesai, mereka harus dikontrol secara ketat pada waktu keluar - lihat 7.1.4.3). Log (buku catatan besar) dapat digunakan untuk mencatat yang masuk dan yang keluar. Kita harus memberikan akses ke ruang itu kepada pada pekerja shift, tukang kebersihan, personel pemeliharaan, dan sebagainya;
— Dalam area yang memerlukan pengamanan sangat ketat, misalnya perpustakaan, penyimpanan media, penyimpanan keamanan remote, dan ruang terminal, pintu-pintunya harus dikunci ketika ruangan-ruangan tersebut tidak dipakai. Apabila aksesnya tidak sering, kita bisa menggunakan kunci; namun untuk akses yang sering, kita lebih baik menggunakan mekanisme (untuk membuka)

yang dioperasikan kartu atau sandi/disk identitas. Daftar yang menyebutkan pemegang kunci/kartu harus disimpan, dan kunci/kartu harus diubah jika staf yang bersangkutan (yang memegang kartu itu) keluar;

— Paling tidak ada dua orang yang selalu bertugas sepanjang waktu; ini untuk meminimisasi resiko pencurian dan sabotase. Tim ini harus diubah (digonta-ganti) secara sering guna meminimisasi terjadinya kolusi (bekerja sama untuk bertindak tidak baik). Pekerja yang dipecat harus diminta pergi sesegera mungkin, bukannya dibiarkan sampai jam kerja selesai (terutama jika orang ini mempunyai akses ke peralatan dan software yang bernilai tinggi atau akses ke informasi rahasia).

— Kopi data dan software esensial harus disimpan di lokasi yang aman yang jauh dari instalasi, agar ia bisa digunakan untuk membantu pemulihan apabila terjadi insiden.

14.2.7 HILANGNYA LAYANAN

1. AC

Tindakan pencegahan terhadap pemberhentian secara total karena hilangnya layanan AC mencakup:

— Perancangan sistem sedemikian rupa sehingga apabila ada satu komponen yang rusak, maka hal ini tidak akan mengakibatkan kerusakan total;

— Pemeliharaan yang teratur;

— Memastikan bahwa gedung tidak digunakan untuk menanggulangi muatan yang aneh-aneh, misalnya dengan pembatasan entri ke area AC, dengan pintu yang bisa menutup sendiri, dan keset yang menarik debu;

— Memastikan bahwa sistem mempunyai kapasitas luang yang memadai guna memungkinkannya menanggulangi penginstalasian peralatan komputer tambahan.

2. Kegagalan (kematian) Listrik

Ini mencakup fault yang sebenarnya dan juga kelemahan layanan yang diakibatkan oleh kesulitan industrial.

Dengan menggunakan fasilitas komputer lain, para pemakai bisa menjadi tidak nyaman, dan sebaiknya kita juga menca dangkan peralatan listrik lain, misalnya:

— Generator darurat yang memberikan supply daya yang normal;
— Peralatan penggenerasi rangkap yang membuat tidak tergantung pada supply induk.

Lampu darurat harus diinstal untuk keselamatan ketika terjadi kegagalan atau kematian listrik.

Peralatan cadangan harus dipelihara dan diuji secara tera tur.

14.2.8 ASURANSI

1. Umum

Disarankan agar memakai perlindungan asuransi; ini guna memenuhi atau meminimisasi akibat finansial dari situasi darurat.

Ini mungkin merupakan polis tersendiri pada perusahaan asuransi, atau polis komputer khusus bisa digunakan. Polis ini harus mencakup peralatan, tape dan disk, dan software.

2. Peralatan

Kebakaran, banjir, kerusakan akibat kecelakaan, dan hilang nya layanan harus dibahas dalam polis asuransi itu (polis asuransi biasanya tidak membahas atau mencakup wear and tear, desain defektif, workmanship atau bahan, atau kerusa kan yang dilindungi oleh kontrak pemeliharaan pemasok).

Polis asuransi tersebut juga harus mencakup kerusakan yang berkembang yang diakibatkan oleh kegagalan fisik (kegagalan elektronik yang tidak mempunyai wujud fisik biasanya tidak disertakan).

Akibat finansial dari waktu pembelian, kegagalan dalam menghasilkan output, atau hilangnya keuntungan harus diser takan atau dibahas dalam kebijaksanaan perlindungan itu.

Ia juga harus melindungi resiko sabotase dan resiko karena hal tertentu, karena in diperlukan oleh setiap instalasi.

3. Tape dan Disk

Tape dan disk yang berisi data penting harus dilindungi (diasuransikan), yang nilainya sama dengan biaya pembelian dan pemrosesannya kembali.

Hilangnya data karena terkena distorsi magnetis biasanya tidak dilindungi oleh asuransi.

Penghapusan kecelakaan biasanya dimasukkan, namun ia dapat dilindungi (atau diasuransikan) dengan premi ekstra.

4. Software

Software dapat diasuransikan atas semua resiko. Pabrikan atau pemasok harus dimintai pendapat mengenai tanggung jawab asuransi itu.

Semua program aplikasi yang ditulis oleh staf perusahaan dapat dianggap sebagai barang-barang kapital, sehingga kita harus memberikan pertimbangan kepada perlindungan asuransi.

14.3 KEAMANAN DATA

14.3.1 TUJUAN

Untuk memastikan keselamatan data dalam departemen operasi.

14.3.2 CAKUPAN

Bagian ini menyoroti resiko akibat terbukanya data dan menyarankan tindakan pencegahannya guna meminimisasi atau menghapus bahaya.

Prosedur untuk memproses data dibahas secara rinci dalam Bab 16-25.

14.3.3 FAKTOR KEAMANAN

Data bisa:

Hilang: Beberapa atau semua data bisa lenyap pada atau antara tahapan.

Berubah: Perubahannya disebabkan oleh kesalahan, penanganan yang salah, atau malfungsi.

Terganggu: Pengubahan yang disengaja, pencurian, pengkopian secara tidak sah, atau terlihat oleh seseorang yang seharusnya tidak boleh melihatnya.

Beberapa langkah untuk melindungi data dapat dilakukan oleh Manajer Operasi dengan menetapkan prosedur yang sistematik dan bisa diketahui oleh semua staf di departemennya, dan dengan melakukan pengecekan secara berkala terhadap status keamanan semua stafnya. Selanjutnya, ia bisa bekerja sama dengan fungsi sistem dan pemrograman untuk melakukan pengecekan apakah ia telah melakukan pengecekan secara cukup, dimana hal ini dibuktikan oleh routine komputer guna mencegah atau mendeteksi kesalahan.

14.3.4 INPUT

1. Umum

Input dalam konteks ini mencakup:

— Data mentah yang diantarkan ke departemen operasi, yang biasanya dalam bentuk dokumen sumber;

— Data yang dipersiapkan untuk diserahkan ke komputer, biasanya dalam bentuk form yang dilubangi (punched), media magnetis, atau secara langsung dari peralatan on-line.

Resiko hilang, berubah, dan terganggu dapat dikurangi dengan prosedur yang logis dan supervisi atau pengawasan yang baik.

Semua pekerjaan harus ditetapkan kewenangannya dan diserahkan melalui channel atau saluran yang ditentukan secara jelas.

2. Terminal (Bab 25)

Kita harus menentukan tindakan yang diperbolehkan pada terminal, dan harus menyediakan alat untuk mengontrol akses, misalnya dengan password, kode pemakai, lock (kunci) peralatan.

Password harus hanya diketahui oleh staf yang memerlukannya, dan ia harus diubah secara berkala. Ia harus bisa melumpuhkan pemakai yang tak berhak yang ingin melakukan akses.

Apabila data rahasia ditransmisikan, maka kita harus menggunakan teknik-teknik enkripsi.

Apabila tidak dipakai, terminal harus dikunci sistemnya sampai password dimasukkan kembali.

3. Batching/penumpukan (Bab 16)

Data mentah dan data yang dibuat atau dipersiapkan darinya harus ditumpuk agar mudah dalam penanganannya, pengontrolannya, hubungannya dengan pengembalian media yang diproses ke dokumen sumber, dan kemudahan dalam pencarian lokasi serta pengoeksian kesalahannya.

Slip batch (catatan urutan tumpukan) harus disertakan dalam data melalui berbagai routine, dan kita harus melakukan pengecekan tentang jumlah dokumen atau kartu, nilai totalnya, kuantitasnya, dan sebagainya, pada berbagai tahapan.

Log (catatan dalam buku besar) kontrol data harus dipeliha ra guna mencatat kemajuan atau perkembangan batch (tumpukan) untuk menunjukkan dimana batch terletak (dimana suatu item berada dalam tumpukannya).

Semua ketidaksesuaian/ketidakcocokan harus segera diseli diki, dan kita harus menetapkan prosedur yang menunjukkan bagaimana query ditangani dan apakah dan kapan data bisa dikeluarkan untuk pemrosesan lebih lanjut.

Prosedur untuk menangani input yang tidak lengkap harus dibuat.

4. Konversi Data (Bab 17)

Resiko atas data sangat tinggi jika pekerjaan dikirimkan dari departemen yang ada di lokasi lain atau dikirimkan ke luar, yakni ke biro layanan, untuk preparasi.

Layanan kurir yang bereputasi harus digunakan untuk transit semacam itu, dan dalam hal ini kita juga harus menggunakan perlindungan asuransi.

Dokumen vital dan yang tak dapat diganti (atau dibuat lagi) harus dikopi sebelum dikirimkan.

Pemrosesan ganda yang tak disengaja dapat dicegah dengan menerapkan kontrol batch yang baik, namun sebagai tindakan pencegahan, kita bisa membatalkan dokumen sumber selagi ia diproses (dengan menggunakan cap). Nomor urut dokumen juga dapat dikontrol oleh counter yang ada dalam program terse but.

5. Kerahasiaan

Data harus dilindungi dari gangguan dengan cara memastikan bahwa hanya orang-orang yang berhak-lah yang mengakses ke data tersebut, dengan berhati-hati dalam memilih staf yang menanganinya, dan dengan mengunci dokumen dan kartu ketika tidak sedang digunakan.

Staf yang diberi tugas menangani data ini harus berjumlah lebih dari satu orang. Informasi yang rahasia memerlukan perhatian khusus. Tindakan pencegahan untuk melindungi kerahasiaan ini mencakup:

— Dengan membatasi penanganan informasi seperti itu hanya ke beberapa staf yang terpilih karena rasa tanggung jawab dan kewaspadaan mereka (staf temporer jangan diijinkan mengakses data rahasia);
— Dengan menggunakan kode sebagai pengganti nama untuk membuat sulit pengidentifkasian;
— Dengan meremukkan barang-barang sisa (kertas-kertas) rahasia yang tidak digunakan lagi;
— Apabila stasionari rahasia terpotong, maka karbonnya harus diremuk dengan pemrosesan output;
— Data rahasia harus dipak guna mencegah orang yang tak berhak melihatnya (misalnya, dengan lembaran penutup yang kosong).

14.3.5 PEMROSESAN KOMPUTER

1. Umum

Sebisa mungkin, pekerjaan produksi harus dijalankan menurut jadwal yang telah ditetapkan. Hak (pengesahan) untuk menyimpang dari jadwal harus didelegasikan secara seksama, aturan yang presisi harus ditetapkan, dan variasinya harus dilaporkan. Kita harus memperhatikan secara khusus tentang dependensi pekerjaan (11.2.7) dan deadline (11.4.4.3).

Kita harus melakukan pengecekan guna memastikan bahwa setiap pekerjaan telah dikuasakan secara tepat. Jika pengecekan seperti itu bisa dibangun atau dimasukkan ke dalam sistem pengoperasian, maka pengecekannya akan lebih cermat.

2. Integritas Hardware

Inventaris hardware komputer harus dipelihara dan harus dilakukan pengauditan yang teratur terhadap hardware itu.

Kita harus melakukan pencobaan untuk menggunakan secara penuh fasilitas seperti itu guna mengecek:

— Kesalahan diantara perangkat;
— Malfungsi hardware;

— Kesalahan yang terjadi pada media penyimpanan, dengan pengecekan paritas, pencacahan catatan, dan sebagainya.

Fasilitas pemrosesan duplikat bisa meminimisasi down-time dan kesalahan.

3. Penanganan Media

Data dapat hilang atau terganggu karena penanganan media yang salah atau tidak hati-hati. Biaya minimum yang kita keluarkan untuk tindakan (penanganan) seperti itu adalah waktu yang perlukan untuk menciptakan data lagi; biaya maksimumnya bisa berupa gangguan terhadap operasi efektif pada perusahaan secara keseluruhan.

Para operator harus dilatih untuk menangani media secara benar (20.3), dan mereka harus diberi petunjuk atau in struksi guna memberi referensi kepada mereka.

Media harus dikembalikan ke perpustakaan file atau penyimpanan stasionari segera setelah selesai digunakan, dan dikontrol sehingga kondisi fisik, status, dan lokasinya diketahui sepanjang waktu (20.2).

Kita gunakan log untuk mencatat penggunaan dan malfungsi. Media yang fault harus segera dikeluarkan, misalnya disk yang rusak tidak boleh ditransfer ke drive yang lain, karena ia akan merusak drive itu dan akhirnya berakibat pada disk-disk lain.

4. File

Kita harus menugasi anggota staf operasi yang bertanggung jawab untuk mengontrol pencatatan file, perpindahan inter nalnya, dan statusnya (misalnya, penyimpanan keamanan, retensi normal, dan pengeluaran/penerbitan - lihat 19.3.3) dan penggunaan file data yang tidak sah.

Catatan header file harus berisi informasi yang cukup guna memastikan bahwa kita telah menggunakan edisi atau versi yang benar, dan untuk memastikan bahwa file yang 'read- only' tidak mempunyai write-ring (tidak bisa ditulisi).

Label fisik tidak boleh menunjukkan penggunaan file, misalnya file harus dilabeli 'XYZ', bukannya dilabeli 'Payroll'.

Kita harus memperhatikan kebutuhan transportasi media magnetis. Kotak yang mengandung bahan pelapis harus digunakan untuk wadah guna melindungi file dari radiasi. File harus dihindarkan dari temperatur yang tinggi. (Lihat juga 20.3.3, 20.4.3.5).

5. Kecurangan/ Penipuan

Kita harus melakukan tindakan pencegahan guna mencegah penggunaan fasilitas untuk:

— Memanipulasi data;
— Menjalankan pekerjaan yang tak sah;
— Mengambil/membuat kopi file atau output secara gelap.

Tindakan pencegahannya meliputi:

— Membuat kopi file master (induk) file program, dan file back-up dan menyimpan mereka dalam lokasi yang aman yang jauh dari ruang komputer. Akses ke kopi-kopi tersebut harus dikontrol secara ketat. Auditor bisa menggunakan kopi ini untuk mengecek bahwa file-file yang operasional belum rusak, dan perusahaan asuransi akan meminta dengan sangat agar tindakan seperti itu dilakukan;

— Mengikuti atau menganut prinsip 'split knowledge' (pemecahan pengetahuan), dimana dua orang atau lebih hanya akan bisa menggunakan atau memanfaatkan fungsi yang dikontrol keamanan itu jika mereka bersama-sama (misalnya, untuk memperoleh file yang bernilai, diperlukan dua orang pemegang kunci);

— Melakukan pengontrolan terhadap stasionari guna memastikan bahwa jumlah stasionari yang digunakan telah benar dan jumlah kopi yang dihasilkan juga benar (pengontrolan ini terutama penting untuk cek yang diproduksi oleh komputer atau dokumen yang bernilai uang);

— Membuang output yang tidak diinginkan, misalnya ketika menggunakan stasionari tiga-bagian sebagai pengganti stasionari dua-bagian, atau terjadi kegagalan ketika beberapa pencetakan telah dihasilkan. Output yang tercetak harus diremukkan dulu sebelum dibuang;

— Mengecek log dan laporan untuk mengetahui bahwa pekerjaan yang ditetapkan saja yang dijalankan dan dalam waktu yang diharapkan. Segala perubahan mendadak terhadap pola penggunaan harus diselidiki (13.2.5);

— Melakukan pengawasan yang baik dan memastikan bahwa paling tidak ada dua orang yang selalu berada di ruang komputer. Tim (dua orang ini atau lebih) yang berada di ruang komputer harus diubah atau ditukar dari waktu ke waktu guna meminimisasi peluang terjadinya kolusi.

14.3.6 OUTPUT

1. Umum

Resiko hilang, berubah, dan terganggu dapat diminimisasi dengan tindakan pencegahan biasa, yaitu dengan cara membatasi akses untuk orang-orang yang berhak saja (14.2.6.3), pengawasan yang baik, dan pelatihan.

Semua pekerjaan yang dikumpulkan harus dicek untuk mendeteksi adanya penampungan atau penyimpanan yang tak diijinkan setelah dihasilkannya output.

2. Pemrosesan Output (Bab 23)

Kita harus berhati-hati dalam melakukan operasi seperti peledakan (pembuangan), pemotongan, dan yang sejenis. Peralatan yang terlibat atau dipakai pada dasarnya sederhana, namun dapat merusak atau menghancurkan output dalam sekejap.

Pengawasan harus dilakukan untuk melihat apakah jumlah kopi yang diperlukan saja yang dibuat dan apakah semua kopi tersebut diakui.

3. Pengumpulan dan Pengiriman (Bab 24)

Pengumpulan output merupakan tugas yang perlu ditetapkan, dan output yang menunggu pengumpulan tidak boleh ditinggalkan begitu saja. Output rahasia atau penting harus diberikan kepada anggota staf yang berwenang saja, dengan dilin dungi sedemikian rupa sehingga tak bisa terlihat oleh orang yang tak berhak, misalnya dengan pelindung lembaran kertas kosong, dan ia harus dikunci sampai ia dikumpulkan.

Output yang ditujukan ke lokasi lain harus diantarkan oleh layanan kurir apabila metode lain untuk pengirimannya secara aman tidak ada (misalnya, transportasi yang dimiliki sendiri oleh perusahaan).

Output harus ditandai secara jelas untuk mencegah terjadinya pengantaran yang salah tujuan.

14.4 KEAMANAN SISTEM

14.4.1 TUJUAN

Untuk memastikan keamanan dan integritas sistem.

14.4.2 CAKUPAN

Bagian ini mendeskripsikan tindakan-tindakan pencegahan untuk meminimisasi resiko terhadap sistem, dimana sistem ini diartikan sebagai software (sistem pengoperasian dan program utiliti) dan program aplikasi. Tujuannya adalah untuk menyorot resiko keamanan, bukannya untuk mendeskrip sikan rincian prosedur yang dibahas pada Bab 16-25.

14.4.3 TANGGUNG JAWAB

Ukuran keamanan dibangun atau dimasukkan ke dalam sistem pada waktu tahap desain oleh analis dan programmer. Manajer Operasi harus memastikan bahwa ia telah menggabungkan pengecekan keamanan yang memadai ke dalam sistem sebelum sistem itu bisa diterima untuk dioperasikan.

14.4.4 KEAMANAN PERENCANAAN

Suatu sistem harus:

— Direncanakan untuk memenuhi atau mencapai tujuan-tujuan keamanan;
— Diuji untuk melihat atau mengetahui bahwa ia berfungsi menurut spesifikasinya;
— Diinspeksi atau diawasi guna memastikan bahwa hanya input yang benarlah yang akan diterima dan output yang benar saja yang akan dihasilkan;
— Dimonitor untuk mengecek bahwa ia terus berfungsi secara efisien.

Ukuran keamanan harus:

— Sederhana - kekompleksan akan menimbulkan salah pengertian dan meningkatkan resiko kesalahan;
— Terpadu - dibangun sebagai bagian dari sistem;
— Didokumentasi secara tepat - untuk memberikan uji coba audit dan sebagai alat pengecekan independen;
— Memungkinkan kesalahan dan fault dilokasikan seawal mungkin;
— Memberikan kemudahan akses untuk pengoreksian di bawah kondisi yang terkontrol;
— Menghindari delay produksi yang tidak perlu;
— Bersifat informatif - ia tidak hanya mendeteksi sesuatu yang salah, namun juga mendeteksi apa yang salah, dan bagaimana cara pengoreksiannya.

14.4.5 UKURAN KEAMANAN UMUM

Ukuran yang relevan dengan keamanan data (14.3) juga relevan dengan keamanan sistem.

14.4.6 KEAMANAN SOFTWARE (BAB 27)

1. Penggunaan Versi Yang Benar

Kita harus menetapkan prosedur untuk memastikan bahwa kita telah mensahkan dan menggunakan versi yang benar. Apabila dilakukan perubahan terhadap software, Manajer Operasi harus memastikan bahwa para stafnya mengetahui perubahan itu (8.4 Maklumat Teknis). Rencana pengimplementasian harus mencakup pengaturan kesesuaian apabila terjadi kesalahan. Versi software yang telah kuno harus dikeluarkan (namun disimpan untuk digunakan dalam hal pencocokan) dan versi software back-up (cadangan) yang baru harus tersedia atau bisa digunakan apabila terjadi malfungsi pada perangkat.

2. Perubahan (gangguan) Software Yang Mendadak (tak disengaja)

Prosedur yang ada harus memastikan bahwa software tidak terganggu oleh kesalahan sistem atau kesalahan operator. Resikonya bisa dikurangi dengan pengujian sistem secara memadai, pelatihan yang cukup, dan pengadaan cadangan serta dokumentasi.

3. Perubahan Terhadap Software

Perubahan terhadap software harus disahkan dan ditandatan gani oleh orang yang berwenang, dan tidak boleh dilakukan tanpa adanya wewenang.

14.4.7 PEMELIHARAAN PROGRAM APLIKASI OPERASIONAL (19.4.4)

Perubahan terhadap program operasional hanya boleh dilakukan dengan menetapkan prosedur yang menunjukkan tingkat kewenangan yang diperlukan. Demikian pula halnya, versi program yang baru tidak boleh dioperasionalkan tanpa adanya kewenangan yang diperlukan. Semua perubahan harus didokumentasikan secara tepat.

Koreksi harus dilakukan terhadap kopi program dan file, bukan terhadap aslinya, apabila terjadi perubahan lebih lanjut.