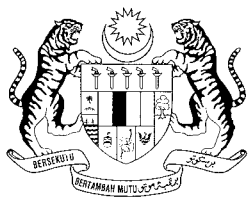


KERAJAAN MALAYSIA

PEKELILING AM BIL. 3 TAHUN 2000

RANGKA DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI KERAJAAN

JABATAN PERDANA MENTERI
MALAYSIA

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Ketua Pengurusan Badan Berkanun Persekutuan
Semua Y.B. Setiausaha Kerajaan Negeri
Semua Ketua Pengurusan Pihak Berkuasa Tempatan

JABATAN PERDANA MENTERI MALAYSIA
KOMPLEKS JABATAN PERDANA MENTERI
PUSAT PENTADBIRAN KERAJAAN
PERSEKUTUAN
62502 PUTRAJAYA

Telefon : 603-88881957
Faks : 603-88883721

Rujukan Kami : UPTM (S) 159/526/1(2)

Tarikh : 1 Oktober 2000

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Ketua Pengurusan Badan Berkanun
Semua Y.B. Setiausaha Kerajaan Negeri
Semua Ketua Pengurusan Pihak Berkuasa Tempatan

PEKELILING AM BIL. 3 TAHUN 2000

RANGKA DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI KERAJAAN

TUJUAN

Pekeliling ini bertujuan untuk menjelaskan Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan serta perkara-perkara berkaitan yang perlu diberi pertimbangan dan diambil tindakan oleh agensi-agensi Kerajaan.

LATAR BELAKANG

2. Kerajaan sentiasa memberi perhatian terhadap keselamatan teknologi maklumat dan komunikasi *(information and communications technology)* atau ICT terutamanya dalam usaha menjayakan pembangunan dan pelaksanaan Aplikasi Perdana Koridor Raya Multimedia. Kerajaan juga sedar akan repositori maklumat semasa yang sangat besar dalam simpanannya, dan dijangka akan bertambah besar dengan terlaksananya projek Aplikasi Perdana yang diterajui Perkhidmatan Awam. Nilai serta kegunaan repositori maklumat juga dijangka akan terus meningkat hasil dari peningkatan pengguna yang bergantung kepada sistem ICT. Ini merupakan sebahagian daripada kesan ledakan pembangunan ICT yang telah mencorak budaya kerja serta cara penyampaian

perkhidmatan Kerajaan kepada rakyat. Trend menunjukkan semakin banyak agensi Kerajaan mengubah hala kepada penggunaan ICT yang lebih meluas untuk mengurangkan kos operasi dan meningkatkan produktiviti dan kualiti perkhidmatan kepada pelanggan.

3. Pertumbuhan pesat penggunaan ICT di kalangan ini, terutama melalui kemudahan Internet, mendedahkan maklumat secara lebih luas dan ini memungkinkan berlakunya pencerobohan yang boleh mengakibatkan kebocoran maklumat rahsia rasmi dan maklumat rasmi Kerajaan. Keadaan ini jika tidak diberi perhatian rapi boleh menimbulkan masalah yang lebih besar di masa hadapan. Di samping itu perlu ada keseimbangan antara kawalan keselamatan yang terlalu ketat sehingga membatasi penyebaran maklumat penyampaian perkhidmatan, dengan kawalan yang terlalu longgar yang boleh memudaratkan keselamatan atau kepentingan Perkhidmatan Awam dan Negara.

4. Menyedari pentingnya usaha-usaha menjamin keselamatan ICT, satu rangka Dasar Keselamatan ICT Kerajaan telah digubal berpandukan kepada prinsip-prinsip keselamatan ICT yang kukuh, tanggungjawab terhadap keselamatan maklumat, kesedaran terhadap ancaman dan langkah-langkah peningkatan tahap keselamatan maklumat.

RANGKA DASAR KESELAMATAN ICT KERAJAAN

5. Rangka Dasar Keselamatan ICT ini dirumus bagi memenuhi keperluan penguatkuasaan, kawalan dan langkah-langkah yang menyeluruh untuk melindungi aset ICT Kerajaan. Perlindungan keselamatan ini perlu bersesuaian dengan nilai atau sensitiviti aset yang dimaksudkan. Ia juga perlu seimbang dengan kesan yang mungkin timbul akibat kegagalan perlindungan yang sesuai. Pernyataan dasar, prinsip, objektif dan skop dasar ini dijelaskan dalam lampiran kepada Pekeliling ini.

TANGGUNGJAWAB AGENSI

6. Semua agensi Kerajaan adalah dikehendaki mematuhi Rangka Dasar Keselamatan ICT Kerajaan dan melaksanakan tanggungjawab yang ditetapkan. Untuk maksud ini, semua Ketua Jabatan adalah diminta mengambil tindakan-tindakan berikut:

(a) Melantik seorang Pegawai Keselamatan ICT di kalangan pegawai kanan yang bertanggungjawab dalam melaksanakan tindakan-tindakan yang ditetapkan dalam Rangka Dasar Keselamatan ICT. Perlantikan pegawai ini dan sebarang pertukaran perlu dimaklumkan kepada MAMPU.

(b) Menyediakan semua infrastruktur keselamatan ICT menepati prinsip-prinsip keselamatan berpandukan Rangka Dasar Keselamatan ICT dan Arahan Keselamatan yang disediakan oleh Ketua Pegawai Keselamatan Kerajaan.

(c) Menyedia dan mengkaji semula dokumen infrastruktur keselamatan ICT bagi tujuan audit keselamatan ICT.

(d) Mengenal pasti bidang-bidang keselamatan ICT yang perlu diberi perhatian rapi dan mengambil tindakan segera mengatasinya.

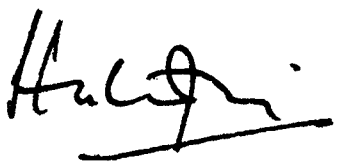
(e) Memastikan tahap keselamatan ICT adalah terjamin setiap masa.

KHIDMAT NASIHAT

7. Sebarang kemusykilan berkaitan dengan Surat Pekeliling ini dan Rangka Dasar Keselamatan ICT Kerajaan bolehlah dirujuk kepada MAMPU, manakala kemusykilan berkaitan dengan Arahan Keselamatan hendaklah dirujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia.

TARIKH KUATKUASA

Surat Pekeliling ini berkuatkuasa mulai tarikh ia dikeluarkan.



(TAN SRI ABDUL HALIM BIN ALI)
Ketua Setiausaha Negara

(Lampiran kepada
Surat Pekeliling Am
Bil. 3 tahun 2000)

RANGKA DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI KERAJAAN

Unit Pemodenan Tadbiran dan
Perancangan Pengurusan Malaysia
(MAMPU)
Jabatan Perdana Menteri

KANDUNGAN

PENGENALAN

Kerajaan sedar akan tanggungjawab untuk memastikan keselamatan aset teknologi maklumat dan komunikasi *(information and communications technology)*, ringkasnya ICT, yang dimiliki atau di bawah jagaan dan kawalannya. Ini termasuk semua data, peralatan, rangkaian dan kemudahan ICT. Tanggungjawab ini juga harus dipikul oleh ahli pentadbiran Kerajaan, penjawat awam atau sesiapa sahaja yang mengakses dan yang menggunakan aset ICT Kerajaan.

RASIONAL

2. Tujuan utama keselamatan ICT adalah untuk menjamin kesinambungan urusan Kerajaan dengan meminimumkan kesan insiden keselamatan. Keselamatan ICT berkait rapat dengan perlindungan maklumat dan aset ICT. Ini kerana komponen peralatan dan perisian yang merupakan sebahagian daripada aset ICT Kerajaan adalah pelaburan besar dan perlu dilindungi. Begitu juga dengan maklumat yang tersimpan di dalam sistem ICT. Ia amat berharga kerana banyak sumber yang telah digunakan untuk menghasilkannya dan sukar untuk dijana semula dalam jangkamasa yang singkat. Tambahan pula terdapat maklumat yang diproses oleh sistem ICT adalah sensitif dan terperingkat. Pendedahan tanpa kebenaran atau pembocoran rahsia boleh memudaratkan kepentingan negara. Sebarang penggunaan aset ICT kerajaan selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber Kerajaan.

3. Memandangkan pentingnya aset ICT Kerajaan dilindungi, maka satu Dasar Keselamatan ICT Kerajaan adalah perlu diwujudkan.

PERNYATAAN DASAR KESELAMATAN ICT KERAJAAN

4. Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

5. Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT, iaitu:

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

(c) Mempastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

(d) Mempastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

6. Dasar Keselamatan ICT Kerajaan merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

(a) Kerahsiaan — Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.

(b) Integriti — Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan.

(c) Tidak Boleh Disangkal—Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.

(d) Kesahihan — Data dan maklumat hendaklah dijamin kesahihannya.

(e) Kebolehsediaan — Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

7. Selain itu, langkah-langkah ke arah keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

PRINSIP-PRINSIP DASAR KESELAMATAN ICT KERAJAAN

8. Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT Kerajaan adalah seperti berikut:

(a) Akses atas dasar "perlu mengetahui"

(b) Hak akses minimum

(c) Akauntabiliti

(d) Pengasingan

(e) Pengauditan

(f) Pematuhan

(g) Pemulihan

(h) Saling bergantung

(a) Akses Atas Dasar Perlu Mengetahui

9. Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan akses di bawah prinsip ini adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut:

(i) ***Klasifikasi Maklumat***

Keselamatan ICT Kerajaan hendaklah mematuhi "Arahan Keselamatan" perenggan 53, muka surat 15, di mana maklumat dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad. Data, bahan atau maklumat rasmi yang sensitif

atau bersifat terperingkat perlu dilindungi dari pendedahan, dimanipulasi atau diubah semasa dalam penghantaran. Penggunaan kod dan tandatangan digital mesti dipertimbangkan bagi melindungi data yang dikirim secara elektronik. Dasar kawalan akses ke atas aplikasi atau sistem juga hendaklah mengikut klasifikasi maklumat yang sama, iaitu sama ada rahsia besar, rahsia, sulit atau terhad.

(ii) ***Tapisan Keselamatan Pengguna***

Dasar Keselamatan ICT Kerajaan adalah mematuhi prinsip bahawa pengguna boleh diberi kebenaran mengakses kategori maklumat tertentu setelah siasatan latarbelakang menunjukkan tiada sebab atau faktor untuk menghalang pengguna daripada berbuat demikian.

(b) Hak Akses Minimum

10. Hak akses kepada pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas adalah diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu data atau maklumat.

(c) Akauntabiliti

11. Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT kerajaan. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

12. Akauntabiliti atau tanggungjawab pengguna termasuklah:

(i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.

(ii) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa.

(iii) Menentukan maklumat sedia untuk digunakan.

(iv) Menjaga kerahsiaan kata laluan.

(v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.

(vi) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.

(vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

(d) Pengasingan

13. Prinsip pengasingan bermaksud bahawa semua tugas-tugas mewujud, memadam, kemaskini, mengubah dan mengesahkan data diasingkan. Ia bertujuan untuk mengelak akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat, dimanipulasi dan seterusnya, mengekalkan integriti dan kebolehsediaan.

14. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. Ia bertujuan untuk mengasingkan akses kepada domain kedua-dua kumpulan tersebut seperti akses kepada fail data, fail program, kemudahan sistem dan komunikasi, manakala pemisahan antara domain pula adalah untuk mengawal dan mengurus perubahan pada konfigurasi dan keperluan sistem.

15. Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:

(i) Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan.

(ii) Persekitaran penerimaan iaitu peringkat di mana sesuatu aplikasi diuji.

(iii) Persekitaran sebenar di mana aplikasi sedia untuk dioperasikan.

(e) Pengauditan

16. Pengauditan adalah tindakan untuk mengenalpasti insiden berkaitan keselamatan atau mengenalpasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router, firewall,* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail.* Pentingnya *audit trail* ini menjadi semakin ketara apabila wujud keperluan untuk mengenalpasti punca masalah atau ancaman kepada keselamatan ICT. Oleh itu, rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta merta.

17. Pengauditan juga perlu dibuat ke atas rekod-rekod manual seperti dokumen operasi, nota serah tugas, kelulusan keluar pejabat, memorandum, borang kebenaran, surat kuasa, senarai inventori dan kemudahan akses log. Ini adalah kerana dalam kes-kes tertentu, dokumen ini diperlukan untuk menyokong *audit trail* sistem komputer.

18. Keseluruhannya, sistem pengauditan ini adalah penting dalam menjamin akauntabiliti. Antara lain, sistem ini dapat dirujuk bagi menentukan perkara-perkara berikut:

(i) Mengesan pematuhan atau perlanggaran keselamatan.

(ii) Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya perlanggaran keselamatan.

(iii) Menyediakan bahan bukti bagi menentukan sama ada berlakunya perlanggaran keselamatan.

(f) Pematuhan

19. Pematuhan adalah merupakan prinsip penting dalam menghindar dan mengesan sebarang perlanggaran Dasar. Pematuhan kepada Dasar Keselamatan ICT Kerajaan boleh dicapai melalui tindakan berikut:

(i) Mewujud proses yang sistematik khususnya dalam menjamin keselamatan ICT untuk memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan.

(ii) Merumus pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenalpasti.

(iii) Melaksana program pemantauan keselamatan secara berterusan untuk memastikan standard, prosedur dan garis panduan keselamatan dipatuhi.

(iv) Menguatkuasa amalan melapur sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

(g) Pemulihan

20. Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Antara lain, pemulihan boleh dilakukan melalui tindakan-tindakan berikut:

(i) Merumus dan menguji Pelan Pemulihan Bencana/Kesinambungan Perkhidmatan—*(Disaster Recovery/Business Resumption Plan).*

(ii) Mengamalkan langkah-langkah membuat salinan data dan lain-lain amalan baik dalam penggunaan ICT seperti menghapuskan virus, langkah-langkah pencegahan kebakaran dan amalan "clear desk".

(h) Saling Bergantung

21. Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip di atas. Setiap prinsip adalah saling lengkap-melengkapi antara satu dengan lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisma keselamatan, dapat menjamin keselamatan yang maksimum. Prinsip saling bergantung meliputi beberapa peringkat di mana di tahap minimum, mengandungi langkah-langkah berikut:

(i) Sambungan kepada Internet - Semua komunikasi antara sistem ICT dengan sistem luar hendaklah melalui mekanisma pusat untuk mengurus, menguatkuasa dan mengawas sebarang bahaya keselamatan. Melalui sistem ini, semua trafik dalaman hendaklah melalui *gateway firewall* yang diurus secara berpusat. Semua trafik dari luar ke dalam hendaklah juga melalui laluan ini atau melalui kumpulan modem yang dikawal secara berpusat. Dengan itu, penggunaan modem dalaman tidak dibenarkan.

(ii) *Backbone* Rangkaian - *Backbone* rangkaian akan hanya mengendalikan trafik yang telah dikod untuk meminimumkan intipan.

(iii) Rangkaian Jabatan - Semua rangkaian jabatan akan dihubungkan ke *backbone* melalui *firewall* yang mana akan pula mengkod semua trafik di antara rangkaian jabatan dengan rangkaian di peringkat yang seterusnya atau pusat data.

(iv) Pelayan Jabatan - Semua data dan maklumat yang kritikal atau sensitif akan hanya disimpan di pelayan jabatan atau di pelayan yang diurus secara pusat. Ini akan meminimumkan pendedahan, pengubahan atau kecurian. Semua data dan maklumat sensitif akan dikodkan.

OBJEKTIF DASAR KESELAMATAN ICT KERAJAAN

22. Objektif utama Dasar Keselamatan ICT Kerajaan ialah seperti berikut:

(i) Memastikan kelancaran operasi kerajaan dan meminimumkan kerosakan atau kemusnahan;

(ii) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

(iii) Mencegah salahguna atau kecurian aset ICT kerajaan.

23. Dasar Keselamatan ICT Kerajaan ini juga bertujuan memudahkan perkongsian maklumat sesuai dengan keperluan operasi kerajaan. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

SKOP DASAR KESELAMATAN ICT KERAJAAN

24. Sistem ICT Kerajaan terdiri daripada manusia, peralatan, perisian, telekomunikasi, kemudahan ICT dan data. Sistem ini adalah aset yang amat berharga di mana masyarakat, swasta dan juga Kerajaan bergantung untuk menjalankan urusan rasmi Kerajaan dengan lancar. Dengan itu, Dasar Keselamatan ICT Kerajaan menetapkan keperluan-keperluan asas berikut:

(i) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.

(ii) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, bisnes dan masyarakat.

25. Memandangkan sistem ICT sangat kompleks dan terdedah kepada kelemahan, ancaman dan risiko, adalah tidak mudah untuk memenuhi keperluan ini. Sistem ICT dan komponennya yang saling berhubungan dan bergantungan antara satu dengan lain kerapkali mewujudkan pelbagai kelemahan. Sesetengah risiko hanya menjadi kenyataan setelah masa berlalu manakala sesetengahnya timbul apabila berlaku perubahan. Walau bagaimanapun risiko seperti ini hendaklah dikenalpasti dan ditangani sewajarnya.

26. Bagi menangani risiko ini dari semasa ke semasa, Dasar Keselamatan ICT Kerajaan akan diperjelaskan lagi melalui pengeluaran Standard Keselamatan ICT yang mengandungi garis panduan serta langkah-langkah keselamatan ICT. Kegunaan kesemua dokumen ini secara bersepadu adalah disarankan. Ini adalah kerana pembentukan dasar, standard, garis panduan dan langkah-langkah keselamatan ini diorientasikan untuk melindungi kerahsiaan data, maklumat dan sebarang kesimpulan yang boleh dibuat daripadanya.

27. Bagi menentukan Sistem ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT Kerajaan ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasuk, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan ke dalam semua aset ICT. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

(i) Data dan Maklumat - Semua data dan maklumat yang disimpan atau digunakan dipelbagai media atau peralatan ICT.

(ii) Peralatan ICT - Semua peralatan komputer dan periferal seperti komputer peribadi, stesen kerja, kerangka utama dan alat-alat prasarana seperti *Uninterrupted Power Supply* (UPS), punca kuasa dan pendingin hawa.

(iii) Media Storan - Semua media storan dan peralatan yang berkaitan seperti disket, kartrij, CD-ROM, pita, cakera, pemacu cakera dan pemacu pita.

(iv) Komunikasi dan Peralatan Rangkaian - Semua peralatan berkaitan komunikasi seperti pelayan rangkaian, *gateway, bridge, router* dan peralatan *PABX*.

(v) Perisian - Semua perisian yang digunakan untuk mengendali, memproses, menyimpan, menjana dan mengirim maklumat. Ini meliputi semua perisian sistem, perisian utiliti, perisian rangkaian, program aplikasi, pangkalan data, fail program dan fail data.

(vi) Dokumentasi - Semua dokumentasi yang mengandungi maklumat berkaitan dengan penggunaan dan pemasangan peralatan dan perisian. Ia juga meliputi data dalam semua bentuk media seperti salinan kekal, salinan elektronik, *transparencies*, risalah dan *slides*.

(vii) Manusia - Semua pengguna yang dibenarkan termasuk pentadbir dan pengurus serta mereka yang bertanggungjawab terhadap keselamatan ICT.

(viii) Premis Komputer dan Komunikasi - semua kemudahan serta premis yang diguna untuk menempatkan perkara (i) - (vii) di atas.

28. Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

29. Di samping itu, Dasar Keselamatan ICT Kerajaan ini juga adalah saling lengkap-melengkapi dan perlu dilaksanakan secara konsisten dengan undang-undang dan peraturan yang sedia ada.

TANGGUNGJAWAB KETUA-KETUA JABATAN

30. Semua Ketua-ketua Jabatan perlu mematuhi Dasar Keselamatan ICT Kerajaan. Tugas dan tanggungjawab Ketua-ketua Jabatan adalah seperti berikut:

(i) Menentukan semua pegawai dan staf jabatan memahami keperluan standard, garis panduan, prosedur dan langkah keselamatan di bawah Dasar Keselamatan ICT Kerajaan.

(ii) Menentukan semua pegawai dan staf jabatan mematuhi standard, garis panduan, prosedur dan langkah keselamatan di bawah Dasar Keselamatan ICT Kerajaan. Tindakan sewajarnya hendaklah diambil apabila berlaku sebarang perlanggaran keselamatan.

(iii) Menjalankan penilaian risiko dan program keselamatan berpandukan kepada standard, garis panduan, prosedur dan langkah keselamatan ICT.

(iv) Mengadakan Pelan Rancangan Pematuhan yang bertujuan untuk mengurus risiko yang timbul akibat daripada ketidakpatuhan kepada standard, garis panduan, prosedur dan langkah keselamatan ICT.

(v) Melaporkan kepada MAMPU, Jabatan Perdana Menteri sebarang insiden perlanggaran keselamatan seperti kejadian-kejadian berikut:

- Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa.
- Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian.
- Kata laluan atau mekanisma kawalan sistem akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan.
- Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerapkali gagal dan komunikasi tersalah hantar.
- Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.

31. Tugas-tugas di atas hendaklah dilaksanakan oleh Pegawai Keselamatan ICT Jabatan yang bertanggungjawab kepada Ketua Pegawai Maklumat (CIO) sepertimana yang dilantik di bawah Arahan KSN Rujukan PM(S) 18114 Jld 13 (74) bertarikh 22 Mac 2000.

TANGGUNGJAWAB AGENSI PUSAT

32. Agensi pusat yang bertanggungjawab ke atas keselamatan ICT Kerajaan adalah Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri. Tanggungjawab MAMPU adalah seperti berikut:

(i) Memberi pendedahan dan penjelasan mengenai Dasar Keselamatan ICT Kerajaan.

(ii) Mengemaskini Dasar Keselamatan ICT Kerajaan termasuk menetapkan standard, garis panduan, prosedur dan langkah keselamatan dari semasa ke semasa.

(iii) Menyediakan perkhidmatan berpusat untuk menerima laporan insiden keselamatan ICT, penyebaran maklumat dan pelarasan tindakan pembetulan.

(iv) Memantau pelaksanaan dan menguatkuasa Dasar Keselamatan ICT Kerajaan.

PINDAAN DAN KEMASKINI

33. Dasar Keselamatan ICT Kerajaan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Dasar ini hendaklah dibaca bersama dokumen-dokumen mengenai standard, garis panduan, prosedur dan langkah keselamatan ICT Kerajaan yang akan dikeluarkan dari semasa ke semasa.

MAKLUMAT LANJUT

Sebarang pertanyaan mengenai kandungan dokumen ini atau permohonan untuk keterangan lanjut, boleh ditujukan kepada:

Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia
(MAMPU) Jabatan Perdana Menteri
(Bahagian Keselamatan ICT Kerajaan)
Aras 6 Blok B2 Parcel B
Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA
Telefon: 03-8888 2250
Faks: 03-8888 3286
E-Mel: ictsec@mampu.gov.my

Rangka Dasar Keselamatan ICT Kerajaan ini juga boleh diakses di laman web MAMPU JPM
(http://www.mampu.gov.my)

PINDAAN DAN KEMASKINI

33. Dasar Keselamatan ICT Kerajaan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Dasar ini hendaklah dibaca bersama dokumen-dokumen mengenai standard, garis panduan, prosedur dan langkah keselamatan ICT Kerajaan yang akan dikeluarkan dari semasa ke semasa.

MAKLUMAT LANJUT

Sebarang pertanyaan mengenai kandungan dokumen ini atau permohonan untuk keterangan lanjut, boleh ditujukan kepada:

Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia
(MAMPU) Jabatan Perdana Menteri
(Bahagian Keselamatan ICT Kerajaan)
Aras 6 Blok B2 Parcel B
Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA
Telefon: 03-8888 2250
Faks: 03-8888 3286
E-Mel: ictsec@mampu.gov.my

Rangka Dasar Keselamatan ICT Kerajaan ini juga boleh diakses di laman web MAMPU JPM
(http://www.mampu.gov.my)