DASAR KESELAMATAN ICT

KEMENTERIAN DALAM NEGERI

VERSI 2.0

Dasar Keselamatan ICT Kementerian Dalam Negeri terpakai untuk Kementerian Dalam Negeri dan Agensi / Jabatan di dalamnya.

Document authorization

Document	: Dasar Keselamatan ICT kementerian Dalam Negeri
Effective date	:
Document Owner	:

Prepared by:

Name	Department	Date

Review by:

Name	Department	Date

Endorsed by:

Name	Department	Date

Revison History :

Version no.	Date	Summary of change	Updates by
1.0	Mac 2009	Original release	KDN
2.0	Dis 2014	Adding the following section to map the existing DKICT with the new released 2013 standard: 0205, 0206, 0207, 0615 0709, 0808, 0809, 0810, 0811, 0812, 0906, 0907 and 1105 Ammendment on 0807 - change to "**setahun sekali"**	KDN

KANDUNGAN

A. 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 merangkumi data atau maklumat, perkakasan, perisian, sistem sokongan dan manusia (yang mengendalikan aset ICT). Tanggungjawab ini juga harus dipikul oleh penjawat awam atau sesiapa sahaja yang menggunakan aset ICT Kerajaan selaras dengan motto Kementerian iaitu **'Keselamatan Tanggungjawab Bersama'.**

'Dasar Keselamatan ICT KDN' mengandungi peraturan-peraturan yang mesti dipatuhi semasa menggunakan aset ICT KDN yang dikawal selia sepenuhnya oleh Bahagian Pengurusan Teknologi Maklumat (Bahagian IT). Dasar ini juga menerangkan tanggungjawab dan peranan semua pengguna dalam melindungi aset ICT Kerajaan.

B. RASIONAL DASAR KESELAMATAN ICT

'**Keselamatan ICT**' ditakrifkan sebagai keadaan di mana segala urusan menyedia dan membekal perkhidmatan berjalan secara berterusan tanpa gangguan yang boleh menjejaskan urusan pentadbiran dan sistem penyampaian perkhidmatan kerajaan.[1]

Secara ringkasnya, **objektif Keselamatan ICT** adalah untuk melindungi aset ICT; mengurangkan kesan atau impak insiden Keselamatan ICT; dan menjamin kesinambungan urusan pentadbiran Kerajaan dan sistem penyampaian perkhidmatan Kerajaan (proses yang berterusan) dengan gangguan yang minima.

Aset ICT Kerajaan perlu dilindungi kerana ianya merupakan pelaburan besar Kerajaan bagi meningkatkan mutu, kecekapan dan keberkesanan sistem penyampaian perkhidmatan Kerajaan.

'**Aset ICT' dikategorikan** kepada lima (5) elemen penting di dalam Kementerian iaitu :[2]

(i) Maklumat atau Data;
(ii) Perisian;
(iii) Perkakasan;
(iv) Sistem Sokongan atau Infrastruktur atau Utiliti; dan
(v) Manusia.

[1] Merujuk kepada *Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002*

[2] Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005.

Maklumat yang tersimpan di dalam sistem ICT Kerajaan amat berharga kerana banyak sumber yang telah digunakan untuk mewujudkannya dan sukar untuk dijana semula dalam jangka masa yang singkat. Tambahan pula, terdapat maklumat yang diproses oleh sistem ICT adalah sensitif dan **terperingkat** (Terhad, Sulit, Rahsia dan Rahsia Besar).

Pendedahan tanpa kebenaran atau pembocoran rahsia boleh memudaratkan kepentingan negara. Sebarang penggunaan aset ICT selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber Kerajaan.

Ancaman atau insiden Keselamatan ICT boleh memberi kesan ke atas semua pihak termasuklah aset ICT yang dikendalikan. Terdapat **sembilan (9) jenis insiden Keselamatan ICT** iaitu: [3]

(i) **Pelanggaran Dasar (*Violation of Policy*)**

Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar Dasar Keselamatan ICT.

(ii) **Penghalangan Penyampaian Perkhidmatan (*Denial of Service*)**

Ancaman ke atas keselamatan sistem komputer di mana perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal termasuk *denial of service* (DoS), *distributed denial of service* (DDoS) dan *sabotage*.

(iii) **Pencerobohan (*Intrusion*)**

Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem (*system tampering*), pindaan data (*modification of data*) dan pindaan kepada konfigurasi sistem.

(iv) **Pemalsuan (*Forgery*)**

Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*) dan penipuan (*hoaxes*).

(v) ***Spam***

Spam adalah emel yang dihantar ke akaun emel orang lain yang tidak dikenali penghantar dalam satu masa dan secara berulang-kali (kandungan emel yang sama). Ini menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan.

[3] Merujuk kepada Surat Pekeliling Am Bil. 4 Tahun 2006 : Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam

(vi) ***Malicious Code***

Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.

(vii) ***Harrassment/Threats***

Gangguan dan ancaman melalui pelbagai cara iaitu emel dan surat yang bermotif personal dan atas sebab tertentu.

(viii) ***Attempts/Hack Threats/Information Gathering***

Percubaaan (samada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran termasuk *spoofing, phishing, probing, war driving* dan *scanning.*

(ix) **Kehilangan Fizikal (*Physical Loss*)**

Kehilangan capaian dan kegunaan disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT berpunca dari ancaman pencerobohan.

Ancaman dan kesan insiden Keselamatan ICT semakin meningkat dan mampu menjejaskan sistem penyampaian perkhidmatan Kerajaan dan infrastruktur informasi kritikal Kerajaan *Critical National Infomation Infrastructure* (CNII). Memandangkan pentingnya aset ICT dilindungi, maka satu Dasar Keselamatan ICT KDN perlu diwujudkan.

'Dasar Keselamatan ICT' ditakrifkan sebagai dokumen peringkat tertinggi yang menyatakan hasrat dan hala tuju pihak pengurusan organisasi dalam usaha melindungi aset ICT. Dokumen ini disasarkan kepada setiap warga KDN, **pembekal, pakar runding dan pihak-pihak lain** yang mempunyai kepentingan di dalam mengendalikan maklumat KDN.

Isu Keselamatan ICT Kerajaan telah diberi penekanan yang tinggi disebabkan insiden Keselamatan ICT di agensi Kerajaan semakin meningkat, kos projek ICT Kerajaan semakin tinggi, serta kebergantungan sistem penyampaian perkhidmatan Kerajaan dan kebanyakan urus tadbir Kerajaan menggunakan ICT sebagai *key enabler* juga semakin meningkat. Oleh itu, penekanan ke atas kesedaran dan tahap Keselamatan ICT adalah penting dan perlu diberi perhatian yang serius.

Dasar Keselamatan ICT KDN mempunyai **Enam (6) kepentingan** iaitu :

(i) Menjamin urusan kerja dan perkhidmatan supaya lancar dan berterusan;
(ii) Melindungi aset ICT;
(iii) Keperluan perundangan (sekiranya berlaku perlanggaran dasar);
(iv) Mengimbangi antara kos dengan keberkesanan Keselamatan ICT;
(v) Meminimumkan kesan insiden Keselamatan ICT; dan
(vi) Menjamin keutuhan Keselamatan ICT.

Perlanggaran 'Dasar Keselamatan ICT' KDN **ditakrifkan** sebagai sebarang penggunaan aset ICT selain daripada maksud dan tujuan yang telah ditetapkan di dalam Dasar Keselamatan ICT KDN seperti pencerobohan, kecurian maklumat, membalas emel SPAM atau *junkmail*, penyebaran emel layang atau fitnah, dan sebagainya adalah merupakan satu (1) perlanggaran dasar dan akan dikenakan tindakan tata tertib serta disiplin.

C. ASAS KESELAMATAN ICT

Terdapat tiga (3) komponen asas dalam Keselamatan ICT iaitu :

(i) **Kerahsiaan** (***C****onfidentiality*) – Memastikan data dan maklumat boleh dibaca oleh pihak yang berhak sahaja, dilindungi dari pihak yang tidak berkenaan dan tidak didedahkan sewenang-wenangnya atau dibiarkan dicapai tanpa kebenaran;

(ii) **Integriti** (***I****ntegrity*) – Memastikan data dan maklumat adalah tepat dan lengkap seperti asal serta dikemaskini atau diubah dengan cara yang dibenarkan; dan

(iii) **Ketersediaan** (***A****vailability*) – Memastikan data dan maklumat boleh digunakan dan dicapai pada bila-bila masa oleh pengguna yang sah dan dibenarkan sahaja.

D. OBJEKTIF DASAR KESELAMATAN ICT

(i) Objektif utama Dasar Keselamatan ICT KDN ialah seperti berikut :

(a) Memastikan kelancaran operasi KDN dan meminimumkan kerosakan atau kemusnahan;

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

(c) Mencegah salah guna, kecuaian atau kecurian aset ICT.

(ii) Dasar Keselamatan ICT KDN ini juga bertujuan memudahkan perkongsian maklumat sesuai dengan keperluan operasi KDN. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

E. PRINSIP DASAR KESELAMATAN ICT

Terdapat lapan (8) prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT KDN, iaitu :

(i) **Akses Atas Dasar Perlu Mengetahui**

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:

(a) Klasifikasi Maklumat

Keselamatan ICT KDN 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, di manipulasi 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; dan

(b) Tapisan Keselamatan Pengguna

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

(ii) **Hak Akses Minimum**

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, mengemas kini, mengubah atau membatalkan sesuatu data atau maklumat.

(iii) **Akauntabiliti**

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. 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.

Akauntabiliti atau tanggungjawab pengguna termasuklah :

(a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

(b) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;

(c) Menentukan maklumat sedia untuk digunakan;

(d) Menjaga kerahsiaan kata laluan;

(e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

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

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

(iv) **Pengasingan**

(a) Prinsip pengasingan bermaksud bahawa semua tugas-tugas mewujud, memadam, mengemas kini, 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; dan

(b) 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.

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

(a) Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan;

(b) Persekitaran penerimaan iaitu peringkat di mana sesuatu aplikasi diuji dan dibuat perakuan penerimaan pengguna; dan

(c) Persekitaran sebenar di mana aplikasi sedia untuk beroperasi.

(v) **Pengauditan**

(a) Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti 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 mengenal pasti punca masalah atau ancaman kepada keselamatan ICT. Oleh itu, rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta-merta;

(b) 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; dan

(c) 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; dan

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

(vi) **Pematuhan**

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

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

(b) Merumus pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenal pasti;

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

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

(vii) **Pemulihan**

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:

(a) Merumus dan menguji Pelan Pemulihan Bencana— (*Disaster Recovery Plan*); dan

(b) 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*.

(viii) **Saling Bergantung**

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 mekanisme keselamatan, dapat menjamin keselamatan yang maksimum. Prinsip saling bergantung meliputi beberapa peringkat di mana di tahap minimum, mengandungi langkah-langkah berikut:

(a) Sambungan kepada internet - Semua komunikasi antara sistem ICT dengan sistem luar hendaklah melalui mekanisme 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;

(b) *Backbone* Rangkaian - *Backbone* rangkaian akan hanya mengendalikan trafik yang telah di kod untuk meminimumkan intipan;

(c) Rangkaian KDN - Semua rangkaian KDN akan dihubungkan ke *backbone* melalui *firewall* yang mana akan pula mengkod semua trafik di antara rangkaian KDN dengan rangkaian di peringkat yang seterusnya atau pusat data; dan

(d) Pelayan KDN - Semua data dan maklumat yang kritikal atau sensitif akan hanya disimpan di pelayan KDN atau di pelayan yang diurus secara berpusat. Ini akan meminimumkan pendedahan, pengubahan atau kecurian. Semua data dan maklumat sensitif akan dikodkan.

F. SKOP DASAR KESELAMATAN ICT

Skop Dasar Keselamatan ICT KDN meliputi aset ICT yang berikut :-

(i) Sistem ICT KDN terdiri daripada perkakasan, perisian, manusia, perkhidmatan dan data atau maklumat. Ianya adalah aset yang amat berharga di mana pengguna (agensi-agensi Kerajaan, pihak swasta, warganegara dan bukan warganegara yang bermastautin) bergantung

untuk menjalankan urusan rasmi dengan lancar. Dengan itu, Dasar Keselamatan ICT KDN menetapkan keperluan-keperluan asas berikut:

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

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

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

(iii) Bagi menangani risiko ini dari semasa ke semasa, Dasar Keselamatan ICT KDN 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.

(iv) Bagi menentukan Sistem ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT KDN ini merangkumi perlindungan semua bentuk maklumat Kerajaan yang dimasukkan, 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:

(a) **Perkakasan** - Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan KDN. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) **Perisian** - Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat

yang menyediakan kemudahan pemprosesan maklumat kepada KDN;

(c) **Perkhidmatan** – Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh :

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

(d) **Data atau Maklumat** – Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif KDN. Contoh : Sistem dokumentasi, prosedur operasi, rekod-rekod KDN, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain.

(e) **Manusia** – Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian KDN bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

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

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

G. PINDAAN DAN KEMASKINI

Dasar Keselamatan ICT KDN adalah tertakluk kepada semakan dan pindaan dari masa 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.

H. MAKLUMAT LANJUT

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

Kementerian Dalam Negeri,
Bahagian Pengurusan Teknologi Maklumat (Bahagian IT),
Aras 5, Blok D2, Kompleks D,
Pusat Pentadbiran Kerajaan Persekutuan,
62546 PUTRAJAYA.

Telefon : **03-8886 3081**
Faks : **03-8889 1749**
E-Mel : **kdncert@moha.gov.my**

Dasar Keselamatan ICT KDN ini juga boleh diakses di portal Intranet KDN (**http://www.moha.gov.my**)

I. DASAR WAJIB DAN TERPAKAI

Dasar ini adalah wajib dan terpakai kepada setiap warga KDN, pembekal, pakar runding dan pihak-pihak lain yang mencapai, mengurus, menyelenggara, memproses, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT KDN, yakni **KERAJAAN MALAYSIA**. Pengguna bertanggungjawab untuk membaca, memahami dan menandatangani '**Surat Akuan Pematuhan Dasar Keselamatan ICT**' Kementerian Dalam Negeri (KDN).

Lampiran A

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT KDN

Nama : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan / Bahagian / Unit : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

1. Saya telah mengikuti Taklimat Dasar Keselamatan ICT KDN;
2. Saya juga telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT KDN; dan
3. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....
(Tanda Tangan Pegawai / Kakitangan)

Tarikh : .....

Disahkan Oleh :
Pegawai Keselamatan ICT (ICTSO) KDN

.....
( )

Tarikh : .....

Diperakukan Oleh :
Ketua Pegawai Maklumat (CIO) KDN

.....
( )

Tarikh : .....

PERKARA 01 : PEMBANGUNAN, PELAKSANAAN DAN PENYELENGGARAAN DASAR KESELAMATAN ICT KDN

Huraian :	KDN dan agensi-agensi di bawahnya hendaklah mewujudkan, melaksanakan dan menyelenggarakan dasar-dasar yang jelas yang dapat menjamin perlindungan ke atas kerahsiaan, integriti dan ketersediaan maklumat dan seterusnya menjamin kesinambungan urusan serta perkhidmatan dengan meminimumkan kesan insiden Keselamatan ICT.
Objektif :	Untuk memberi hala tuju dan peraturan-peraturan bagi mengguna dan melindungi aset ICT selaras dengan keperluan undang-undang.

DKICTKDN-0101 Pelaksanaan Dan Penyelenggaraan Dasar Keselamatan ICT KDN

Seksyen ini bertujuan memastikan hala tuju pengurusan KDN untuk melindungi aset ICT selaras dengan keperluan perundangan. Adalah menjadi tanggungjawab Ketua Setiausaha KDN ke atas pelaksanaan dasar dengan dibantu oleh Jawatankuasa Pengurusan Keselamatan ICT yang terdiri dari Ketua Pegawai Maklumat (CIO), Setiausaha Bahagian IT, Pengarah KDN CERT, Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik.

Pasukan petugas untuk mengendalikan operasi keselamatan ICT adalah Pasukan KDN CERT. Ahli Pasukan KDN CERT adalah terdiri dari Pengarah KDN CERT, Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik serta wakil daripada semua agensi di dalamnya.

Dasar Keselamatan ICT KDN hendaklah diterima pakai oleh pengurusan dan disebarkan kepada semua warga KDN.

DKICTKDN-0102 Pemakaian Dasar Keselamatan ICT KDN

Dasar Keselamatan ICT KDN adalah terpakai kepada setiap warga KDN, pembekal, pakar runding dan pihak-pihak lain yang mempunyai kepentingan di dalam mengendalikan maklumat KDN.

DKICTKDN-0103 Semakan Dan Pindaan Dasar

Dasar Keselamatan ICT KDN adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Prosedur penyelenggaraan Dasar Keselamatan ICT KDN adalah termasuk yang berikut :

(a) Menyemak dasar ini sekurang-kurangnya sekali setahun bagi mengenal pasti dan menentukan perubahan yang diperlukan;

(b) Mengemukakan cadangan perubahan secara bertulis kepada Bahagian Pengurusan Teknologi Maklumat (Bahagian IT), Kementerian Dalam Negeri dan dibawa ke dalam Mesyuarat Jawatankuasa Pemandu ICT KDN (JPICT) untuk kelulusan; dan

(c) Memaklumkan perubahan dasar yang telah dipersetujui oleh Bahagian Pengurusan Teknologi Maklumat (Bahagian IT), Kementerian Dalam Negeri kepada semua pengguna.

PERKARA 02 : PENGURUSAN KESELAMATAN ICT

Huraian :	Satu rangka kerja pengurusan keselamatan ICT perlu diwujudkan supaya keselamatan ICT dilaksanakan dengan lebih sistematik, berstruktur, lancar dan berkesan.
Objektif :	Untuk menguruskan keselamatan ICT di KDN dan agensi di bawahnya

DKICTKDN-0201 Pengurusan Keselamatan ICT

Setiausaha Bahagian / Ketua Bahagian KDN adalah bertanggungjawab untuk :

(a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT KDN;

(b) Mewujud dan mengetuai jawatankuasa pengurusan keselamatan ICT KDN;

(c) Memastikan semua pengguna ICT KDN memahami dan mematuhi Dasar Keselamatan ICT KDN;

(d) Memastikan semua keperluan keselamatan ICT KDN (sumber kewangan, kakitangan dan perlindungan keselamatan) adalah mencukupi;

(e) Memastikan penilaian risiko, program penguatkuasaan, kesedaran dan pembudayaan keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT KDN; dan

(f) Menandatangani `Surat Akuan Pematuhan' bagi mematuhi Dasar Keselamatan ICT KDN (Lampiran A).

DKICTKDN-0202 Struktur Organisasi

Seksyen ini bertujuan memastikan struktur formal diwujudkan untuk mengurus keselamatan ICT KDN dan Jabatan di bawahnya.

Jawatankuasa Pemandu ICT KDN dan KDN CERT adalah bertanggungjawab terhadap pengurusan keselamatan ICT KDN. Jawatankuasa Pemandu ICT Agensi adalah bertanggungjawab terhadap pengurusan keselamatan ICT Agensi.

Perkara yang perlu dipatuhi termasuk yang berikut :

(a) Komitmen pengurusan atasan ke atas keselamatan ICT dilaksanakan dengan aktif dan telus;

(b) Aktiviti pengurusan keselamatan ICT diselaraskan oleh Ketua Setiausaha / Setiausaha Bahagian / Ketua Bahagian dari semua peringkat organisasi berdasarkan peranan masing-masing;

(c) Tanggungjawab yang jelas bagi semua pengguna ICT KDN dalam pengurusan keselamatan ICT;

(d) Keperluan untuk pengurusan kerahsiaan maklumat dikenal pasti, dilaksana dan dikaji secara berkala;

(e) Memastikan jalinan perhubungan/komunikasi dengan pihak yang relevan dipelihara; dan

(f) Memastikan kajian semula ke atas keselamatan maklumat dijalankan mengikut peraturan yang ditetapkan.

DKICTKDN-0203 Pihak Luar / Asing

Seksyen ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak luar / asing dikawal.

Perkara yang perlu dipatuhi termasuk yang berikut :

(a) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;

(b) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pengguna; dan

(c) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga.

Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai.

(a) Dasar Keselamatan ICT KDN;

(b) Tapisan Keselamatan;

(c) Perakuan Akta Rahsia Rasmi 1972 (Akta 88); dan

(d) Hak Harta Intelek.

DKICTKDN-0204 Jawatankuasa Pengurusan Keselamatan ICT

Seksyen ini bertujuan menerangkan peranan dan tanggungjawab ahli jawatankuasa pengurusan keselamatan ICT KDN

DKICTKDN-020401

(a) **Ketua Pegawai Maklumat (CIO)**

Peranan dan tanggungjawab adalah termasuk seperti berikut :

i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT KDN;

ii. Membantu Ketua Setiausaha dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT KDN;

iii. Menentukan keperluan keselamatan ICT KDN;

iv. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT KDN; dan

v. Menandatangani `Surat Akuan Pematuhan' bagi mematuhi Dasar Keselamatan ICT KDN (Lampiran A).

DKICTKDN-020402

(b) **Pegawai Keselamatan ICT (ICTSO)**

Peranan dan tanggungjawab adalah termasuk seperti berikut :

i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT KDN;

ii. Mengurus keseluruhan program-program keselamatan ICT KDN;

iii. Menguatkuasakan Dasar Keselamatan ICT KDN;

iv. Memberi penerangan, pendedahan dan menguatkuasa Dasar Keselamatan ICT KDN kepada semua pengguna;

v. Mewujudkan garis panduan dan prosedur selaras dengan keperluan Dasar Keselamatan ICT KDN;

vi. Melaksanakan pengurusan risiko keselamatan ICT KDN;

vii. Melaksanakan pengauditan, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya;

viii. Memberi amaran kepada KDN terhadap kemungkinan berlakunya ancaman keselamatan ICT seperti *virus, worm* dan penggodam serta memberi khidmat

nasihat dan bantuan teknikal bagi menyediakan langkah-langkah perlindungan yang bersesuaian;

ix. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT KDN (KDN CERT) dan GCERT MAMPU dan memaklumkannya kepada Ketua Setiausaha, CIO dan Pengarah CERT KDN;

x. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;

xi. Memberi perakuan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT KDN;

xii. Menyedia dan melaksana program-program kesedaran dan pembudayaan mengenai keselamatan ICT; dan

xiii. Menandatangani `Surat Akuan Pematuhan' bagi mematuhi Dasar Keselamatan ICT KDN (Lampiran A).

DKICTKDN-020403

(c) **Setiausaha Bahagian Pengurusan ICT**

Peranan dan tanggungjawab adalah termasuk seperti berikut :

i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT KDN;

ii. Memastikan kajian semula dan pelaksanaan kawalan keselamatan ICT selaras dengan keperluan Kementerian;

iii. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO untuk tindakan;

iv. Memastikan penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KDN dilaksanakan;

v. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai Pentadbir Sistem ICT (*sysadmin*) yang berhenti, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas; dan

vi. Menandatangani `Surat Akuan Pematuhan' bagi mematuhi Dasar Keselamatan ICT (Lampiran A).

DKICTKDN-020404

(d) **Pentadbir Sistem ICT**

Peranan dan tanggungjawab adalah termasuk seperti berikut :

i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT KDN;

ii. Menjaga kerahsiaan kata laluan (*password*);

iii. Menjaga kerahsiaan konfigurasi aset ICT;

iv. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai semua pengguna ICT KDN yang digantung kerja, berhenti, bersara, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas;

v. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna luar dan pihak ketiga yang berhenti atau tamat projek;

vi. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan dasar pemilik sumber maklumat sebagaimana yang telah ditetapkan;

vii. Memantau aktiviti capaian harian pengguna;

viii. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran; membatalkan atau memberhentikannya dengan serta merta; dan memaklumkan kepada ICTSO dan Setiausaha Bahagian Pengurusan ICT untuk tindakan selanjutnya;

ix. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala;

x. Menyimpan dan menganalisis rekod jejak audit (*log file(s)*); dan

xi. Menandatangani `Surat Akuan Pematuhan' bagi mematuhi Dasar Keselamatan ICT (Lampiran A).

DKICTKDN-020405

(e) **Pengguna Dalaman**

Peranan dan tanggungjawab adalah termasuk seperti berikut:

i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT KDN;

ii. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;

iii. Menjaga kerahsiaan maklumat Kerajaan yang meliputi maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran,

penyampaian, pertukaran dan pemusnahan;

iv. Menjaga kerahsiaan kata laluan (*password*);

v. Memastikan maklumat berkaitan adalah tepat dan lengkap dari masa ke semasa;

vi. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum;

vii. Menghadiri program-program kesedaran dan pembudayaan mengenai keselamatan ICT; dan

viii. Menandatangani `Surat Akuan Pematuhan' bagi mematuhi Dasar Keselamatan ICT (Lampiran A).

DKICTKDN-0205 Keselamatan Maklumat Dalam Pengurusan Projek

Seksyen ini bertujuan untuk memastikan setiap pengurusan projek yang dilaksanakan oleh KDN dan Jabatan di bawahnya mengambilkira aspek keselamatan maklumat secara holistik.

Setiausaha Bahagian / Ketua Bahagian KDN adalah bertanggungjawab untuk :

(a) Menjadikan objektif keselamaan maklumat sebahagian daripada objektif projek;

(b) Melaksanakan penilaian terhadap risiko keselamatan maklumat difasa awal (pada permulaan fasa) perlaksanaan projek sebelum kawalan keselamatan yang berkaitan dikenalpasti;

(c) Menjadikan isu keselamatan maklumat sebagai agenda dalam setiap fasa kaedah perlaksanaan projek;

(d) Memastikan pengurusan projek mematuhi manual keselamatan dan polisi DKICT dalam setiap aktiviti pengurusan projek;

(e) Memastikan pengurus projek telah mendapat latihan kesedaran dan pendedahan yang mencukupi berkenaan tanggungjawab untuk memastikan keselamatan maklumat sentiasa terjamin;

(f) Memastikan aktiviti bagi menjamin keselamatan maklumat dinyatakan secara jelas dalam jadual perancangan perlaksanaan projek;

(g) Memastikan semua pihak yang terlibat dalam sesuatu projek maklum tentang arahan berkaitan keselamatan maklumat dan mereka diikat dengan perjanjian (seperti Akta Rahsia Rasmi).

DKICTKDN-0206 Polisi Keselamatan Maklumat Berkaitan Hubungan Pembekal

Seksyen ini menjelaskan keperluan untuk mendokumentasikan strategi mitigasi risiko keselamatan maklumat bilamana pembekal dibenarkan untuk akses ke aset KDN.

Setiausaha Bahagian / Ketua Bahagian KDN adalah bertanggungjawab untuk :

(a) Mengenalpasti dan mendokumenkan jenis-jenis pembekal (seperti khidmat servis IT, pembekal infrastruktur IT, logstik, keewangan dsb.);

(b) Mengenalpasti jenis aset maklumat yang dibenarkan untuk diakses oleh pembekal serta melakukan pemantauan dan pengawalan terhadap aset tersebut secara berterusan;

(c) Mengadakan latihan kesedaran kepada semua pihak yang terlibat (KDN dan pembekal) untuk mendedahkan mereka dengan polisi, proses, dan prosidur berkaitan keselamatan maklumat.

(d) Mewujudkan mekanisma/proses pengurusan pembekal dengan mengambil kira aspek keselamatan maklumat sebagai teras;

(e) Memastikan pemantauan berterusan dilakukan terhadap semua pembekal dengan melaksanakan pengukuran prestasi dan pematuhan terhadap garis panduan keselamatan maklumat. Proses dan prosidur berkaitan perlu diwujudkan;

(f) Mewujudkan kontrak rasmi bersama pembekal yang dapat menjamin keselamatan maklumat KDN disamping segala urusan bersama pembekal hendaklah dilaksanakan secara rasmi;

(g) Memastikan pihak pembekal mewujudkan Pelan Kesinambungan Perkhidmatan dan Rancangan Pemulihan Bencana mereka khususnya jika pembekal menyediakan khidmat yang kritikal kepada KDN;

(h) Mewujudkan perjanjian yang jelas agar pihak pembekal memastikan keselamatan maklumat yang digunakan terjamin sepanjang akses dibenarkan dan seterusnya memulangkan kembali semua asset maklumat sekiranya kontrak mereka tamat atau ditamatkan.

DKICTKDN-0207 Rangkaian Pembekal ICT

Seksyen ini menjelaskan kandungan perjanjian bersama pembekal yang perlu diwujudkan bagi memastikan risiko keselamatan maklumat berkaitan rangkaian pembekal khidmat ICT dan produk diambil kira.

Setiausaha Bahagian / Ketua Bahagian KDN adalah bertanggungjawab untuk :

(a) Mengenalpasti keperluan keselmatan maklumat khusus berkaitan dengan perolehan rangkaian pembekal servis ICT dan produk sebagai tambahan kepada keperluan umum keselamatan maklumat berkaitan hubungan pembekal yang telah dikenal pasti;

(b) Memastikan rangkain pembekal yang terlibat dalam menyediakan khidmat servis ICT berkongsi hal berkaitan keselamatan maklumat (polisi, prosidur, proses) kepada setiap aras pembekal termasuk sub-pembekal atau sub-sub-pembekal;

(c) Khusus untuk rangkaian pembekal produk, KDN perlu memastikan pembekal utama berkongsi praktis pembangunan produk KDN dikesemua peringkat pembekal bagi memastikan keselamatan maklumat terjamin;

(d) Melaksanakan proses pemantauan rangkaian pembekal servis ICT dan produk dengan kaedah yang berkesan bagi menjamin keperluan keselamatan maklumat sentiasa dipatuhi;

(e) Mendapatkan jaminan bahawa komponen produk yang kritikal boleh berfungsi mengikut spesifikasi dan dikesan sumbernya dari rangkaian pembekal yang pelbagai;

(f) Mewujudkan peraturan yang khusus bagi mengawal perkongsian maklumat dikalangan rangkain pembekal;

(g) Mewujudkan mekanisma/proses khusus untuk mengurus rangkaian pembekal khidmat servis ICT dan produk bagi memastikan keselamatan maklumat terjamin. Mekanisma yang diwujudkan wajar mampu untuk mengurus risiko sekiranya komponen produk yang dibekalkan tidak lagi boleh dibekalkan kerana perubahan trend dan teknologi yang berlaku.

PERKARA 03 : PENGURUSAN ASET ICT

Huraian :	Setiap aset ICT perlu dikenal pasti, dikelaskan, direkodkan ke dalam sistem inventori, didokumenkan, diselenggarakan dan dilupuskan apabila tiba masanya.
Objektif :	Untuk memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT KDN.

DKICTKDN-0301 Pengurusan Aset ICT

Adalah menjadi tanggungjawab Ketua Setiausaha / Ketua Jabatan untuk mengurus aset ICT di bawah kawalannya.

DKICTKDN-0302 Tanggungjawab Ke Atas Aset ICT

Seksyen ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.

Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut:

(a) Memastikan semua aset ICT dikenal pasti dan maklumat aset ICT di rekod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini dalam Sistem Pengurusan Aset;

(b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan

(c) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan;

(d) Memastikan pengurusan aset ICT yang meliputi penyelenggaraan dan pelupusan hendaklah mematuhi peraturan yang telah ditetapkan.

DKICTKDN-0303 Pengelasan Maklumat

Seksyen ini bertujuan memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan tahap kerahsiaan terutamanya melibatkan dokumen terperingkat seperti Terhad, Sulit, Rahsia dan Rahsia Besar (Akta Rahsia Rasmi – Akta 88).

Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada KDN.

DKICTKDN-0304 Pelabelan Dan Pengendalian Maklumat

Pelabelan dan pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengikut standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. Antara langkah-langkah keselamatan yang perlu diambil kira adalah seperti berikut :

(a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

(b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari masa ke semasa;

(c) Menentukan maklumat sedia untuk digunakan;

(d) Menjaga kerahsiaan kata laluan (*password*);

(e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

(f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan; dan

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

PERKARA 04 KESELAMATAN SUMBER MANUSIA

Huraian :	Semua peranan dan tanggungjawab warga KDN, pembekal, pakar runding dan pihak-pihak lain hendaklah jelas dan didokumenkan mengikut keperluan Dasar Keselamatan ICT KDN.
Objektif :	Untuk memastikan semua sumber manusia yang terlibat warga KDN, pembekal, pakar runding dan pihak-pihak lain yang terlibat memahami tanggungjawab dan peranan mereka dalam keselamatan Aset ICT KDN.

DKICTKDN-0401 Keselamatan Sumber Manusia

Ketua Setiausaha / Ketua Jabatan adalah bertanggungjawab ke atas sumber manusia yang terlibat secara langsung atau tidak langsung dalam pengendalian aset ICT di bawah kawalannya.

DKICTKDN-0402 Sebelum Berkhidmat

Seksyen ini bertujuan memastikan warga KDN, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT KDN.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut :

(a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga KDN, pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;

(b) Menjalankan tapisan keselamatan untuk warga KDN, pembekal, pakar runding dan pihak-pihak lain yang terlibat selaras dengan keperluan perkhidmatan; dan

(c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

DKICTKDN-0403 Dalam Perkhidmatan

Seksyen ini bertujuan memastikan warga KDN, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong Dasar Keselamatan ICT KDN serta meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut :

(a) Memastikan warga KDN, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh KDN;

(b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada warga KDN, dan sekiranya perlu diberi kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari masa ke semasa; dan

(c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga KDN, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sekiranya berlaku perlanggaran dasar dengan perundangan dan peraturan ditetapkan KDN.

DKICTKDN-0404 Bertukar Atau Tamat Perkhidmatan

Seksyen ini bertujuan memastikan pertukaran atau tamat perkhidmatan warga KDN, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan diurus dengan teratur.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut :

(a) Memastikan semua aset ICT dikembalikan kepada KDN mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

(b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan KDN dan/atau terma perkhidmatan.

DKICTKDN-0405 Program Kesedaran, Pembudayaan Dan Latihan Keselamatan ICT

Setiap pengguna perlu diberikan kesedaran, latihan atau kursus mengenai keselamatan ICT yang bersesuaian dengan peranan dan tanggungjawab masing-masing secara berterusan.

Program menangani insiden juga penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT KDN dan Kerajaan.

PERKARA 05 : KESELAMATAN FIZIKAL DAN PERSEKITARAN

Huraian :	Premis dan peralatan memproses maklumat yang kritikal dan sensitif hendaklah ditempatkan di kawasan yang selamat dan dilindungi dari sebarang ancaman fizikal dan persekitaran.
Objektif :	Untuk menghalang capaian yang tidak dibenarkan, kerosakan dan gangguan terhadap persekitaran premis, peralatan dan maklumat.

DKICTKDN-0501 Keselamatan Fizikal Dan Persekitaran

Ketua Setiausaha / Ketua Jabatan adalah bertanggungjawab untuk mengesan, mencegah dan menghalang pencerobohan ke atas kawasan yang menempatkan peralatan, simpanan maklumat dan kemudahan pemprosesan maklumat yang boleh mengakibatkan kecurian, kerosakan dan gangguan kepada premis serta maklumat.

DKICTKDN-0502 Kawalan Kawasan Terhad

Seksyen ini bertujuan untuk memberi garis panduan langkah-langkah yang perlu dilakukan untuk menghalang capaian yang tidak sah, kecurian, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat KDN. Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut :

(a) Menggunakan keselamatan *perimeter* (halangan seperti dinding, pagar kawalan yang melibatkan biometrik, kad pintar, *scanner gateway, hand-held device metal detector*, RFID dsb.), pengawal keselamatan, alat pengawasan CCTV, alat penggera) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;

(b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;

(c) Mereka bentuk dan melaksanakan keselamatan fizikal khas untuk pelawat-pelawat seperti kaunter pelawat di dalam pejabat, bilik dan kemudahan;

(d) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam (*natural disaster*);

(e) Melaksana perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan

(f) Memastikan kawasan-kawasan penghantaran dan pemunggahan dimasuki oleh pihak yang diberi kebenaran sahaja.

DKICTKDN-0503 Keselamatan Peralatan

Seksyen ini bertujuan untuk memberi garis panduan langkah-langkah yang perlu dilakukan untuk menghalang dari berlaku sebarang kehilangan, kerosakan, kecurian atau kompromi ke atas aset ICT dan gangguan ke atas sistem penyampaian perkhidmatan KDN.

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut :

(a) **Perkakasan**

i. Menempatkan dan mengawal perkakasan ICT supaya risiko ancaman dan bencana dari persekitaran serta percubaan menceroboh sentiasa pada tahap minimum; dan

ii. Semua cadangan pengubahsuaian, pembelian, penempatan dan pemindahan peralatan-peralatan ICT hendaklah dirujuk terlebih dahulu kepada CIO.

(b) **Dokumen**

Bagi memastikan integriti, kerahsiaan dan kebolehsediaan maklumat serta pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi :

i. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin;

ii. Menggunakan tanda atau label keselamatan seperti **Rahsia besar**, **Rahsia**, **Sulit** atau **Terhad** pada dokumen;

iii. Satu sistem pengurusan dokumen terperingkat hendaklah diwujudkan bagi menerima, memproses, menyimpan dan menghantar dokumen-dokumen tersebut supaya ianya diuruskan berasingan daripada dokumen-dokumen tidak terperingkat; dan

iv. Menggunakan kaedah enkripsi (*encryption*) ke atas dokumen terperingkat yang disediakan dan dihantar secara elektronik (samada bentuk *softcopy*, e-mel atau *sms*).

(c) **Media Storan** (disket, pita magnetik, cakera keras, CD-ROM, *optical disk, flash disk,* storan atas talian dan lain-lain)

Keselamatan media storan perlu diberi perhatian khusus kerana ia berupaya menyimpan maklumat rasmi dan rahsia rasmi KDN dan Kerajaan.

Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat :

i. Menyediakan ruang penyimpanan dan peti keselamatan (*secured container*) yang mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;

ii. Menghadkan akses kepada pengguna yang dibenarkan sahaja;

iii. Sebarang pelupusan hendaklah merujuk kepada tatacara pelupusan (Pekeliling

Perbendaharaan dan MAMPU); dan

iv. Mengadakan sistem pengurusan media termasuk inventori, pergerakan, pelabelan dan *backup / restore*.

DKICTKDN-0504 Prasarana Sokongan

(a) **Kawalan Persekitaran**

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT KDN, semua cadangan perolehan dan pengubahsuaian fizikal hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Perkara yang perlu dipatuhi adalah seperti berikut :

i. Merancang dan menyediakan pelan keseluruhan pusat data termasuk ruang peralatan komputer, ruang percetakan dan ruang atur pejabat;

ii. Melengkapi semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;

iii. Memasang peralatan perlindungan di tempat yang bersesuaian, mudah dikenali dan dikendalikan;

iv. Menyimpan bahan mudah terbakar di luar kawasan kemudahan penyimpanan aset ICT;

v. Meletakkan semua bahan cecair di tempat yang bersesuaian dan berjauhan dari aset ICT;

vi. Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran perkakasan komputer; dan

vii. Menyemak dan menguji semua infrastruktur sokongan sekurang-kurangnya satu (1) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.

(b) **Bekalan Kuasa**

i. Melindungi semua peralatan ICT KDN dari kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai kepada peralatan ICT;

ii. Menggunakan peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan; dan

iii. Menyemak dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.

(c) **Utiliti**

i. Semua kemudahan utiliti seperti penghawa dingin, bekalan air, kumbahan dan pengalihan udara perlu dilindungi dari kegagalan bekalan elektrik dan sebarang gangguan; dan

ii. Kemudahan utiliti perlu diperiksa dan diuji agar sentiasa berfungsi dengan baik bagi mengurangkan risiko kegagalan;

(d) **Prosedur Kecemasan**

i. Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan oleh KSU atau Pegawai Keselamatan Kementerian;

ii. Melaporkan insiden kecemasan persekitaran seperti kebakaran kepada Pegawai Keselamatan KDN;

iii. Mewujudkan, menguji dan mengemas kini pelan kecemasan dari masa ke semasa; dan

iv. Mengadakan latihan *fire drill* mengikut jadual secara berkala.

(e) **Keselamatan Kabel**

Kabel elektrik dan telekomunikasi yang menyalurkan data atau menyokong sistem penyampaian perkhidmatan hendaklah dilindungi daripada pencerobohan dan kerosakan.

Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut :

i. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;

ii. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;

iii. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan

iv. Membuat pelabelan kabel menggunakan kod tertentu.

DKICTKDN-0505 Penyelenggaraan Peralatan

Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.

Langkah-langkah keselamatan yang perlu diambil tetapi tidak hanya terhad kepada perkara-perkara berikut :

(a) Mematuhi spesifikasi yang ditetapkan oleh pihak prinsipal bagi semua perkakasan yang diselenggara;

(b) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;

(c) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan

(d) Memaklumkan kepada pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

DKICTKDN-0506 Peminjaman Peralatan ICT Untuk Kegunaan Di Luar Pejabat

Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko.

Langkah-langkah keselamatan yang perlu diambil tetapi tidak hanya terhad kepada perkara berikut :

(a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh Kementerian bagi membawa keluar peralatan, perisian atau maklumat tertakluk kepada tujuan yang dibenarkan;

(b) Melindungi dan mengawal peralatan sepanjang masa;

(c) Merekodkan aktiviti peminjaman dan pemulangan peralatan mengikut peraturan yang telah ditetapkan; dan

(d) Menyemak peralatan yang dipulangkan berada dalam keadaan baik.

DKICTKDN-0507 Pengendalian Peralatan ICT Luar Yang Dibawa Masuk / Keluar

Bagi peralatan yang dibawa masuk ke premis KDN atau Kerajaan, langkah keselamatan yang perlu diambil adalah seperti berikut :

(a) Memastikan peralatan yang dibawa masuk tidak mengancam keselamatan ICT KDN;

(b) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh Kementerian bagi membawa masuk / keluar peralatan; dan

(c) Menyemak peralatan yang dibawa keluar tidak mengandungi maklumat KDN terutamanya maklumat terperingkat.

DKICTKDN-0508 Pelupusan Peralatan ICT

(a) Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Kerajaan.

(b) Menghapuskan semua kandungan peralatan mengikut peraturan yang ditetapkan khususnya maklumat rahsia rasmi terlebih dahulu sama ada melalui *shredding, grinding, degauzing* atau pembakaran sebelum pelupusan;

(c) Membuat penduaan bagi maklumat yang hendak disimpan sekiranya diperlukan sebelum pelupusan.

(d) Rujuk Surat Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan" untuk maklumat lanjut.

DKICTKDN-0509 *Clear Desk* dan *Clear Screen*

Prosedur *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan salah guna, kerosakan, kecurian atau kehilangan.

Langkah-langkah keselamatan yang perlu diambil tetapi tidak hanya terhad kepada perkara berikut :

(a) Menggunakan kemudahan *password screen saver* atau *logout domain controller* apabila meninggalkan komputer;

(b) Menyimpan bahan-bahan sensitif di dalam laci, kabinet fail dan bilik yang berkunci;

(c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat; dan

(d) Memastikan semua dokumen yang terdapat dalam memori pencetak, pengimbas, mesin faksimile, mesin fotostat dan *mobile devices* dipadam.

PERKARA 06 : PENGURUSAN OPERASI DAN KOMUNIKASI

Huraian :	Prosedur pengurusan operasi dan komunikasi hendaklah didokumenkan, diselenggarakan dan mudah didapati apabila diperlukan.
Objektif :	Untuk memastikan kemudahan pemprosesan maklumat dan komunikasi sentiasa berfungsi dengan baik dan selamat dari sebarang ancaman atau gangguan.

DKICTKDN-0601 Pengurusan Operasi Dan Komunikasi

Adalah menjadi tanggungjawab Ketua Setiausaha / Ketua Jabatan untuk memastikan kesemua kemudahan pemprosesan maklumat adalah terjamin selamat dan berjalan lancar.

DKICTKDN-0602 Tanggungjawab Dan Prosedur Operasi

Seksyen ini bertujuan memastikan kemudahan pemprosesan maklumat beroperasi seperti yang ditetapkan.

Perkara-perkara yang mesti dipatuhi tetapi tidak hanya terhad kepada yang berikut :

(a) Semua prosedur operasi hendaklah didokumenkan dengan jelas lagi teratur, dikemas kini dan sedia diguna pakai oleh pengguna mengikut keperluan;

(b) Setiap perubahan kepada sistem dan kemudahan pemprosesan maklumat mestilah dikawal;

(c) Tugas dan tanggungjawab perlu diasingkan bagi mengurangkan risiko kecuaian dan penyalahgunaan aset Kementerian; dan

(d) Kemudahan ICT untuk pembangunan, pengujian dan operasi mestilah diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah ke atas sistem yang sedang beroperasi.

DKICTKDN-0603 Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak-Pihak Lain Yang Terlibat

Seksyen ini bertujuan memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal, pakar runding dan pihak-pihak lain yang terlibat.

Perkara-perkara yang mesti dipatuhi tetapi tidak hanya terhad kepada yang berikut :

(a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat;

(b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari masa ke semasa; dan

(c) Pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyelenggara dan menambah baik dasar keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.

DKICTKDN-0604 Perancangan Dan Penerimaan Sistem

Seksyen ini bertujuan untuk mengurangkan risiko kegagalan sistem.

Perkara-perkara yang mesti dipatuhi tetapi tidak hanya terhad kepada yang berikut :

(a) Penggunaan peralatan dan sistem mestilah dipantau, ditala (*tuned*) dan perancangan perlu dibuat bagi memenuhi keperluan kapasiti akan datang untuk memastikan prestasi sistem di tahap optimum; dan

(b) Kriteria penerimaan untuk peralatan dan sistem baru, peningkatan dan versi baru perlu ditetapkan dan ujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem.

DKICTKDN-0605 Perlindungan Dari *Malicious* Dan *Mobile Code*

Seksyen ini bertujuan untuk melindungi integriti maklumat dan perisian dari ancaman *malicious code* seperti *viruses, worms, trojan horses, logic bombs* dan sebagainya.

Perkara-perkara yang mesti dipatuhi tetapi tidak hanya terhad kepada yang berikut :

(a) Kawalan pencegahan, pengesanan dan pemulihan untuk melindungi daripada *malicious code*;

(b) Dalam keadaan di mana *mobile code* dibenarkan, konfigurasinya hendaklah memastikan bahawa ia beroperasi berdasarkan kepada dasar keselamatan yang jelas dan penggunaan *mobile code* yang tidak dibenarkan adalah dilarang sama sekali;

(c) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System (IDS)* dan Intrusion Protection System (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;

(d) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; dan

(e) Mengemas kini anti virus dengan *pattern* anti virus yang terkini.

DKICTKDN-0606 Penduaan (*Backup*)

Seksyen ini bertujuan untuk mengekalkan integriti, kesediaan maklumat dan kemudahan pemprosesan maklumat.

Perkara-perkara yang mesti dipatuhi tetapi tidak hanya terhad kepada yang berikut :

(a) Membuat dan menguji secara berkala *backup* maklumat dan perisian berdasarkan prosedur *backup;*

(b) Membuat *backup* ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;

(c) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat;

(d) Menguji sistem *backup* dan prosedur restore sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya waktu kecemasan;

(e) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan

(f) Merekod dan menyimpan salinan *backup*.

DKICTKDN-0607 Pengurusan Keselamatan Rangkaian

Seksyen ini bertujuan untuk memastikan perlindungan keselamatan maklumat dalam rangkaian serta infrastruktur sokongan. Perkara-perkara yang mesti dipatuhi tetapi tidak hanya terhad kepada yang berikut :

(a) Rangkaian perlu dikawal, dipantau dan diurus sebaiknya, bertujuan untuk mengawal daripada sebarang ancaman bagi menjamin keselamatan sistem dan aplikasi yang menggunakan rangkaian, termasuk maklumat yang dipindahkan melaluinya;

(b) Ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian perlu dikenal pasti dan dimasukkan dalam mana-mana perjanjian perkhidmatan rangkaian sama ada perkhidmatan berkenaan disediakan secara dalaman atau melalui khidmat luar;

(c) Tanggunjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibernarkan;

(d) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;

(e) *Firewall* hendaklah dipasang serta dikonfigurasi serta diselia oleh pentadbir rangkaian;

(f) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;

(g) Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat KDN;

(h) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;

(i) Sebarang penyambungan rangkaian yang bukan di bawah kawalan KDN adalah tidak dibenarkan;

(j) Semua pengguna hanya dibenarkan menggunakan rangkaian KDN/jabatan sahaja dan penggunaan modem adalah dilarang sama sekali; dan

(k) Kemudahan bagi wireless LAN perlu dipastikan kawalan keselamatan.

DKICTKDN-0608 Pemantauan Rangkaian Berpusat

Seksyen ini bertujuan untuk memastikan pemantauan rangkaian berpusat kerajaan dapat berfungsi secara berkesan dan berterusan.

Perkara-perkara yang mesti dipatuhi tetapi tidak hanya terhad kepada yang berikut :

(a) KDN hendaklah memastikan pemantauan yang dilaksanakan oleh Pemantauan Rangkaian Infrastruktur ICT Sektor Awam Malaysia (PRISMA), MAMPU ke atas rangkaian KDN dapat berfungsi secara berkesan dan berterusan;

(b) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;

(c) Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; dan

(d) Semua trafik keluar dan masuk hendaklah melalui firewall di bawah kawalan KDN/jabatan.

DKICTKDN-0609 Pengendalian Media

Seksyen ini bertujuan untuk memastikan tidak berlaku pendedahan, pengubahsuaian, peralihan atau pemusnahan media secara tidak sah, yang boleh mengganggu aktiviti perkhidmatan.

Perkara-perkara yang mesti dipatuhi tetapi tidak hanya terhad kepada yang berikut :

(a) Prosedur perlu disediakan untuk pengurusan media mudah alih;

(b) Media yang tidak digunakan perlu dilupuskan secara selamat mengikut prosedur yang telah ditetapkan;

(c) Prosedur untuk mengendali dan menyimpan media perlu diwujudkan untuk melindunginya daripada didedah tanpa kebenaran atau disalah guna;

(d) Dokumentasi sistem perlu dilindungi dari capaian yang tidak dibenarkan;

(e) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;

(f) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;

(g) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; dan

(h) Menyimpan semua media di tempat yang selamat.

DKICTKDN-0610 Pertukaran Maklumat

Seksyen ini bertujuan untuk memastikan keselamatan pertukaran maklumat dan perisian dalam KDN dan mana-mana entiti luar terjamin.

Perkara-perkara yang mesti dipatuhi tetapi tidak hanya terhad kepada yang berikut :

(a) Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;

(b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara KDN dengan pihak luar;

(c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KDN;

(d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan

(e) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat KDN.

DKICTKDN-0611 Perkhidmatan Perdagangan Elektronik

Seksyen ini bertujuan untuk memastikan keselamatan perkhidmatan perdagangan elektronik (e-dagang) dan penggunaannya.

Perkara yang mesti dipatuhi tetapi tidak hanya terhad kepada yang berikut :

(a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;

(b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan

(c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.

DKICTKDN-0612 Pemantauan Aktiviti Pemprosesan Maklumat

Seksyen ini bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

Perkara yang mesti dipatuhi tetapi tidak hanya terhad kepada yang berikut :

Pengauditan dan Forensik ICT

ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut:

(a) Sebarang percubaan pencerobohan kepada sistem ICT KDN/jabatan;

(b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*Denial Of Service*), spam, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*);

(c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;

(d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;

(e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;

(f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (bandwidth) rangkaian;

(g) Aktiviti penyalahgunaan akaun emel; dan

(h) Aktiviti penukaran alamat IP (IP Address) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian.

Jejak Audit

Setiap sistem mestilah mempunyai jejak audit (Audit Trail). Jejak Audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.

Jejak audit hendaklah mengandungi maklumat-maklumat berikut:

(a) Rekod setiap aktiviti transaksi;

(b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;

(c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan

(d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

Jejak audit hendaklah disimpan utnuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara.

Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.

Sistem Log

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:

(a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;

(b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan

(c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.

Pemantauan Log

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) *Log Audit* yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;

(b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala;

(c) Maklumat log perlu direkodkan dan dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;

(d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;

(e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan

(f) Masa yang berkaitan dengan sistem pemprosesan maklumat dalam KDN atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.

DKICTKDN-0613 Keselamatan Komunikasi : Internet

(a) Hak akses menggunakan perkhidmatan internet KDN hendaklah dilihat sebagai satu kemudahan yang disediakan oleh KDN untuk membantu melicinkan pentadbiran atau

memperbaiki perkhidmatan yang disediakan. Pengguna harus mengambil maklum bahawa semua aset ICT di bawah kawalannya (termasuk maklumat) adalah **Hak Milik Kerajaan**. Oleh yang demikian, pengguna perlu mengakses atau *logon* menerusi kawalan pengguna (*Active Directory)* untuk pengesahan pengguna;

(b) Laman web yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan. Kategori laman yang **ditegah** capaian adalah seperti berikut:

i. *Pornography & Nudity*;
ii. *Adult & Mature Content*;
iii. *Gay & Lesbian*;
iv. *Games*;
v. *Gambling*;
vi. *Chat, Instant Messaging & Social Networking*;
vii. *Spam URLs*; dan
viii. *Spyware*.

Kecuali atas sebab-sebab kerja, kajian dan penyelidikan yang dibenarkan oleh Ketua Setiausaha / Ketua Jabatan. Pihak Bahagian Pengurusan Teknologi Maklumat (Bahagian IT) akan membuka laman web / portal yang diluluskan mengikut kaedah *whitelist*.

(c) Bahan yang diperolehi dari Internet hendaklah ditentukan **ketepatan** dan **kesahihannya**. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan;

(d) Bahan rasmi hendaklah **disemak** dan **mendapat pengesahan** daripada Ketua Setiausaha / Ketua Jabatan atau pegawai yang diberi kuasa sebelum dimuat naik ke Internet;

(e) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar, sumber terbuka (OSS) dan di bawah **Hak Cipta Terpelihara**. Pengguna adalah dilarang memuat naik, memuat turun, menyimpan dan menggunakan **perisian yang tidak sah** (***pirated software***);

(f) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan **yang dibenarkan** oleh KDN;

(g) Pengguna adalah dilarang menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan, imej atau bahan-bahan yang mengandungi unsur-unsur **lucah**;

(h) Pengguna adalah dilarang menyedia, memuat naik, memuat turun dan menyimpan maklumat Internet yang melibatkan sebarang pernyataan **fitnah** atau **hasutan** yang boleh memburuk dan menjatuhkan imej Kerajaan serta orang awam;

(i) Pengguna adalah dilarang memuat naik, memuat turun dan menyimpan gambar atau teks yang bercorak **penentangan** yang boleh membawa keadaan **huru-hara** dan **menakutkan** pengguna Internet yang lain;

(j) Pengguna adalah dilarang memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan atas talian (***streaming***) seperti permainan elektronik, video dan lagu. Ia boleh mengakibatkan kelembapan perkhidmatan dan operasi sistem rangkaian komputer (melibatkan penggunaan ***bandwitdh*** yang tinggi);

(k) Pengguna adalah dilarang menyebarkan maklumat rasmi dengan menggunakan kemudahan ***chatting*** atau ***instant messaging***

(l) Pengguna adalah dilarang menggunakan kemudahan Internet untuk tujuan peribadi seperti laman web ***blog*** individu;

(m) Pengguna adalah dilarang menjalankan aktiviti-aktiviti komersial seperti **jualan langsung, skim pelaburan internet, politik dan sebagainya**;

(n) Pengguna adalah dilarang melakukan aktiviti **jenayah** seperti menyebarkan bahan yang membabitkan **perjudian**, **senjata**, **aktiviti pengganas dan sebagainya** yang boleh mengancam kepada kesejahteraan dan ketenteraman awam;

(o) Pengguna yang diberi kebenaran untuk memuat naik, memuat turun, menghantar (***file-transfer-protocol***) dan menyimpan kad elektronik, video, lagu dan kepilan fail hendaklah tidak melebihi saiz **lima (5) megabait.**

(p) Pengguna adalah dilarang menggunakan kemudahan **modem peribadi**, ***streamyx*** dan ***access point*** *(**wireless**)* untuk membuat capaian terus ke Internet kecuali setelah mendapat kebenaran daripada Ketua Setiausaha / Ketua Jabatan atau pegawai yang diberi kuasa;

(q) Pengguna tidak boleh membiarkan komputer berada **atas talian (*on-line*)** jika tidak digunakan. *Log off* komputer sebelum keluar pejabat supaya tidak disalah gunakan oleh mana-mana pihak;

(r) Mana-mana pengguna termasuk pihak luar adalah dilarang menggunakan sebarang peralatan komputer membabitkan **storan luar** untuk tujuan muat turun/naik maklumat internet seperti *thumb*/*pen drive*, *disket*, *CDRW*, *DVD writetable* dan *external hard disk* sebelum diimbas terlebih dahulu dengan sebarang produk *anti-malware* (*virus, worms, trojan backdoor, spyware* dsb.) bagi mengelakkan *malware outbreak* di rangkaian KDN dan berlaku insiden keselamatan ICT; dan

(s) Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada **Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003** bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.

DKICTKDN-0614 Keselamatan Komunikasi: Mel Elektronik / E-mel

(a) Pemilikan akaun e-mel rasmi bukanlah hak mutlak seseorang. Ia adalah kemudahan yang tertakluk kepada peraturan **KDN**, **Kerajaan** dan **undang-undang siber Negara** dan boleh ditarik balik jika penggunaannya melanggar peraturan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

(b) Setiap e-mel yang disediakan hendaklah **mematuhi format** yang telah ditetapkan oleh jabatan. Penggunaan huruf besar dan warna yang tidak sesuai dalam kandungan e-mel adalah tidak digalakkan dan dianggap tidak beretika. Sebaik-baiknya, gabungan huruf besar dan huruf kecil digunakan dan dipraktikkan di tempat-tempat yang bersesuaian di samping mengamalkan penggunaan bahasa yang betul, ringkas dan sopan;

(c) **Kata laluan** (*password*) **perlu dikawal** untuk mengelakkan daripada diketahui oleh orang yang tidak diberi kuasa menggunakannya:

i. Kata laluan tidak boleh dicatat di atas kertas;
ii. Gunakan atau setkan kata laluan yang kukuh melalui gabungan nombor, huruf, tanda dan simbol (contoh : **P4s$w0rcl**);
iii. Kata laluan perlu ditukar sekurang-kurangnya setiap tiga (3) bulan sekali; dan
iv. Kata laluan tidak boleh dikongsikan kepada orang lain.

(d) Memastikan **subjek** dan **kandungan e-mel** adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;

(e) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul. Penghantar boleh menggunakan kemudahan **'salinan kepada' (*cc*)** sekiranya e-mel tersebut perlu dimaklumkan kepada penerima lain. Bagaimanapun, penggunaan ***'blind cc (bcc)'*** tidak digalakkan.

(f) Kemudahan *reply* digunakan untuk menjawab e-mel kepada penghantar asal dan *forward* untuk memanjangkan e-mel atau dimajukan kepada penerima lain. Sebagai amalan baik, e-mel penghantar hendaklah dijawab **selewat-lewatnya tiga (3) hari** dari tarikh e-mel berkenaan diterima. Kemudahan penghantaran e-mel jawab automatik (*auto reply*) semasa berada di luar pejabat bagi tempoh waktu yang panjang telah pun disediakan oleh Kementerian.

(g) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi **sepuluh (10) megabait** semasa penghantaran dan penerimaan. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan (contoh : fail ***.zip**);

(h) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui seperti e-mel ***SPAM*** atau ***junkmail***. Pengguna adalah dilarang untuk membuka, menjawab atau memberi maklum balas kepada e-mel berkenaan;

(i) Setiap pengguna perlu mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan komunikasi dan transaksi maklumat melalui e-mel bagi mengelakkan penyamaran (***spoofing***). Pengguna adalah dilarang untuk menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah. Ini bertujuan untuk melindungi maklumat Kerajaan daripada sebarang bentuk penyalahgunaan;

(j) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan. Pengguna hendaklah memastikan jumlah e-mel yang disimpan di dalam kotak masuk (*inbox*) *server* e-mel adalah tidak melebihi **lima ratus (500)** megabait dan mengutamakan

penyimpanan e-mel yang perlu sahaja. Saiz mailbox untuk **pegawai peringkat pengurusan tertinggi** adalah *unlimited.* Penyimpanan salinan e-mel pada komputer masing-masing adalah digalakkan bagi tujuan keselamatan dan penjimatan ruang penyimpanan di *server* e-mel serta memudahkan kerja-kerja *house-keeping* e-mel arkib;

(k) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi hendaklah dihapuskan (*delete*). Pengguna perlu menghapuskan atau memuat turun semua e-mel bertempoh **tiga (3) bulan** ke komputer masing-masing;

(l) Semua warga KDN adalah layak mendapat akaun emel sesuai dengan jawatan dan mengikut prosedur semasa. Setiap pengguna bertanggungjawab terhadap akaun yang telah diberikan. Sebarang perubahan status penggunaan (bertukar keluar atau berhenti) hendaklah dimaklumkan kepada Pentadbir e-mel;

(m) Tempoh penyimpanan e-mel di dalam *server* e-mel adalah dihadkan kepada **empat belas (14) hari** atau **dua (2) minggu** selepas seseorang kakitangan bertukar ke agensi lain atau berhenti berkhidmat;

(n) **Kriptografi** atau penyulitan mesti dilakukan ke atas semua e-mel rahsia rasmi (Rahsia Besar, Rahsia dan Sulit) termasuk lampiran dokumen yang dihantar, diterima dan disimpan;

(o) Penggunaan percuma *web-based mail* (yahoo mail, gmail, waumail dsb.) untuk kegunaan rasmi adalah dilarang sama sekali tetapi dibenarkan untuk tujuan bukan rasmi seperti aktiviti ***subscription***;

(p) Pengguna adalah dilarang menggunakan e-mel untuk tujuan **komersial** (seperti jualan langsung) atau **politik**;

(q) Pengguna adalah dilarang menghantar dan memiliki bahan-bahan yang salah di sisi undang-undang seperti bahan **lucah**, **perjudian** dan **jenayah**;

(r) Pengguna adalah dilarang menghantar e-mel atau memanjangkan e-mel (***forwarded e-mail***) yang tidak rasmi atau pun yang tiada kena-mengena dengan urusan kerja rasmi kepada akaun **warga_kdn@moha.gov.my** kerana penerimanya juga di kalangan Menteri, Timbalan Menteri dan pengurusan atasan KDN. Besar kemungkinan juga isi kandungan e-mel tersebut menyentuh sensitiviti perkauman, kepercayaan, keluarga dan politik orang lain;

(s) Pengguna adalah dilarang menghantar dan melibatkan diri dalam e-mel yang berunsur **hasutan**, **e-mel sampah** (*junkmail*), e-mel ***spam***, **e-mel layang**, **fitnah**, **ciplak, *phishing*** atau aktiviti-aktiviti lain yang **ditegah** oleh undang-undang Kerajaan Malaysia dan Siber Negara;

(t) Pengguna adalah dilarang menyebarkan kod perosak seperti ***virus***, ***worm***, ***trojan horse*** dan ***trap door*** yang boleh merosakkan sistem komputer dan maklumat pengguna lain;

(u) Pengguna adalah dilarang menghantar semula e-mel yang gagal sampai ke destinasi sebelum menyiasat punca kejadian;

(v) Pengguna tidak digalakkan membenar pihak ketiga untuk menjawab emel kepada penghantar asal bagi pihaknya;

(w) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah **tepat**;

(x) Pengguna tidak boleh membiarkan perkhidmatan e-mel berada atas **atas talian (*on-line*)** jika tidak digunakan. *Log off* e-mel sebelum keluar pejabat supaya tidak disalah gunakan oleh mana-mana pihak;

(y) Mana-mana pengguna termasuk pihak luar adalah dilarang menggunakan sebarang peralatan komputer membabitkan **storan luar** untuk tujuan muat turun / naik e-mel seperti *thumb* / *pen drive*, *disket*, *CDRW*, *DVD writetable* dan *external hard disk* sebelum diimbas terlebih dahulu dengan sebarang produk *anti-malware* (*virus, worms, trojan backdoor, spyware* dsb.) bagi mengelakkan *malware outbreak* di rangkaian KDN dan insiden keselamatan ICT; dan

(z) Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada **Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003** bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.

DKICTKDN-0615 Bawa Peranti Sendiri (BYOD)

(a) Peranti peribadi yang dibenarkan untuk digunakan seperti komputer riba, telefon pintar, dan tablet untuk tujuan rasmi perlu didaftarkan dan perlu mematuhi peraturan semasa;

(b) Pengguna tertakluk kepada syarat dan polisi yang ditetapkan di dalam Dasar Keselamatan ICT KDN; dan

(c) Pengguna perlu mendapatkan kata laluan bagi menggunakan rangkaian KDN daripada Helpdesk IT. Capaian tanpa menggunakan kata laluan yang sah adalah melanggar polisi Dasar Keselamatan ICT KDN.

PERKARA 07 : KAWALAN CAPAIAN

Huraian :	Capaian ke atas maklumat, kemudahan pemprosesan maklumat dan proses-proses utama dalam teras perkhidmatan perlu dikawal mengikut ketetapan yang ditentukan oleh pengurusan, pemilik data, proses, operasi atau sistem.
Objektif :	Untuk mengawal capaian ke atas maklumat.

DKICTKDN-0701 Pengurusan Kawalan Capaian

Ketua Setiausaha / Ketua Jabatan adalah bertanggungjawab untuk memastikan kawalan capaian ke atas aset ICT termasuk maklumat, perkhidmatan rangkaian dan kemudahan-kemudahan yang berkaitan diwujudkan dan dilaksanakan dengan berkesan berasaskan keperluan urusan dan keselamatan.

DKICTKDN-0702 Keperluan Kawalan Capaian

Seksyen ini bertujuan mengawal capaian ke atas maklumat, kemudahan-kemudahan pemprosesan maklumat dan perkhidmatan. Peraturan kawalan capaian hendaklah mengambil kira penyebaran dan pengesahan maklumat.

Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.

Perkara-perkara yang perlu dipastikan tetapi tidak hanya terhad kepada yang berikut :

(a) Kawalan capaian ke atas maklumat dan proses perkhidmatan mengikut keperluan keselamatan dan peranan pengguna seperti hak perlu mengetahui (need to know basis);

(b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;

(c) Kawalan capaian ke atas perkhidmatan internet;

(d) Kawalan capaian ke atas perkhidmatan yang menggunakan kemudahan atau peralatan dan *gadget* mudah alih; dan

(e) Kawalan ke atas kemudahan pemprosesan maklumat.

DKICTKDN-0703 Pengurusan Capaian Pengguna

Seksyen ini bertujuan memastikan bahawa sistem maklumat dicapai oleh pengguna yang sah dan menghalang capaian yang tidak sah.

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut :

(a) Mewujudkan prosedur pendaftaran dan penamatan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan;

(b) Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat;

(c) Akaun pengguna yang diwujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran Bahagian Pengurusan Teknologi Maklumat secara bertulis dan direkodkan;

(d) Pemilikan akaun dan capaian pengguna bukanlah hak mutlak seseorang dan ia adalah tertakluk kepada peraturan Kementerian dan tindakan pengemaskinian dan/atau penamatan hendaklah di ambil atas sebab seperti berikut:

i. Pengguna melanggar peraturan;

ii. Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan oleh Ketua Setiausaha/Jabatan;

iii. Pengguna bercuti atau bertugas di luar pejabat dalam satu tempoh yang lama seperti mana yang ditentukan oleh Ketua Setiausaha/Jabatan;

iv. Pengguna bertukar jawatan, tanggungjawab dan/atau bidang tugas;

v. Pengguna yang sedang dalam prosiding dan/atau dikenakan tindakan tatatertib oleh Pihak Berkuasa Tatatertib; dan

vi. Pengguna bertukar, berpindah agensi, bersara dan/atau tamat perkhidmatan.

(e) Penggunaan akaun milik orang lain atau atau akaun yang dikongsi bersama adalah dilarang.

Aktiviti capaian oleh pengguna direkod, diselenggara dengan sistematik dan dikaji dari masa ke semasa. Maklumat yang direkod termasuk identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya.

DKICTKDN-0704 Tanggungjawab Pengguna

Seksyen ini bertujuan memastikan pengguna melaksanakan langkah berkesan ke atas kawalan capaian untuk menghalang penyalahgunaan, kecurian maklumat dan kemudahan proses maklumat.

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut:

(a) Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaiks erta prosedur yang ditetapkan oleh KDN/Jabatan seperti berikut:

i. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;
ii. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;

iii. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan simbol (contoh : **P4s$w0rcl**);;
iv. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekali pun;
v. Kata laluan *Windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak diruang guna sama;
vi. Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;
vii. Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula;
viii. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;
ix. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan
x. Mengelakkan penggunaan semula kata laluan yang baru digunakan.

(b) Mematuhi amalan terbaik pemilihan dan penggunaan kata laluan. **Kata laluan** (*password*) **perlu dikawal** untuk mengelakkan daripada diketahui oleh orang yang tidak diberi kuasa menggunakannya:

(c) Memastikan kemudahan dan peralatan yang tidak digunakan mendapat perlindungan sewajarnya; dan

(d) Mematuhi amalan *clear desk* dan *clear screen policy*.

DKICTKDN-0705 Kawalan Capaian Rangkaian

Seksyen ini bertujuan menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan :

(a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian KDN, rangkaian Kementerian lain dan rangkaian awam;

(b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan, yang menepati kesesuaian penggunaannya; dan

(c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

DKICTKDN-0706 Kawalan Capaian Sistem Pengoperasian

Seksyen ini bertujuan untuk memastikan bahawa capaian ke atas sistem pengoperasian dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Kaedah yang digunakan hendaklah mampu menyokong pengesahan pengguna, mewujudkan audit trail ke atas semua capaian, menjana amaran (*alert*), pengesahan capaian (*authentication*) dan mengehadkan tempoh penggunaan.

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut:

(a) Mengawal capaian ke atas sistem operasi menggunakan prosedur *log-on* yang terjamin;

(b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna.

(c) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti;

(d) Mengehadkan dan mengawal penggunaan program utiliti yang berkemampuan mengatasi sebarang kawalan sistem dan aplikasi (*time-limit*);

(e) Menamatkan sesebuah sesi yang tidak aktif sekiranya tidak digunakan bagi satu tempoh yang ditetapkan (*log-off*); dan

(f) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

DKICTKDN-0707 Kawalan Capaian Sistem Aplikasi

Seksyen ini bertujuan menghalang capaian tidak sah ke atas maklumat yang terdapat di dalam sistem aplikasi. Kawalan capaian membenarkan pengguna mencapai sistem aplikasi dan maklumat mengikut tahap capaian yang ditentukan dan menyediakan mekanisme perlindungan bagi menghalang capaian tidak sah ke atas aplikasi dan maklumat daripada utiliti yang sedia ada dalam sistem operasi dan perisian *malicious* yang berupaya melangkaui kawalan sistem.

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut:

(a) Mengehadkan capaian ke atas maklumat dan fungsi sistem aplikasi oleh pengguna selaras dengan peraturan Kementerian (menetapkan *IP Address* komputer pengguna atau *ID* pengguna yang dibenarkan sahaja terhadap sesuatu sistem aplikasi atau *server*); dan

(b) Mewujudkan persekitaran pengkomputeran yang khusus dan terasing untuk sistem yang berklasifikasi tinggi.

DKICTKDN-0708 Peralatan Mudah Alih Dan Kerja Jarak Jauh

Seksyen ini bertujuan memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh. Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut:

(a) Mewujudkan peraturan dan garis panduan keselamatan yang bersesuaian untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi;

(b) Peralatan mudah alih hendaklah disimpan dan dikunci ditempat yang selamat apabila tidak digunakan;

(c) Mewujudkan peraturan dan garis panduan untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; dan

(d) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.

DKICTKDN-0709 Kawalan Capaian Sistem Pangkalan Data

Seksyen ini bertujuan untuk memastikan capaian ke atas pangkalan data dan data dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Kaedah yang digunakan hendaklah mampu menyokong pengesahan pengguna, mewujudkan jejak audit ke atas semua capaian, menjana amaran (alert), pengesahan capaian dan penyimpanan data.

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada perkara berikut:

(a) Capaian ke atas pangkalan data hendaklah dikawal.

(b) Penggunaan perisian yang membolehkan capaian terus ke pangkalan data secara pihak ketiga sama ada melalui perisian web (cth : phpmyadmin) atau sebagainya adalah tidak dibenarkan.

(c) Mewujudkan pengenalan diri (ID) yang unik bagi setiap pengguna dan hanya digunakan untuk pengguna berkenaan sahaja.

(d) Aplikasi yang perlu mengakses ke pangkalan data perlu menggunakan pengenalan diri yang berbeza daripada pengenalan diri pembangun aplikasi dan pentadbir pangkalan data.

PERKARA 08 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

Huraian :	Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem maklumat sedia ada atau sistem maklumat baru hendaklah menyatakan keperluan-keperluan kawalan keselamatan.
Objektif :	Untuk memastikan aspek keselamatan dikenal pasti dan diambil kira dalam semua sistem maklumat dan/atau perkhidmatan termasuk sistem pengoperasian, infrastruktur, sistem aplikasi dan sistem perisian. Aspek keselamatan ini mesti dikenal pasti, dijustifikasikan, dipersetujui dan didokumentasikan sebelum sesuatu sistem maklumat direka bentuk dan dilaksanakan.

DKICTKDN-0801 Perolehan, Pembangunan dan Penyelenggaraan Sistem Maklumat

Ketua Setiausaha / Ketua Jabatan adalah bertanggungjawab untuk :

(a) Memastikan kaedah keselamatan yang bersesuaian dikenal pasti, dirancang dan dilaksanakan pada setiap peringkat perolehan, pembangunan dan penyelenggaraan sistem maklumat;

(b) Melindungi kerahsiaan, integriti dan kesahihan maklumat menggunakan kaedah tertentu;

(c) Memastikan sistem fail dan aktiviti berkaitan beroperasi dengan baik dan selamat; dan

(d) Menjaga dan menjamin keselamatan sistem maklumat.

DKICTKDN-0802 Keperluan Keselamatan Sistem Maklumat

Seksyen ini bertujuan menjelaskan keperluan memastikan bahawa aspek keselamatan dikenal pasti, dipersetujui dan di dokumen pada setiap peringkat perolehan, pembangunan dan penyelenggaraan.

Perkara yang perlu dipatuhi adalah termasuk pernyataan keperluan bagi sistem maklumat baru atau penambahbaikan ke atas sistem sedia ada hendaklah menjelaskan mengenai kawalan jaminan keselamatan.

DKICTKDN-0803 Pemprosesan Aplikasi Dengan Tepat

Seksyen ini bertujuan memastikan kawalan keselamatan yang sesuai diolah dan diterapkan ke dalam aplikasi bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut:

(a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin kesahihan dan ketepatan;

(b) Menggabungkan semakan pengesahan ke dalam aplikasi untuk mengenal pasti sebarang kerosakan maklumat sama ada disebabkan oleh ralat pemprosesan atau tindakan yang disengajakan;

(c) Mengenal pasti dan melaksanakan kawalan untuk mengesah dan melindungi integriti mesej dalam sistem aplikasi; dan

(d) Melaksanakan proses pengesahan ke atas output data bagi menjamin kesahihan dan ketepatan pemprosesan sistem aplikasi.

DKICTKDN-0804 Kawalan Kriptografi

Seksyen ini bertujuan untuk melindungi kerahsiaan, kesahihan dan integriti maklumat melalui teknik kriptografi.

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut:

(a) membangun kawalan kegunaan dan melaksanakan suatu peraturan kawalan kriptografi dan pengurusan kunci yang digunakan untuk menyokong teknik kriptografi bagi melindungi maklumat;

(b) Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa;

(c) Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik; dan

(d) Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

DKICTKDN-0805 Keselamatan Fail-Fail Sistem

Seksyen ini bertujuan memastikan capaian ke atas fail-fail sistem dan kod sumber program adalah terkawal dan aktiviti-aktiviti sokongan dilaksanakan dalam kaedah yang selamat. Kawalan perlu diambil untuk mengelakkan pendedahan maklumat sensitif semasa proses pengujian dilaksanakan.

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut:

(a) Mewujudkan prosedur untuk mengawal pemasangan perisian ke dalam sistem yang sedang beroperasi;

(b) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;

(c) Kod sumber atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji;

(d) Mengawal capaian ke atas kod sumber atau atur cara sistem bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;

(e) Memilih dengan berhati-hati, melindungi dan mengawal data-data ujian; dan

(f) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.

DKICTKDN-0806 Keselamatan Dalam Proses Pembangunan Dan Sokongan

Seksyen ini bertujuan memastikan keselamatan perisian sistem aplikasi dan maklumat dikawal supaya selamat dalam semua keadaan.

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut:

(a) Mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan yang formal;

(b) Mengkaji semula dan menguji aplikasi kritikal semasa melaksanakan perubahan ke atas sistem yang sedang beroperasi untuk memastikan tiada impak negatif ke atas keselamatan atau operasi organisasi;

(c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian, data dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;

(d) Mengimbas dengan menggunakan kemudahan perkakasan/perisian imbasan terhadap sistem-sistem aplikasi berasaskan web (*web based application*) untuk mengenal pasti kelemahan-kelemahan keselamatan ICT dan seterusnya menjalankan langkah-langkah pengukuhan;

(e) Menghalang sebarang peluang untuk membocorkan maklumat; dan

(f) Mengawal selia dan memantau pembangunan perisian oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat. Kod sumber bagi semua aplikasi dan perisian adalah menjadi hak milik organisasi.

DKICTKDN-0807 Pengurusan Penilaian Kerentanan (*Vulnerability Assessment*) atau Penilaian Struktur Keselamatan (*Security Posture Assessment*)

Seksyen ini bertujuan memastikan pelaksanaan pengurusan penilaian kerentanan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya. Pelaksanaan pengurusan penilaian keterdedahan ini perlu juga dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan sekurang-kurangnya **setahun** sekali bergantung kepada tahap kritikal sistem pengoperasian dan sistem aplikasi yang sedia ada.

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut:

(a) Memperoleh maklumat teknikal kerentanan yang tepat pada masanya ke atas sistem maklumat yang digunakan;

(b) Menilai tahap pendedahan organisasi terhadap kerentanan tersebut; dan

(c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan (*Hardening*).

DKICTKDN-0808 Sekatan Dalam Instalasi Perisian

Seksyen ini menjelaskan peraturan berhubung instalasi perisian yang perlu diwujud dan dilaksanakan.

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut:

(a) Pengguna hanya dibenarkan menggunakan perisian yang disediakan oleh BPTM sahaja kecuali perisian yang mendapat persetujuan Setiausaha Bahagian (SUB) masing-masing atas tujuan rasmi.

DKICTKDN-0809 Polisi Pembangunan Sistem Selamat

Seksyen ini berperanan untuk memastikan keselamatan maklumat direkabentuk dan dilaksanakan didalam kerangka pembangunan sistem maklumat.

Perkara-perkara yang perlu diambilkira tetapi tidak hanya terhad kepada yang berikut:

(a) Mewujudkan persekitaran yang selamat untuk pembangunan sistem maklumat;

(b) Mewujudkan garis panduan jelas perihal keselamatan maklumat didalam proses pembangunan perisian/sistem maklumat;

(c) Mengenalpasti keperluan keselamatan didalam fasa rekabentuk perisian/sistem maklumat;

(d) Mengadakan titik semakan keselamatan didalam jadual perbatuan projek pembangunan perisian/sistem maklumat;

(e) Mewujudkan repositori yang selamat untuk perisian/sistem maklumat yang dibangunkan;

(f) Memastikan keselamatan dalam kawalan versi;

(g) Mengenalpasti aplikasi yang diperlukan untuk merekod pengetahuan berkaitan keselamatan sistem maklumat;

(h) Membina kemahiran pemaju perisian/sistem maklumat supaya mereka mampu menjauhi, mengenalpasti, dan merungkai setiap kelemahan yang dikesan didalam

perisian/sistem maklumat yang dibangunkan. Teknik pengaturcaraan selamat wajar dipraktik;

(i) Piawaian tentang teknik pengaturcaraan selamat wajar dirujuk;

(j) Kumpulan pemaju perlu diberi latihan secukupnya tentang skil pengujianan dan penyemakan kod perisian;

(k) Jika pembangunan perisian dilaksanakan dengan menggunakan sumber luar, KDN perlu mendapatkan jaminan bahawa pemaju yang dilantik memenuhi peraturan, polisi, prosidur, dan proses berkaitan pembangunan sistem selamat.

DKICTKDN-0810 Prinsip Kejuruteraan Sistem Selamat

Seksyen ini menjelaskan kepentingan untuk mewujud, mendokumen, dan menyelenggara prinsip-prinsip kejuruteraan sistem maklumat untuk digunapakai sewaktu pembangunan sistem maklumat.

Perkara-perkara yang perlu diambilkira tetapi tidak hanya terhad kepada yang berikut:

(a) Prosidur kejuruteraan sistem maklumat selamat yang berasaskan kepada prinsip-prinsip keselamatan kejuruteraan sistem perlu dibangun, didokumen, dan dilaksana di dalam setiap projek pembangunan sistem maklumat;

(b) Aspek keselamatan perlu perlu diberi penekanan dalam setiap lapisan rekabentuk struktur sistem maklumat (seperti lapisan bisnes, lapisan data, dan lapisan applikasi);

(c) Setiap teknologi baru yang bakal diguna pakai oleh KDN perlu dianalisis bagi menilai risiko keselamatan. Rekabentuk teknologi perlu disemak dari sudut kelemahan dan potensi serangan oleh pencerobоh sistem maklumat;

(d) Setiap prosidur dan prinsip kejuruteraan sistem maklumat yang dibangunkan perlu disemak dari masa ke semasa bagi memastikan ianya kekal relevan dan mampu menangani ancaman keselamatan yang sentiasa berubah mengikut masa;

(e) Prinsip dan prosidur kejuruteraan sistem selamat juga perlu digunapakai sekiranya KDN melaksanakan pembangunan sistem maklumat mengunakan sumber luar. Pematuhan kepada prinsip dan prosidur berkaitan perlu dinyatakan dengan jelas dalam perjanjian bersama pemaju luar.

DKICTKDN-0811 Persekitaran Pembangunan Sistem Selamat

Seksyen ini menjelaskan keperluan untuk memastikan persekitaran pembangunan sistem adalah selamat dan dilindungi bagi memastikan pembangunan, pengintegrasian, dan pengujianan sistem maklumat terjamin.

Perkara-perkara yang perlu diambilkira tetapi tidak hanya terhad kepada yang berikut:

(a) Sensitiviti data yang perlu diproses, disimpan, dan dipindahkan melalui sistem maklumat yang dibangunkan;

(b) Keperluan dalaman dan luaran yang berkaitan (seperti regulasi dan polisi);

(c) Kawalan keselamatan yang telah sedia laksana dalam KDN yang menyokong aktiviti pembangunan sistem maklumat;

(d) Kebolehpercayaan personel yang bekerja dalam persekitaran pembangunan sistem maklumat;

(e) Tahap penglibatan suber luar dalam pembangunan sistem maklumat;

(f) Keperluan untuk mengasingkan beberapa persekitaran yang berbeza;

(g) Kawalan akses ke persekitaran pembangunan sistem malumat;

(h) Pemantauan perubahan terhadap persekitaran dan kod sumber;

(i) Pendua kepada data-data projek pembangunan sistem maklumat disimpan di lokasi berasingan dari persekitaran pembangunan sistem maklumat;

(j) Kawalan terhadap pergerakan data dari dan kepada persekitaran;

(k) Setelah strategi perlindungan persekitaran ditentukan, KDN sewajarnya mendokumenkan proses-proses yang berkaitan didalam kerangka pembangunan sistem selamat dan menjadikannya sebagai rujukan kumpulan pemaju.

DKICTKDN-0812 Pengujianan Keselamatan Sistem

Seksyen ini menjelaskan keperluan untuk melaksanakan pengujianan terhadap fungsi-fungsi keselamatan sistem maklumat semasa fasa pembangunan berlangsung.

Perkara-perkara yang perlu diambilkira tetapi tidak hanya terhad kepada yang berikut:

(a) Persiapan rapi untuk melaksanakan pengujianan keselamatan sistem maklumat perlu dilakukan termasuk jadual pengujianan, data input, jangkaan keputusan, dan kondisi pengujianan;

(b) Untuk sistem maklumat yang dibangunkan sepenuhnya oleh KDN, pengujianan keselamatan sistem maklumat boleh dilakukan oleh kumpulan dalaman terlebih dahulu kemudian baru diikuti dengan pengujianan penerimaan secara bebas oleh pengguna sebenar sistem.

PERKARA 09 : PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

Huraian :	Semua insiden keselamatan ICT yang berlaku di KDN dan agensi-agensi di bawahnya mestilah dilaporkan dengan serta-merta kepada KDN CERT dan dikendalikan mengikut peraturan atau prosedur pengurusan pengendalian insiden keselamatan ICT Kerajaan yang ditetapkan.
Objektif :	Untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan, dan memastikan sistem ICT KDN dan agensi-agensi di bawahnya dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej KDN dan sistem penyampaian perkhidmatan awam.

DKICTKDN-0901 Pengurusan Pengendalian Insiden Keselamatan ICT

Ketua Setiausaha / Ketua Jabatan adalah bertanggungjawab untuk memastikan Bahagian / Seksyen / Unit di bawah kawalannya mematuhi dasar mengenai pengurusan pengendalian insiden keselamatan ICT KDN dengan merujuk kepada KDN CERT, pekeliling am, surat pekeliling am, garis panduan dan prosedur operasi standard yang telah dikeluarkan oleh Kementerian dan Kerajaan.

DKICTKDN-0902 Insiden Keselamatan ICT

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar Dasar Keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat.

KDN CERT hendaklah melaksanakan tindakan ke atas insiden keselamatan ICT mengikut peraturan atau prosedur yang ditetapkan oleh Kerajaan dari masa ke semasa.

Insiden keselamatan ICT hendaklah dilaporkan kepada ICTSO dan KDN CERT dengan kadar segera tetapi tidak hanya terhad kepada yang berikut:

(a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;

(b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;

(c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;

(d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan

(e) Berlaku percubaan menceroboh, penyelewengan dan insideninsiden yang tidak dijangka.

DKICTKDN-0903 Mekanisme Pelaporan Insiden Keselamatan ICT

(a) **Pelaporan**

Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada Pegawai Keselamatan ICT (ICTSO) KDN dan kepada CERT Kementerian (KDN CERT) atau / dan kepada *Government Computer Emergency Response Team* (GCERT) untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan.

(b) **Pelantikan Pegawai Bertanggungjawab**

Pegawai Keselamatan ICT KDN atau ICTSO dan anggota pasukan KDN CERT mestilah dilantik secara rasmi oleh pengurusan KDN, dan semua warga KDN perlu ambil maklum akan pelantikan pegawai-pegawai ini, dan perlu sentiasa bersedia untuk memberi respons apabila diperlukan.

(c) **Tanggungjawab Pengguna**

Semua warga KDN, pembekal, pakar runding dan pihak-pihak lain yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden keselamatan ICT, kerentanan yang diperhatikan atau disyaki terdapat dalam perkhidmatan dan sistem maklumat KDN menerusi mekanisme pelaporan ini. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan pencerobohan.

(d) **Tindakan Dalam Keadaan Berisiko Tinggi**

Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak kepada agensi-agensi lain.

DKICTKDN-0904 Prosedur Pengendalian Insiden Keselamatan ICT

Semua pegawai pasukan pengendali insiden keselamatan ICT KDN CERT perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur operasi standard keselamatan ICT GCERT, MAMPU. Sekiranya insiden sukar untuk diselesaikan pada peringkat KDNCERT, bantuan kepakaran GCERT, MAMPU hendaklah diperolehi. Prosedur pelaporan insiden keselamatan ICT berdasarkan:

(e) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan

(f) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.

DKICTKDN-0905 Pengurusan Maklumat Insiden Keselamatan ICT

(a) **Perancangan**

Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan dan tindakan untuk melaksanakan peningkatan dan kawalan tambahan bagi mengawal kekerapan, kerosakan dan kos kejadian insiden akan datang, dan untuk tujuan mengkaji semula dasar-dasar keselamatan aset ICT sedia ada. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada KDN.

(b) **Bahan Bukti**

Pasukan KDN CERT hendaklah memastikan bahan-bahan bukti berkaitan insiden keselamatan ICT dapat disediakan, disimpan, disenggarakan dan mempunyai perlindungan keselamatan. Penyediaan bahan-bahan bukti seperti jejak audit, *backup* secara berkala, media *backup offline* ini hendaklah mengikut amalan terbaik yang disarankan oleh pihak GCERT, MAMPU dan kerajaan dari masa ke semasa.

Pasukan KDN CERT juga hendaklah memastikan semua bahan bukti adalah selaras dengan peraturan pengumpulan maklumat dari segi kualiti, kelengkapan dan kebolehpercayaan bahan bukti yang termaktub dalam bidang kuasa perundangan berkenaan.

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut:

i. Menyimpan jejak audit dan melindungi integriti semua bahan bukti;

ii. Menyalin bahan bukti oleh personel yang dipertanggungjawabkan;

iii. Merekod semua maklumat aktiviti penyalinan termasuk pegawai terlibat, media, perisian, perkakasan dan *tools* yang digunakan;

iv. Menyediakan tindakan pemulihan segera;

v. Memaklumkan pihak berkuasa perundangan, seperti pegawai undang-undang dan polis (jika perlu); dan

vi. Mendapatkan nasihat dari pihak berkuasa perundangan ke atas bahan bukti yang perlukan.

DKICTKDN-0906 Penilaian Dan Keputusan Terhadap Insiden Keselamatan ICT

CERT KDN bertanggungjawab terhadap insiden keselamatan ICT dan keputusan perlu dibuat jika insiden tersebut boleh diklasifikasikan sebagai insiden keselamatan maklumat mengikut prosidur yang ditetapkan. Pasukan yang terlibat wajar melaksanakan perkara-perkara berikut:

(a) Penilaian perlu dibuat berasaskan skim klasifikasi insiden yang dipersetujui;

(b) Insiden perlu disusun mengikut kepentingan dan implikasi kepada KDN;

(c) Hasil daripada penilaian yang dibuat boleh dipanjangkan kepada CERT supaya pengesahan atau penilaian semula dapat dilakukan;

(d) Hasil daripada penilaian juga perlu direkodkan dengan terperinci untuk rujukan masa depan dan penentusahan.

DKICTKDN-0907 Tindakbalas Terhadap Insiden Keselamatan ICT

Insiden keselamatan maklumat perlu diberi tindakbalas sewajarnya oleh pihak yang bertanggungjawab mengikut prosidur yang berkaitan. Matlamat utama tindakbalas terhadap insiden keselamatan ICT adalah untuk mengembalikan tahap keselamatan ke paras normal dan seterusnya melaksanakan langkah-langkah perlu pemulihan.

Pasukan tindakbalas wajar melaksanakan perkara berikut:

(a) Mengumpul bahan bukti secepat yang mungkin selepas kejadian;

(b) Melaksanakan forensik keselamatan maklumat;

(c) Insiden dimaklumkan kepada pihak yang berkaitan atau perlu tahu;

(d) Semua aktiviti dalam memberi tindakbalas direkod secara sistematik untuk analisis selanjutnya;

(e) Mengendalikan dengan efektif kelemahan-kelemahan keselamatan maklumat yang diketahui menjadi penyebab atau penyumbang kepada sesuatu insiden berlaku;

(f) Selepas sesuatu insiden ditangani dengan sempurna, penutupan kes secara rasmi perlu dilakukan dengan rekod;

(g) Analisa pasca insiden wajar dlakukan untuk mengenalpasti punca insiden;

PERKARA 10 : PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Huraian :	Pengurusan kesinambungan perkhidmatan dan pelan pengurusan kesinambungan perkhidmatan hendaklah diwujudkan dan dilaksanakan berdasarkan kepada persekitaran dan operasi KDN.
Objektif :	Untuk memastikan penyampaian perkhidmatan yang berterusan kepada pelanggan.

DKICTKDN-1001 Pengurusan Kesinambungan Perkhidmatan

Pengurusan Kesinambungan Perkhidmatan adalah mekanisme bagi mengurus dan memastikan kepentingan *stakeholder* sistem penyampaian perkhidmatan dilindungi dan imej KDN terpelihara dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan KDN di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan.

Ketua Setiausaha / Ketua Jabatan adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT KDN.

DKICTKDN-1002 Pelan Kesinambungan Perkhidmatan

Pelan Kesinambungan Perkhidmatan hendaklah dibangunkan bagi menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan KDN. Ini bertujuan memastikan tindakan pemulihan yang cekap dan berkesan dilaksanakan **sebelum, semasa** dan **selepas** berlakunya musibah atau bencana.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut :

(a) **Perakuan Pengurusan**

Pelan ini mestilah diperakukan oleh pihak pengurusan atasan KDN.

(b) **Program Latihan / Kesedaran**

Program latihan / kesedaran kepada semua warga KDN mengenai pelan ini dan proses serta prosedur yang terlibat perlu dilaksanakan.

(c) **Penyelenggaraan Pelan**

Pelan Kesinambungan Perkhidmatan perlu diselenggara secara berkala dan diuji pelaksanaannya terutama apabila terdapat perubahan dalam operasi dan sistem penyampaian perkhidmatan KDN dan Kerajaan.

(d) Sila rujuk kepada **Garis Panduan Pengurusan Kesinambungan Perkhidmatan (BCM) Sektor Awam** yang dikeluarkan oleh MAMPU.

PERKARA 11: PEMATUHAN

Huraian :	Keperluan-keperluan perundangan, peraturan atau ikatan kontrak hendaklah dinyatakan, didokumenkan dan dikemas kini.
Objektif :	Untuk menghindar pelanggaran undang-undang jenayah dan sivil, *statutory*, peraturan atau ikatan kontrak dan sebarang keperluan keselamatan lain.

DKICTKDN-1101 Pematuhan Keperluan Perundangan

Ketua Setiausaha / Ketua Jabatan adalah bertanggungjawab untuk memastikan semua pengguna aset ICT termasuk pembekal dan pakar runding mematuhi dan seterusnya memastikan pelanggaran kepada perundangan yang berkaitan dan keperluan dasar ini dielakkan.

DKICTKDN-1102 Pematuhan Dasar

Langkah-langkah perlu bagi mengelakkan sebarang pelanggaran perundangan termasuklah memastikan setiap pengguna membaca, memahami dan mematuhi Dasar Keselamatan ICT KDN serta undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.

DKICTKDN-1103 Keperluan Perundangan

Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di KDN termasuk agensi-agensi di bawahnya termasuklah seperti berikut :

(a) **Keselamatan Perlindungan Secara Am**

i. *Emergency (Essential Power) Act 1964;*

ii. *Essential (Key Points) Regulations 1965;*

iii. Perakuan Jawatankuasa mengkaji semula peraturan keselamatan Pejabat Tahun 1982;

iv. Dasar Keselamatan Yang Dikuatkuasakan Melalui Surat Pekeliling Am Sulit Bil. 1 Tahun 1985;

v. Dasar Jawatankuasa Tetap Sasaran Penting Bil. 1 Tahun 1985;

vi. Dasar Tetap Sasaran Penting Yang Dikeluarkan Kepada Pihak Yang Terlibat Dalam Pengurusan Sasaran Penting Milik Kerajaan Dan Swasta Yang Diluluskan Oleh Jemaah Menteri Pada 13 Oktober 1993; dan

vii. Surat Pekeliling Am Sulit Bil. 1 Tahun 1993 - Meningkatkan Kualiti Kawalan Keselamatan Perlindungan Di Jabatan-Jabatan Kerajaan.

(b) **Keselamatan Dokumen**

i. *Confidential General Circular Memorandum No.1 of 1959 (Code Words-Allocation & Control);*

ii. Akta Rahsia Rasmi 1972;

iii. Akta Arkib Negara 2003;

iv. Surat Pekeliling Bil. 8 Tahun 1990 - Dasar Keselamatan Kawalan, Penyelenggaraan, Maklumat-Maklumat Ukur Dan Geografi Yang Antara Lainnya Merangkumi Peta-Peta Rasmi Dan Penderiaan Jauh;

v. Surat Pekeliling Am Sulit Bil. 1 Tahun 1972 - Keselamatan Rahsia-Rahsia Kerajaan Daripada Ancaman Penyuluhan (*espionage*);

vi. Surat Pekeliling Am Bil. 2 Tahun 1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1976;

vii. Peraturan Pengurusan Rahsia Rasmi Selaras dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1986 Dan Surat Pekeliling Am Bil. 2 Tahun 1987 Yang Ditandatangani Oleh Ketua Setiausaha Negara Melalui Surat M(R)10308/3/(45) Bertarikh 8 Mei 1987; dan

viii. Kawalan Keselamatan Rahsia Rasmi Dan Dokumen Rasmi Kerajaan Yang Dikelilingkan melalui Surat KPKK(R)200/55 Klt.7(21) Bertarikh 21 Ogos 1999.

(c) **Keselamatan Fizikal Bangunan**

i. Akta Kawasan Larangan Dan Tempat Larangan Tahun 1959;

ii. Dasar Pembinaan Bangunan Berdekatan Dengan Sasaran Penting, Kawasan Larangan Dan Tempat Larangan;

iii. *State Key Points;*

iv. Surat Pekeliling Am Rahsia Bil.1 Tahun 1975 - Keselamatan Jabatan-Jabatan Kerajaan;

v. Surat Bil. KPKK/308/A (2) bertarikh 7/9/79 - Mencetak Pas-Pas Keselamatan dan Kad-Kad Pengenalan Kementerian/Jabatan;

vi. Surat Pekeliling Am Bil. 4 Tahun 1982 - Permohonan Ruang Pejabat Sama Ada Dalam Bangunan Guna sama Atau pun Disewa Di Bangunan Swasta; dan

vii. Surat Pekeliling Am Bil. 14 Tahun 1982 – Pelaksanaan Pelan Pejabat Terbuka.

(d) **Keselamatan Individu**

i. *Government Security Officer: Terms of Reference – Extract On Training Of Departmental Security Office Confidenti;*

ii. *General Circular Memorandum;*

iii. *Instruction On Positive Vetting Procedure;*

iv. Surat Pekeliling Am Sulit Bil.1/1966 - Perkara Keselamatan Tentang Persidangan- Persidangan/ Perjumpaan/Lawatan Sambil Belajar Antarabangsa;

v. Surat Pekeliling Tahun 1966 – Tapisan Keselamatan Terhadap Pakar/Penasihat Luar Negeri**;**

vi. Surat Pekeliling Am Sulit Bil.1/1967 – Ceramah Keselamatan bagi Pegawai-Pegawai Kerajaan dan mereka-mereka yang Bukan Pegawai-Pegawai Kerajaan yang bersama dalam Perwakilan Rasmi Malaysia semasa melawat Negara-Negara Tabir Buluh dan Tabir Besi;

vii. Surat Pekeliling Am Sulit Bil. 2 Tahun 1977 - Melaporkan Perjumpaan/ Percakapan Di Antara Diplomat/ Orang-Orang Perseorangan Dari Negeri-Negeri Asing Dengan Anggota-Anggota Kerajaan; dan

viii. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.

(e) **Keselamatan Aset ICT**

i. Akta Tandatangan Digital 1997;

ii. Akta Jenayah Komputer 1997;

iii. Akta Hak Cipta (Pindaan) 1997;

iv. Akta Multimedia dan Telekomunikasi 1998;

v. Surat Pekeliling Am Bil. 1 Tahun 1993 - Peraturan Penggunaan Mesin Faksimile di Pejabat-Pejabat Kerajaan;

vi. Pekeliling Am Bil. 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat & Komunikasi (ICT);

vii. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan mengenai Tatacara Penggunaan Internet & Mel Elektronik di Agensi - Agensi Kerajaan;

viii. Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002;

ix. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005.

x. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; dan

xi. Akta dan peraturan-peraturan lain yang berkaitan.

DKICTKDN-1104 Pelanggaran Perundangan

Mengambil tindakan undang-undang dan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaian, kelalaian dan pelanggaran keselamatan yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 dan akta lain yang berkaitan.

DKICTKDN-1105 Kebolehsediaan Fasiliti Pemprosesan Maklumat

Untuk memastikan kebolehsediaan fasiliti pemprosesan maklumat ditahap yang tinggi, kaedah pemprosesan bertindan (lebih dari satu lokasi/platform pemprosesan) perlu diwujudkan.

Untuk tujuan itu, perkara berikut wajar diberi tumpuan:

(a) KDN perlu mengenalpasti keperluan kebolehsediaan sistem maklumat (memahami sejauh mana kritikalnya kebolehsediaan sesuatu sistem maklumat);

(b) Jika kebolehsediaan sistem maklumat tidak dapat dipastikan dengan satu lokasi pemprosesan, maka fasiliti pemprosesan bertindan perlu dipertimbangkan;

(c) Fasiliti pemprosesan bertindan perlu diuji bagi memastikan kesiapsediaan menjalankan operasi apabila pemprosesan utama gagal berfungsi;

(d) Kewujudan pemprosesan bertindan boleh membawa risiko kepada kewibawaan dan kerahsiaan maklumat dan sistem maklumat. Hal ini perlu diambil kira semasa sesuatu sistem maklumat itu direkabentuk.

GLOSARI

(a) **Risiko**

Bermaksud kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian.

(b) **Penilaian Risiko**

Bermaksud penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.

(c) **Ancaman**

Bermaksud apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah.

(d) ***Vulnerability***

Bermaksud sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman.

(e) **Insiden Keselamatan**

Bermaksud musibah (*adverse event*) yang berlaku ke atas sistem maklumat.

(f) **Aset ICT**

Bermaksud semua yang mempunyai nilai kepada organisasi merangkumi perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.

(g) ***Clear Desk***

Bermaksud tidak meninggalkan sebarang dokumen yang sensitif di atas meja.

(h) ***Clear Screen***

Bermaksud tidak memaparkan sebarang maklumat sensitif apabila komputer berkenaan ditinggalkan.

(i) ***Mobile Code***

Bermaksud kod perisian yang dipindahkan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi-fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna.

(j) **Kriptografi**

Bermaksud adalah satu sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.