Dasar Keselamatan ICT (DKICT)

JABATAN PERTANIAN

KEMENTERIAN PERTANIAN DAN INDUSTRI ASAS TANI

Jabatan Pertanian (DOA)

Kementerian Pertanian dan Industri Asas Tani

September 2009
Versi 1.0

PRAKATA KETUA PENGARAH PERTANIAN

JABATAN PERTANIAN

Assalamualaikum dan Salam Sejahtera,

Perkembangan pesat dalam ICT mengakibatkan keselamatan ICT dan maklumat yang terkandung di dalamnya tidak boleh dipandang ringan oleh semua pihak. Peningkatan kejadian pencerobohan, penggodaman, penyalahgunaan, pengubahsuaian dan pendedahan maklumat tanpa izin serta serangan virus telah menimbulkan kesedaran pihak DOA untuk membendungnya daripada berlaku.

Keselamatan ICT adalah kritikal dalam perkhidmatan sektor awam. Usaha melindungi aset ICT sesebuah organisasi merupakan satu cabaran dalam persekitaran yang sentiasa menjurus ke arah pengintegrasian kemajuan pesat teknologi dalam satu sistem yang efisien. Sehubungan itu, DOA telah menyediakan Dasar Keselamatan ICT DOA (DKICT DOA) yang bertujuan untuk memberi kesedaran kepada warga DOA betapa pentingnya menjaga maklumat dan aset ICT dengan selamat.

Saya yakin, DKICT DOA ini akan dijadikan sumber rujukan dan panduan untuk semua warga DOA bagi mewujudkan persekitaran keselamatan ICT yang mantap. Semoga dengan pematuhan dasar ini, insiden keselamatan dapat ditangani dengan bijak dan berkesan. Selain itu, kerjasama pematuhan daripada semua warga DOA amat dialu-alukan bagi merealisasikan matlamat DKICT ini.

Salam hormat,

Datuk Roseley Bin Dato' Khalid

Ketua Pengarah Pertanian

Jabatan Pertanian

15 September 2009

KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT (DKICT) Jabatan Pertanian Malaysia (DOA) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna di DOA, Institut dan Pusat di bawah DOA mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT di DOA, Institut dan Pusat masing-masing.

RASIONAL

Tujuan utama keselamatan ICT adalah untuk menjamin kesinambungan urusan Kerajaan dengan meminimumkan kesan insiden keselamatan. Aset ICT perlu dilindungi kerana ianya merupakan pelaburan besar Kerajaan bagi meningkatkan kecekapan dan keberkesanan sistem penyampaian.

Begitu juga dengan maklumat yang tersimpan di dalam sistem ICT. Ia amat berharga kerana banyak sumber yang telah digunakan untuk menghasilkannya dan sukar untuk dijana semula dalam jangka masa yang singkat. Tambahan pula terdapat maklumat yang diproses oleh sistem ICT adalah sensitif dan terperingkat.

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

Ancaman ke atas keselamatan ICT boleh memberi kesan ke atas semua pihak termasuklah aset yang dikendalikan. Ancaman tersebut termasuklah perbuatan jenayah terhadap kakitangan, kecurian, penipuan, vandalisme, kebakaran, bencana alam, ralat atau kegagalan teknikal serta kerosakan yang tidak disengajakan.

Ancaman dari serangan siber dan aktiviti kod-kod jahat melalui Internet semakin meningkat dan mampu menjejaskan sistem penyampaian dan infrastruktur kritikal Kerajaan. Memandangkan pentingnya aset ICT dilindungi, maka satu Dasar Keselamatan ICT Kerajaan perlu diwujudkan.

OBJEKTIF

Dasar Keselamatan ICT DOA diwujudkan untuk menjamin kesinambungan urusan DOA dengan meminimumkan kesan insiden keselamatan ICT.

Objektif utama Dasar Keselamatan ICT DOA adalah seperti berikut:-

(a) Memastikan kelancaran operasi DOA dan meminimumkan kerosakan atau kemusnahan aset ICT DOA;

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

(c) Mencegah salah guna atau kecurian aset ICT Kerajaan;

(d) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;

(e) Meningkatkan tahap keselamatan ICT kepada para kakitangan, pengguna dan pembekal;

(f) Memperkemaskan pengurusan risiko; dan

(g) Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal.

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

PERNYATAAN DASAR

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

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

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

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

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

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

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

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

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

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

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

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

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

SKOP

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

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

Memandangkan sistem ICT sangat kompleks dan terdedah kepada kelemahan, ancaman dan risiko, adalah tidak mudah untuk memenuhi keperluan ini. Sistem ICT dan komponennya yang saling berhubungan dan bergantungan antara satu dengan lain kerap kali mewujudkan pelbagai kelemahan. 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.

Bagi menangani risiko ini secara berterusan, Dasar Keselamatan ICT DOA akan diperjelaskan lagi melalui standard-standard keselamatan ICT yang mengandungi garis panduan serta langkah-langkah keselamatan ICT yang akan dikeluarkan dari semasa ke semasa. 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.

Bagi menentukan Sistem ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT DOA ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, di wujud, di musnah, disimpan, dijana, dicetak, di akses, di edar dalam penghantaran, dan yang dibuat salinan keselamatan ke dalam semua aset ICT. Ini akan dilakukan melalui pewujudan 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 DOA. 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 DOA;

(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 DOA. Contoh: sistem dokumentasi, prosedur operasi, rekod-rekod DOA, 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 DOA bagi mencapai misi dan objektif DOA. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

(f) **Dokumentasi**
Semua dokumen (prosedur dan manual pengguna) yang berkaitan dengan aset ICT pemasangan dan pengoperasian peralatan dan perisian, sama ada dalam bentuk elektronik atau bukan elektronik.

(g) **Premis Komputer dan Komunikasi**
Semua kemudahan serta premis yang digunakan untuk menempatkan Perkara (a) – (f) di atas.

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

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

Dasar ini adalah terpakai kepada semua pengguna di Jabatan Pertanian Malaysia termasuk kakitangan, pembekal dan pakar runding yang mencapai, mengurus, menyelenggara, memproses, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT Jabatan Pertanian Malaysia.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT DOA dan perlu dipatuhi adalah seperti berikut:-

(a) **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 (Sumber: Arahan Keselamatan perenggan 53, muka surat 15):-

(i) Klasifikasi Maklumat

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

(ii) Tapisan Keselamatan Pengguna

Dasar Keselamatan ICT Kerajaan 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.

(b) **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.

(c) **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:-

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

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

(iii) Menentukan maklumat sedia untuk digunakan;

(iv) Menjaga kerahsiaan kata laluan;

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

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

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

(d) **Pengasingan**

(i) 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, di manipulasi dan seterusnya, mengenalkan integriti dan kebolehsediaan; dan

(ii) 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:-

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

(ii) Persekitaran penerimaan di mana sesuatu aplikasi diuji; dan

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

(e) **Pengauditan**

(i) 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;

(ii) 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

(iii) 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.

(f) **Pematuhan**

Dasar Keselamatan ICT DOA hendaklah dibaca, difahami dan dipatuhi. Pematuhan adalah merupakan prinsip penting dalam menghindar dan mengesan sebarang perlanggaran Dasar yang boleh membawa ancaman kepada keselamatan ICT. Pematuhan kepada Dasar Keselamatan ICT Kerajaan boleh dicapai melalui tindakan berikut:

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

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

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

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

(g) **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:-

(i) Mewujudkan, merumuskan dan menguji Pelan Pemulihan Bencana/ kesinambungan perkhidmatan– (*Disaster Recovery Plan/ Business Continuity Plan*); dan

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

(h) **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:-

(i) 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;

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

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

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

Perkara 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR

Objektif : Menerangkan hala tuju, sokongan pengurusan dan peraturan-peraturan bagi mengguna dan melindungi aset ICT selaras dengan keperluan Jabatan Pertanian dan perundangan yang berkaitan.

DM-0101	**Pelaksanaan Dasar**	
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah Jabatan Pertanian dibantu oleh Jawatankuasa Keselamatan ICT DOA yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), semua Pengarah Bahagian, Pengarah Pejabat Pertanian Negeri, Ketua Institut dan Ketua Pusat.	Ketua Pengarah Pertanian
DM-0102	**Penyebaran Dasar**	
	Dasar ini perlu disebarkan kepada semua pengguna Jabatan Pertanian (termasuk kakitangan, pembekal, pakar runding dll.)	ICTSO, STPM
DM-0103	**Penyelenggaraan Dasar**	
	Dasar Keselamatan ICT DOA adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT DOA: a. kenal pasti dan tentukan perubahan yang diperlukan; b. kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Jawatankuasa Keselamatan ICT (JKICT) Jabatan Pertanian; c. perubahan yang telah dipersetujui oleh JKICT Jabatan Pertanian dimaklumkan kepada semua pengguna; dan d. dasar ini hendaklah dikaji semula sekurang-kurangnya dua tahun sekali atau mengikut keperluan semasa.	ICTSO

DM-0104	Pengecualian Dasar	
	Dasar Keselamatan ICT DOA adalah terpakai kepada semua pengguna ICT Jabatan Pertanian dan tiada pengecualian diberikan.	Semua

Perkara 02 ORGANISASI KESELAMATAN

Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT DOA.

DM-0201	**Infrastruktur Organisasi Dalaman**	
DM-020101	**Ketua Pengarah**	
	Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOA; b. memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT DOA; c. memastikan semua pengguna mematuhi Dasar Keselamatan ICT DOA; d. memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; e. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT DOA.	Ketua Pengarah Pertanian
DM-020102	**Ketua Pegawai Maklumat (CIO)**	
	Timbalan Ketua Pengarah (Operasi) Jabatan Pertanian adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab beliau adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOA; b. bertanggungjawab ke atas perkara–perkara yang berkaitan dengan keselamatan ICT DOA; c. membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; d. menentukan keperluan keselamatan ICT; e. membangun dan menyelaras pelaksanaan pelan tindakan dan program kesedaran mengenai keselamatan ICT seperti penyediaan DKICT DOA dan pengauditan; f. mempengerusikan Jawatankuasa Pemandu ICT (JPICT)/Keselamatan ICT (JKICT).	CIO

DM-020103	Pegawai Keselamatan ICT (ICTSO)	
	Jawatan ICTSO bagi DOA adalah disandang oleh Ketua Unit Pentadbir Rangkaian yang merupakan Pegawai Teknologi Maklumat (PTM). Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Mengurus keseluruhan program-program keselamatan ICT DOA; b. menguatkuasakan pelaksanaan Dasar Keselamatan ICT DOA; c. memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT DOA kepada semua pengguna; d. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT DOA; e. menjalankan pengurusan risiko; f. menjalankan audit, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h. melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (CERT) MOA dan memaklumkannya kepada CIO; i. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; j. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT DOA; dan k. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	ICTSO

DM-020104	**Pengurus ICT**	
	Ketua Seksyen Teknologi dan Pengurusan Maklumat (STPM) adalah merupakan Pengurus ICT DOA. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOA; b. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan DOA; c. menentukan kawalan akses semua pengguna terhadap aset ICT DOA; d. melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; e. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT DOA.	Pengurus ICT
DM-020105	**Pentadbir Sistem ICT**	
	Pegawai di setiap unit di Seksyen Teknologi dan Pengurusan Maklumat adalah merupakan Pentadbir Sistem ICT DOA dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOA; b. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; c. menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT DOA; d. memantau aktiviti capaian harian pengguna; e. bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan baik; f. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatal atau memberhentikannya dengan serta-merta; g. menyimpan dan menganalisis rekod jejak audit; h. menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	Pentadbir Sistem ICT

DM-020106	Pengguna	
	Peranan dan tanggungjawab pengguna adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOA; b. mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. lulus tapisan keselamatan; d. melaksanakan prinsip-prinsip Dasar Keselamatan ICT DOA dan menjaga kerahsiaan maklumat DOA; e. melaksanakan langkah-langkah perlindungan seperti berikut :- i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. menentukan maklumat sedia untuk digunakan; iv. menjaga kerahsiaan kata laluan; v. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; g. menghadiri program-program kesedaran mengenai keselamatan ICT; dan h. menandatangani "Surat Akuan Pematuhan" (Lampiran 3) bagi mematuhi Dasar Keselamatan ICT DOA.	Pengguna

DM-020107	Jawatankuasa Pemandu ICT/ Keselamatan ICT DOA	
	Keanggotaan DOA adalah seperti berikut: **Pengerusi**: CIO **Ahli**: i. Pengarah Bahagian Pengurusan ii. Pengarah Bahagian Perancangan, Teknologi Maklumat dan Komunikasi iii. Pengarah Bahagian Pengembangan dan Industri Asas Tani iv. Pengarah Bahagian Hortikultur v. Pengarah Bahagian Pengurusan dan Pemuliharaan Sumber Tanah vi. Pengarah Bahagian Kejuruteraan Pertanian vii. Pengarah Bahagian Padi, Tanaman Industri dan Florikultur viii. Pengarah Bahagian Perlindungan Tanaman dan Kuarantin Tumbuhan ix. Pengarah Bahagian Kawalan Racun Perosak x. Pengarah Bahagian Kawalan Kualiti Tanaman xi. Pengarah Bahagian Pembangunan Sumber Manusia xii. Ketua Seksyen Teknologi dan Pengurusan Maklumat xiii. Pegawai Perhubungan Awam DOA xiv. ICTSO DOA **Urus Setia**:STPM, BPICT DOA Carta struktur organisasi DOA seperti di Lampiran 1. **Bidang kuasa**: a. Menyelenggara dokumen DKICT DOA; b. memantau tahap pematuhan; c. menilai aspek teknikal keselamatan projek-projek ICT; d. membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam jabatan yang mematuhi keperluan DKICT DOA; e. menyemak semula sistem ICT supaya sentiasa mematuhi keperluan keselamatan dari semasa ke semasa; f. memberi nasihat kepada JPICT; g. menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;	JPICT DOA

	h. memastikan DKICT DOA selaras dengan dasar-dasar ICT kerajaan semasa; dan i. menyediakan laporan keselamatan ICT kepada JPICT, dan membincangkan serta menyelesaikan isu-isu berbangkit.	
DM-020108	**Pasukan Kecil Keselamatan ICT DOA**	
	Keanggotaan pasukan kecil ini adalah seperti berikut: **Pengerusi**: Pengurus ICT **Ahli**: a. Pegawai Teknologi Maklumat b. Penolong Pegawai Teknologi Maklumat c. Wakil Unit ICT dari semua DOA (*ICT Desk Officer*) **Urus Setia**: ICTSO **Bidang tugas**: a. Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; b. merekod dan menjalankan siasatan awal insiden yang diterima; c. menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d. menghubungi dan melaporkan insiden yang berlaku kepada CERT MOA dan GCERT MAMPU sama ada sebagai *input* atau untuk tindakan seterusnya; e. menasihati DOA mengambil tindakan pemulihan dan pengukuhan dengan kerjasama bersama CERT MOA; f. menyebarkan makluman berkaitan dengan DOA dengan kerjasama bersama CERT MOA; dan g. menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan dengan kerjasama bersama CERT MOA bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	CERT DOA

DM 0202	Pihak Luar/ Asing	
DM-020201	**Keperluan Keselamatan Kontrak Dengan Pihak Luar/ Asing**	
	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; c. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak luar/asing. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. Dasar Keselamatan ICT DOA; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek.	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem dan Rangkaian ICT dan Pihak Ketiga (Luar/ Asing)

Perkara 03 PENGURUSAN ASET

Objektif : Untuk memberi perlindungan keselamatan yang bersesuaian ke atas semua aset ICT Jabatan Pertanian Malaysia.

DM-0301	**Akauntabiliti Aset**	
DM-030101	**Inventori Aset**	
	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 dikenal pasti dan maklumat aset di rekod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini; b. memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c. memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di DOA; dan d. peraturan bagi pengendalian aset hendaklah dikenal pasti, di dokumen dan dilaksanakan.	Pentadbir Sistem, Semua
DM-0302	**Pengelasan dan Pengendalian Maklumat**	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.		
DM-030201	**Pengelasan Maklumat**	
	Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya oleh Pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	Semua

DM-030202	Pengendalian Maklumat	
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, pertukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan berikut : a. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. memeriksa maklumat dan menentukan ia 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.	Semua

Perkara 04 KESELAMATAN SUMBER MANUSIA

Objektif: Untuk memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan DOA, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga DOA hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

DM-0401	**Keselamatan ICT Dalam Tugas Harian**	
DM-040101	**Sebelum Perkhidmatan**	
	Ini bertujuan memastikan pegawai dan kakitangan DOA, 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. Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan DOA, pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan DOA, 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.	Semua
DM-040102	**Dalam Perkhidmatan**	
	Ini bertujuan memastikan pegawai dan kakitangan DOA, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong Dasar Keselamatan ICT DOA dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan pegawai dan kakitangan DOA, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan mengurus keselamatan aset	Semua

	ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh DOA; b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT DOA secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa; c. memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan DOA,pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh DOA; dan d. memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pihak pengguna boleh merujuk kepada Bahagian Pembangunan Sumber Manusia, DOA.	
DM-040103	**Bertukar Atau Tamat Perkhidmatan**	
	Ini bertujuan memastikan pertukaran atau tamat perkhidmatan pegawai dan kakitangan DOA, 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 DOA 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 DOA dan/atau terma perkhidmatan.	Semua

Perkara 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif : Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan dan ancaman.

DM-0501	**Keselamatan Kawasan**	
DM-050101	**Kawalan Kawasan**	
	Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat DOA. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. menggunakan keselamatan *perimeter* (halangan seperti dinding, pagar kawalan, pengawal keselamatan)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 di dalam pejabat, bilik dan kemudahan ; d. mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana disebabkan oleh kuasa Tuhan atau perbuatan manusia; e. melaksana perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan f. memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Pejabat Ketua Pegawai Keselamatan Kerajaan, CIO dan ICTSO, Pegawai Keselamatan DOA
DM-050102	**Kawalan Masuk Fizikal**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pengguna DOA hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Setiap pelawat boleh mendapatkan Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah	Semua dan pelawat

	dikembalikan semula selepas tamat lawatan; c. Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pengguna berhenti atau bersara; d. Setiap pelawat hendaklah mendaftar di pintu utama di setiap aras terlebih dahulu; e. Kehilangan pas mestilah dilaporkan dengan segera; f. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau mengguna aset ICT DOA.	
DM-050103	**Kawalan Larangan**	
	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di DOA adalah bilik Ketua Pengarah, bilik-bilik Timbalan Ketua Pengarah, Bilik-bilik Pengarah Bahagian, bilik sulit, bilik Server dan Pusat Data (Data Centre) DOA. a. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan c. Semua penggunaan peralatan yang melibatkan penghantaran, kemaskini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	Pentadbir Sistem dan Rangkaian
DM-0502	**Keselamatan Peralatan**	
DM-050201	**Peralatan ICT**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna hendaklah menyemak semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; c. pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;	Semua

	d. pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; e. pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; f. pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g. semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna; h. setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; i. peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); j. semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; k. semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan *(air ventilation)* yang sesuai; l. peralatan ICT yang hendak dibawa keluar dari premis DOA, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan; m. peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden; n. pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; o. pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ianya ditempatkan tanpa kebenaran Pentadbir Sistem ICT; p. sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk di baik pulih; q. sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang	

	lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; r. konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal; s. pengguna dilarang sama sekali mengubah *password administrator* yang telah ditetapkan oleh pihak ICT; t. pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi Jabatan sahaja; u. pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "OFF" apabila meninggalkan pejabat; dan v. memastikan plag dicabut daripada main switch bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
DM-050202	**Media Storan**	
	Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Bagi menjamin keselamatan, langkah-langkah berikut perlu diambil: a. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; b. bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu; c. semua media storan data yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat; d. semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; e. media storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang dikategorikan selamat. Akses untuk memasuki	Semua

	kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; f. akses dan pergerakan kepada media storan perlu direkodkan; g. perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; dan h. mengadakan salinan atau penduaan (*data backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data.	
DM-050203	**Media Tandatangan Digital**	
	Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah-langkah berikut: a. pegawai hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b. tidak boleh dipindah-milik atau dipinjamkan; dan c. sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Semua
DM-050204	**Media Perisian dan Aplikasi**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan Jabatan; b. Sistem aplikasi dalaman tidak dibenarkan diagih/ didemontrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c. Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada CD-ROM, disk atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan d. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua
DM-050205	**Penyelenggaraan**	
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil	Semua dan Pegawai Aset

	termasuklah seperti berikut: a. Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; b. Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; c. Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; d. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan e. Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	
DM-050206	**Peminjaman Perkakasan Untuk Kegunaan di Luar Pejabat**	
	Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan: a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	Semua
DM-050207	**Peralatan di Luar Premis**	
	Perkakasan yang dibawa keluar dari premis DOA adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua
DM-050208	**Pelupusan**	
	Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh DOA ataupun tidak dan ditempatkan di DOA sendiri.	Semua, Pegawai Aset dan STPM

	Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan DOA. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; e. Peralatan yang hendak di lupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; f. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori MyAsset; g. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan h. Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:- i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, Hard disk, Motherboard dan sebagainya. ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di jabatan. iii. Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan. iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab DOA.	

	v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
DM-050209	**Clear Desk dan Clear Screen**	
	Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; b. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci; dan c. Dokumen yang mengandungi bahan-bahan sensitif hendaklah diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	Semua
DM-0503	**Keselamatan Persekitaran**	
DM-050301	**Kawalan Persekitaran**	
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil : a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan pengkomputeran hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;	Semua

	c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan pengkomputeran; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu. h. Kabel komputer juga hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: i. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat; ii. menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; dan Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*.	
DM-050302	**Bekalan Kuasa**	
	Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti UPS (*Uniterruptible Power Supply*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik Server supaya mendapat bekalan kuasa berterusan; dan	STPM, ICTSO, Semua

	c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	
DM-050303	**Prosedur Kecemasan**	
	a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan oleh Pegawai Keselamatan Jabatan; b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut pejabat ; c. Mengadakan, menguji dan mengemas kini pelan kecemasan dari semasa ke semasa; dan d. Mengadakan latihan *fire drill* mengikut jadual.	Semua dan Pegawai Keselamatan Jabatan
DM-0504	**Keselamatan Dokumen**	
DM-050401	**Dokumen**	
	Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi: a. Memastikan sistem penyampaian dokumentasi mempunyai ciri-ciri keselamatan; b. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada; c. Setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; d. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; e. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; f. Pelupusan dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan g. Menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Semua

Perkara 06 PENGURUSAN OPERASI DAN KOMUNIKASI

Objektif: Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.		
DM-0601	**Pengurusan Prosedur Operasi**	
DM-060101	**Pengendalian Prosedur**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumentasikan, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang lengkap, teratur dan jelas seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa mengikut keperluan.	Semua
DM-060102	**Kawalan Perubahan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja ataupun tidak.	Semua

DM-060103	**Pengasingan Tugas dan Tanggungjawab**	
	Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahan yang tidak dibenarkan ke atas aset ICT. Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pengurus ICT, ICTSO
DM-0602	**Perancangan dan Penerimaan Sistem**	
DM-060201	**Perancangan Kapasiti**	
	Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem ICT, ICTSO
DM-060202	**Penerimaan Sistem**	
	Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT, ICTSO
DM-0603	**Perisian Berbahaya**	
DM-060301	**Perlindungan dari Perisian Berbahaya**	
	Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT dari perisian berbahaya: a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus dan *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;	Semua

	c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d. Mengemas kini antivirus dengan paten antivirus yang terkini; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini akan digunakan sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
DM-0604	***Housekeeping***	
DM-060401	***Backup***	
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan *backup* seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan *backup* hendaklah direkodkan dan disimpan di *offsite*. a. Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat *backup* ke atas semua data dan maklumat mengikut kesesuaian operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; c. Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d. *Backup* hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan	Semua

	backup bergantung pada tahap kritikal maklumat; e. DOA hendaklah menyimpan sekurang-kurangnya tiga (3) generasi *backup;* dan f. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	
DM-060402	**Sistem Log**	
	Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara seperti berikut: a. Mewujudkan sistem log bagi merekod 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 tidak sah lain seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah dilaporkan kepada ICTSO dan CIO.	Pentadbir Sistem ICT
DM-0605	**Pengurusan Rangkaian**	
DM-060501	**Kawalan Infrastruktur Rangkaian**	
	Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut :- a. Semua tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta di konfigurasi oleh	STPM, ICTSO

	kontraktor penyelenggara dan diselia oleh Pentadbir Sistem; e. Semua trafik keluar dan masuk Ibu Pejabat Pertanian hendaklah melalui *firewall* di bawah kawalan DOA; f. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer peribadi kecuali mendapat kebenaran ICTSO; g. Memasang perisian *Intrusion Detection System* (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat DOA; h. Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti kemasukan dari atau capaian pada laman web/Internet yang mengandungi maklumat atau unsur-unsur tidak sihat dan berbahaya yang boleh menjejaskan integriti kakitangan, sistem dan maklumat; i. Sebarang penyambungan rangkaian yang bukan di bawah kawalan DOA hendaklah mendapat kebenaran ICTSO; j. Semua pengguna hanya dibenarkan menggunakan rangkaian DOA sahaja di mana penggunaan modem adalah dilarang sama sekali; dan k. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.	
DM-0606 Pengurusan Media		
DM-060601 Penghantaran dan Pemindahan		
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Semua
DM-060602 Prosedur Pengendalian Media		
	Prosedur-prosedur pengendalian media termasuk: a. Melabelkan semua media mengikut tahap keselamatan sesuatu maklumat; b. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;	Semua

	d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	
DM-060603 Keselamatan Sistem Dokumentasi		
	a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyediakan dan memantapkan lagi keselamatan sistem dokumentasi dalam rangkaian; dan c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	Semua
DM-060604 Maklumat Umum		
	Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: a. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b. Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan c. Memastikan segala maklumat yang hendak dipaparkan telah disahkan dan diluluskan sebelum dimuat naik ke laman web.	Semua
DM-0607 Pengurusan Pertukaran Maklumat		
	Pengurusan Pertukaran Maklumat bertujuan untuk memastikan keselamatan pertukaran maklumat dan perisian antara DOA dan agensi luar terjamin. Langkah-langkah bagi Pengurusan Pertukaran Maklumat adalah seperti berikut: a. Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;	Semua

	b. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara DOA dengan pihak luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari DOA; 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 DOA.	
DM-0608	**Pengurusan Mel Elektronik (E-mel)**	
	Penggunaan e-mel di DOA hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di DOA-DOA Kerajaan" dan mana-mana undang-undang bertulis yang berkuat kuasa: Di antara langkah-langkah pengendalian mel elektronik termasuk: a. Mengehadkan jenis dan saiz fail lampiran bagi tujuan mengelakkan jangkitan virus dan serangan e-mel *bombing.* Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu tidak melebihi sepuluh megabait (10 Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; b. Penghantaran e-mel rasmi hendaklah menggunakan e-mel rasmi kerajaan sahaja dan hendaklah memastikan alamat e-mel penerima adalah betul; c. Penggunaan e-mel rasmi jabatan bagi tujuan peribadi adalah tidak dibenarkan; d. Pengguna hendaklah mengelak daripada membuka e-mel dari penghantar yang tidak diketahui atau diragui; e. Penghantaran lampiran dalam format/*extension* " **.exe, *.bat* " dan " **.com*" tidak dibenarkan; f. Hanya kakitangan DOA sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi DOA;	Semua

	g. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; h. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; i. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; j. Pihak Bahagian Pengurusan atau bahagian masing-masing perlu memaklumkan sebarang status pengguna (bertukar jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke DOA) di pejabat masing-masing bagi tujuan pengemaskinian e-mel yang terlibat; k. Pengguna adalah mewakili diri sendiri dan bertanggungjawab ke atas maklumat yang dikeluarkan dalam setiap perhubungan yang dibuat secara elektronik. l. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing. Pembersihan e-mel hendaklah dibuat secara berkala sekurang-kurangnya 2 bulan sekali.	
DM-0609	**Perkhidmatan E-Dagang**	
	Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. Perkara-perkara yang perlu dipatuhi adalah seperti 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	Semua

	pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	
DM-0610 Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak Lain Yang Terlibat		
	Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a. Memasukkan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan 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 semasa ke semasa; dan c. Pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyenggara dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	ICTSO, STPM
DM-0611 Pemantauan		
	Ianya bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, di antaranya 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 di wujud dan hasilnya perlu dipantau secara berkala; c. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d. Aktiviti pentadbiran dan operator sistem perlu direkodkan;	Pentadbir Sistem ICT, ICTSO, STPM

	e. Kesalahan, kesilapan dan / atau penyalahgunaan perlu di log, dianalisis dan diambil tindakan sewajarnya; dan f. Masa yang berkaitan dengan sistem pemprosesan maklumat dalam DOA atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.	

Perkara 07 KAWALAN CAPAIAN

Objektif : Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT DOA.		
DM-0701 Dasar Kawalan Capaian		
DM-070101 Keperluan Kawalan Capaian		
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu di rekod, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d. Kawalan ke atas kemudahan pemprosesan maklumat.	STPM, ICTSO
DM-0702 Pengurusan Capaian Pengguna		
Objektif : Mengawal capaian pengguna ke atas aset ICT DOA.		
DM-070201 Akaun Pengguna		
	Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: a. akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b. akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. akaun pengguna yang di wujud pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d. pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan.	Semua, Pentadbir Sistem ICT

	Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f. pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i) Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) minggu ii) Bertukar bidang tugas kerja; iii) Bertukar ke agensi lain; iv) Bersara; atau v) Ditamatkan perkhidmatan	
DM-070202	**Hak Capaian**	
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Semua
DM-070203	**Pengurusan Kata Laluan**	
	Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh DOA seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c. panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf dan nombor (alphanumerik); d. kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. kata laluan w*indows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f. kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g. kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas	Semua

	kata laluan diset semula; h. kata laluan hendaklah berlainan daripada pengenalan identiti pengguna. i. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan j. Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
DM-070204	**Kad Pintar**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan kad pintar kerajaan elektronik (Kad EG) hendaklah digunakan bagi capaian sistem kerajaan elektronik yang dikhususkan. Proses permohonan kad pintar hendaklah dibuat melalui Bahagian Pengurusan. b. Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain. c. Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat. d. Sebarang kehilangan, kerosakan dan kata laluan disekat terhadap kad pintar perlu dimaklumkan kepada pihak Bahagian Pengurusan.	Semua
DM-0703	**Capaian Sistem Pengoperasian**	
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; b. merekodkan capaian yang berjaya dan gagal; dan c. membekalkan kemudahan untuk pengesahan; bagi sistem kata kunci digunakan, kualiti kata kunci perlu mendapat pengesahan. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan;	Pentadbir Sistem ICT, ICTSO

	b. mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* c. menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; dan d. menyediakan tempoh penggunaan mengikut kesesuaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mengawal capaian ke atas sistem pengoperasian 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 bagi satu tempoh yang ditetapkan; dan e. mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
DM-0704	**Capaian Aplikasi dan Maklumat**	
	Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di DOA adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; b. setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log) bagi mengesan aktiviti-aktiviti yang tidak diingini;	Pentadbir Sistem ICT, ICTSO

	c. mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; d. memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; e. capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; dan f. sebarang maklumat yang perlu dimuat naik ke portal atau laman web hendaklah mendapat kebenaran daripada Pengarah Bahagian masing-masing.	
DM-0705	**Capaian Jarak Jauh**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penghantaran maklumat yang menggunakan capaian jarak jauh menggunakan kaedah ***Remote Access*** mestilah menggunakan kaedah penyulitan (*encryption*). b. Lokasi bagi akses ke sistem ICT DOA hendaklah dipastikan selamat. c. Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada CIO. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	Semua
DM-0706	**Capaian Internet**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan Internet di DOA hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code,* virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian DOA. b. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya. c. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan.	Pentadbir Rangkaian Pengurus ICT

	d. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing*, *video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan. e. Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali. f. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Pengarah/pegawai yang diberi kuasa; g. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; h. Bahan rasmi hendaklah disemak dan mendapat pengesahan dari Pengarah Bahagian sebelum dimuat naik ke Internet; i. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; j. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh DOA; k. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board.* Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan dari CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; l. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian Internet. ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah. m. Pengguna hendaklah berhenti dan memutuskan talian dengan serta merta sekiranya menerima dan disambungkan ke laman Internet yang mengandungi unsur-unsur tidak menyenangkan.	Semua

DM-0707	Pengauditan dan Forensik ICT	
	ICTSO mestilah bertanggungjawab merekod dan menganalisa perkara-perkara berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT DOA; 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 *bandwidth* rangkaian; g. aktiviti penyalahgunaan akaun e-mel; dan h. aktiviti penukaran *IP address* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT. Langkah-langkah yang perlu diambil adalah seperti berikut: a. ICTSO akan menentukan prosedur pengumpulan bahan bukti (*hard disk*/media storan) yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan. b. Proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat. c. Sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, laporan khas perlu disediakan. Semua proses dan hasil siasatan adalah SULIT.	ICTSO

DM-0708	Jejak Audit	
	Setiap sistem mestilah mempunyai jejak audit. 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 untuk 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.	Pentadbir Sistem ICT

Perkara 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Objektif : Memastikan sistem yang dibangunkan atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

DM-0801	**Keselamatan dalam Membangunkan Sistem dan Aplikasi**	
DM-080101	**Keperluan Keselamatan Sistem Maklumat**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; c. Aplikasi perlu mengandungi semakan pengesahan (validation) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pemilik Sistem, Pentadbir Sistem ICT, ICTSO
DM-080102	**Pengesahan Data Input**	
	Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.	Pentadbir Sistem ICT
DM-080103	**Kawalan Prosesan**	
	Kawalan prosesan perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan.	Pentadbir Sistem ICT
DM-080104	**Pengesahan Data Output**	
	Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pentadbir Sistem ICT

DM-0802	**Kawalan Kriptografi**	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui teknik kriptografi. Ini termasuk membangun kawalan kegunaan dan melaksanakan suatu peraturan kawalan kriptografi dan pengurusan kunci yang digunakan untuk menyokong teknik kriptografi bagi melindungi maklumat.		
DM-080201	**Enkripsi**	
	Setiap pengguna hendaklah membuat penyulitan / enkripsi (*encryption*) ke atas maklumat sensitif atau kritikal atau maklumat rahsia rasmi bagi mengelakkan dari pendedahan dan penyelewengan maklumat berlaku.	Semua
DM-080202	**Tandatangan Digital**	
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
DM-080203	**Pengurusan Infrastruktur Kunci Awam (PKI)**	
	Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, di musnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua
DM-0803	**Keselamatan Fail Sistem**	
	Fail sistem perlu dikawal dan dikendalikan dengan baik dan selamat. Antara kawalan dan pengendalian tersebut adalah: a. Proses pengemas kini fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan e. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem ICT

DM-0804 Pembangunan dan Sokongan Sistem		
Objektif: Memastikan keselamatan perisian sistem aplikasi dan maklumat dikawal supaya selamat dalam semua keadaan.		
DM-080401 Perubahan Prosedur		
	Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum diguna pakai. Perkara-perkara yang perlu dipatuhi adalah termasuk 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 DOA; c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d. Menghalang sebarang peluang untuk membocorkan maklumat; e. Mengawal selia dan memantau pembangunan perisian oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat.	Pemilik Sistem, Pentadbir Sistem ICT
DM-080402 Pembangunan Secara *Outsource*		
	Pembangunan perisian aplikasi secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber *(source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik DOA.	STPM, Pentadbir Sistem ICT
DM-080403 Kawalan dari Ancaman Teknikal		
	Kawalan teknikal keterdedahan (vulnerability) perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b. Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; c. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT

Perkara 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

Objektif : Untuk memastikan semua insiden dikendalikan dengan cepat dan berkesan serta memastikan sistem ICT DOA dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej DOA dan sistem penyampaian perkhidmatan awam.

DM-0901	**Mekanisme Pelaporan Insiden Keselamatan ICT**	
	Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera: 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: i. hilang, dicuri atau didedahkan ii. 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 insiden-insiden yang tidak diingini. Sekiranya berlaku insiden keselamatan ICT, maka mekanisme pelaporan adalah seperti berikut: a. **Pelaporan** Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO dan kepada CERT MOA untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. b. **CERT MOA** Pasukan Keselamatan Kecil DOA / CERT MOA akan bertindak menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai *input* atau untuk tindakan seterusnya. c. **Tanggungjawab Pengguna** Semua kakitangan, pembekal, pakar runding dan pihak-pihak lain yang terlibat diingatkan supaya tidak	Semua Semua Pasukan Keselamatan Kecil DOA/ CERT MOA Semua

	melaksanakan sebarang tindakan secara sendiri, tapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden keselamatan ICT kepada ICTSO, kerentanan (*vulnerabality*) yang diperhatikan atau disyaki terdapat dalam sistem maklumat menerusi mekanisme pelaporan ini. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan menceroboh. 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. Prosedur pelaporan insiden keselamatan ICT berdasarkan: a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan b. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	CIO, ICTSO
DM-0902	**Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT**	
	Semua pegawai ICT dari Pasukan Kecil Keselamatan ICT DOA akan bekerjasama dengan pegawai pasukan pengendali insiden keselamatan ICT atau CERT MOA dalam melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur operasi standard keselamatan CERT MOA dan GCERT. Pasukan Kecil Keselamatan ICT DOA akan menerima aduan atau laporan daripada pengguna, laporan yang dikesan dari IPS Jabatan atau laporan dari sumber luar. Seterusnya, maklumat tentang insiden akan didaftarkan. Siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden tersebut. Laporan insiden kemudiannya dimaklumkan kepada CERT MOA dan GCERT MAMPU. Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan dipanjangkan kepada DOA penguat kuasa undang-undang. Pasukan Kecil Keselamatan ICT DOA yang diketuai oleh ICTSO akan menjalankan tindakan pengendalian secara capaian jarak jauh (*remote*) atau *on-site.* Sekiranya laporan tersebut memerlukan bantuan CERT MOA dan GCERT MAMPU, permohonan akan dihantar bagi mendapatkan maklum balas GCERT MAMPU.	ICTSO

	Bagi laporan yang memerlukan bantuan daripada CERT Agensi lain, permohonan akan dihantar melalui GCERT MAMPU dan khidmat nasihat akan disalurkan. CERT MOA seterusnya akan menyediakan laporan dan ICTSO mengesahkan sekiranya Pelan Kesinambungan Perkhidmatan / *Business Resumption Plan* (*BRP*) perlu diaktifkan atau sebaliknya. Pengesahan akan dihantar kepada CIO bagi mengaktifkan *BRP*. Laporan insiden yang tidak memerlukan *BRP* akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan. Carta lengkap mengenai perjalanan laporan insiden seperti di Lampiran 2.	

Perkara 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

DM-1001	**Pelan Kesinambungan Perkhidmatan**	
	Pelan Kesinambungan Perkhidmatan (*Business Continuity Management* - BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JKICT DOA dan perkara-perkara berikut perlu diberi perhatian: a. mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; c. mendokumentasikan proses dan prosedur yang telah dipersetujui; d. mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; e. membuat *backup*; dan f. menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	Pengurus ICT

DM-1002	Pengurusan Kesinambungan Perkhidmatan	
	Pengurusan Kesinambungan Perkhidmatan adalah mekanisme bagi mengurus dan memastikan kepentingan *stakeholder* sistem penyampaian perkhidmatan dilindungi dan imej DOA terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan DOA di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan. Ketua Pengarah Pertanian adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT DOA.	Pengurus ICT, ICTSO, CIO

Perkara 11 PEMATUHAN

Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT DOA.

DM-1101	**Pematuhan dan Keperluan Perundangan**	
	Setiap pengguna di DOA hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT DOA dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di DOA termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT DOA selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber DOA.	Semua
DM-1102	**Pematuhan Dengan Dasar, Piawaian dan Keperluan Teknikal**	
	ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
DM-1103	**Pematuhan Keperluan Audit**	
	Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua
DM-1104	**Keperluan Perundangan**	
	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di DOA: a. Arahan Keselamatan; b. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar	Semua

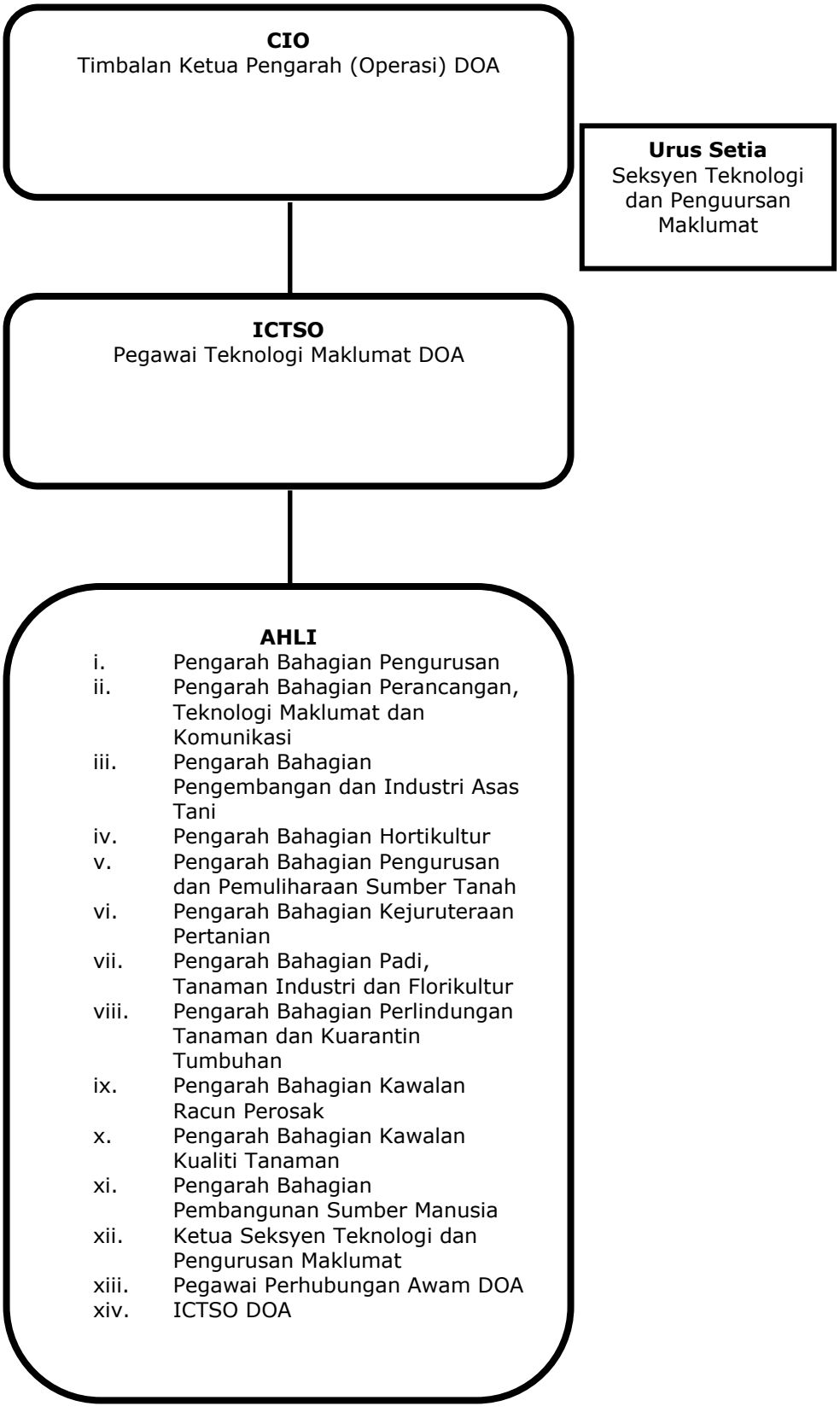
	Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan; c. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook*(MyMIS); d. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan; f. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; g. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; h. Surat Arahan Ketua Setiausaha Negara - Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006; i. Surat Arahan Ketua Pengarah MAMPU - Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan yang bertarikh 1 Jun 2007; j. Surat Arahan Ketua Pengarah MAMPU - Langkah-langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-agensi Kerajaan yang bertarikh 23 November 2007; k. Surat Pekeliling Am Bilangan 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK); l. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)- Tatacara Penyediaan, Penilaian dan Penerimaan Tender; m. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan; n. Akta Tandatangan Digital 1997; o. Akta Rahsia Rasmi 1972; p. Akta Jenayah Komputer 1997; q. Akta Hak cipta (Pindaan) Tahun 1997; r. Akta Komunikasi dan Multimedia 1998; s. Perintah-Perintah Am; t. Arahan Perbendaharaan; u. Arahan Teknologi Maklumat 2007;	
DM-1105	**Pelanggaran Dasar**	
	Pelanggaran Dasar Keselamatan ICT DOA boleh dikenakan tindakan tatatertib.	Semua

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CERTDOA	Organisasi yang ditubuhkan untuk membantu DOA mengurus pengendalian insiden keselamatan ICT di DOA masing-masing dan DOA di bawah kawalannya.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan s maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft / espionage*), penipuan (*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
ICT	*Information and Communication Technology*. (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* (Pegawai Keselamatan ICT) Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(Server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.

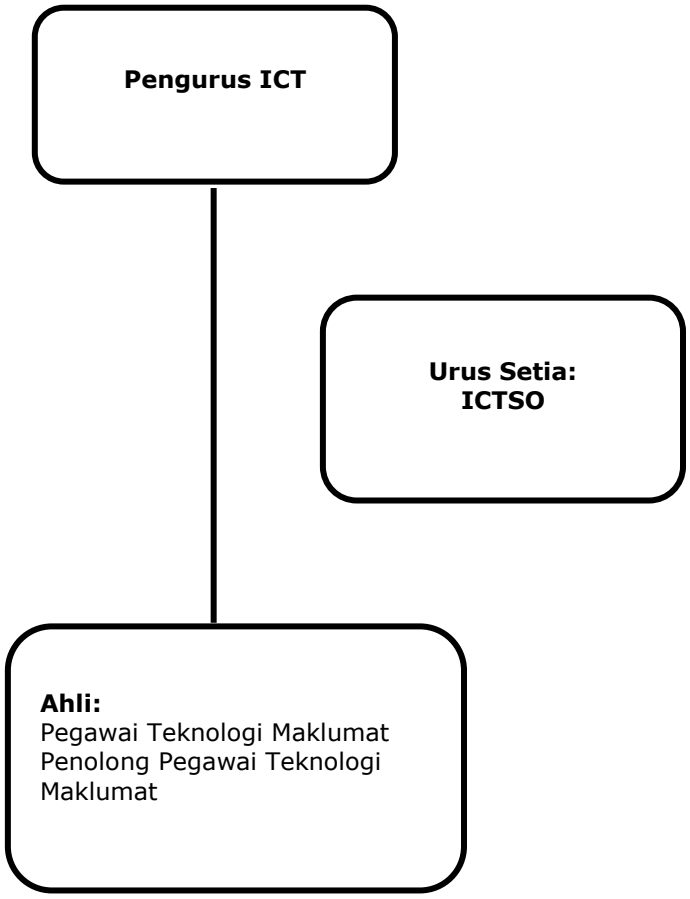
GLOSARI	
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
STPM	Seksyen Teknologi dan Pengurusan Maklumat, Bahagian Perancangan, Teknologi Maklumat dan Komunikasi
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense Multiple Access/Collision Detection (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran 1

Carta 1 (a) : Struktur Organisasi Jawatankuasa Pemandu ICT/Keselamatan ICT DOA

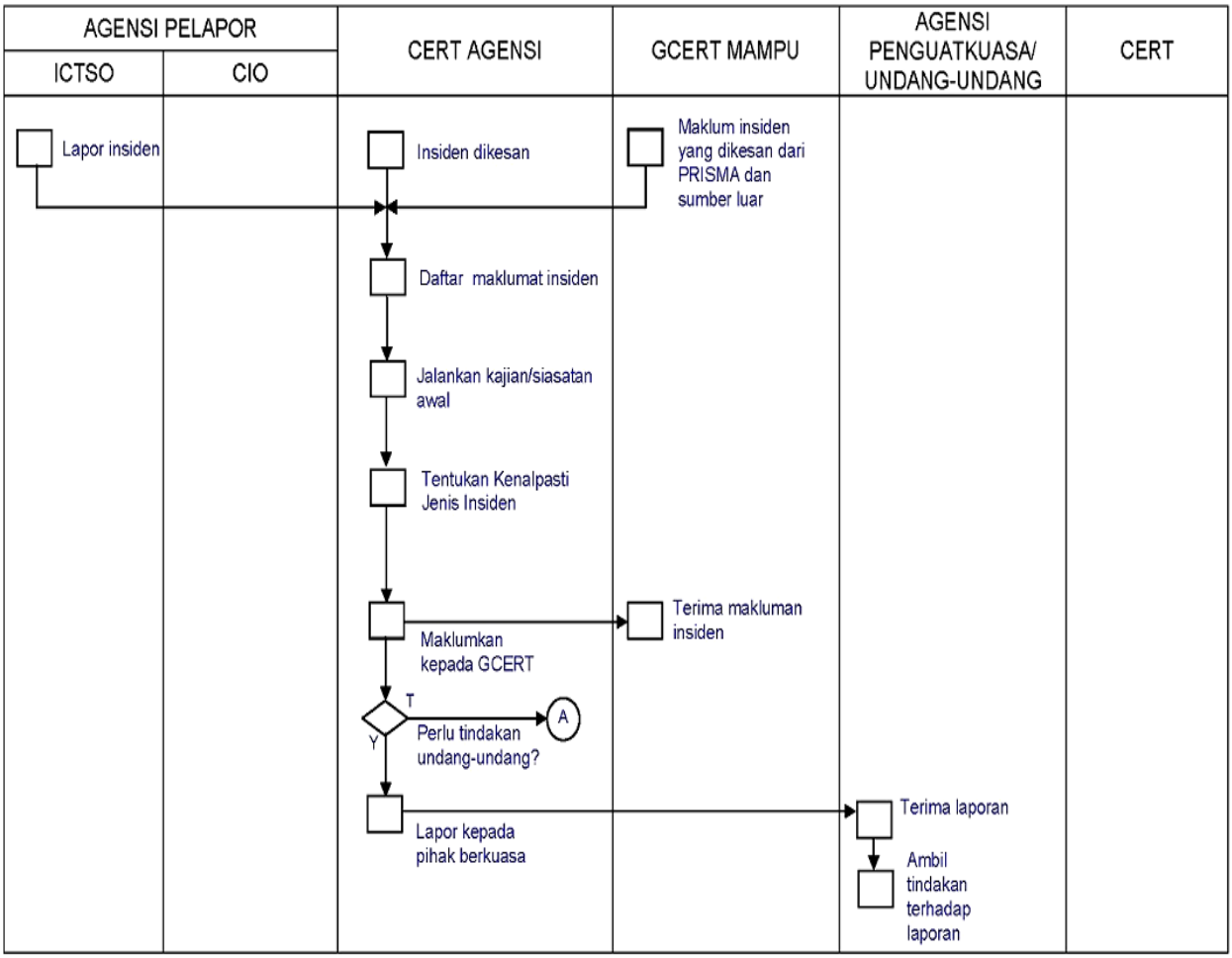


Carta 1 (b) : Struktur Organisasi Pasukan Kecil Keselamatan ICT Jabatan Pertanian (CERT DOA)

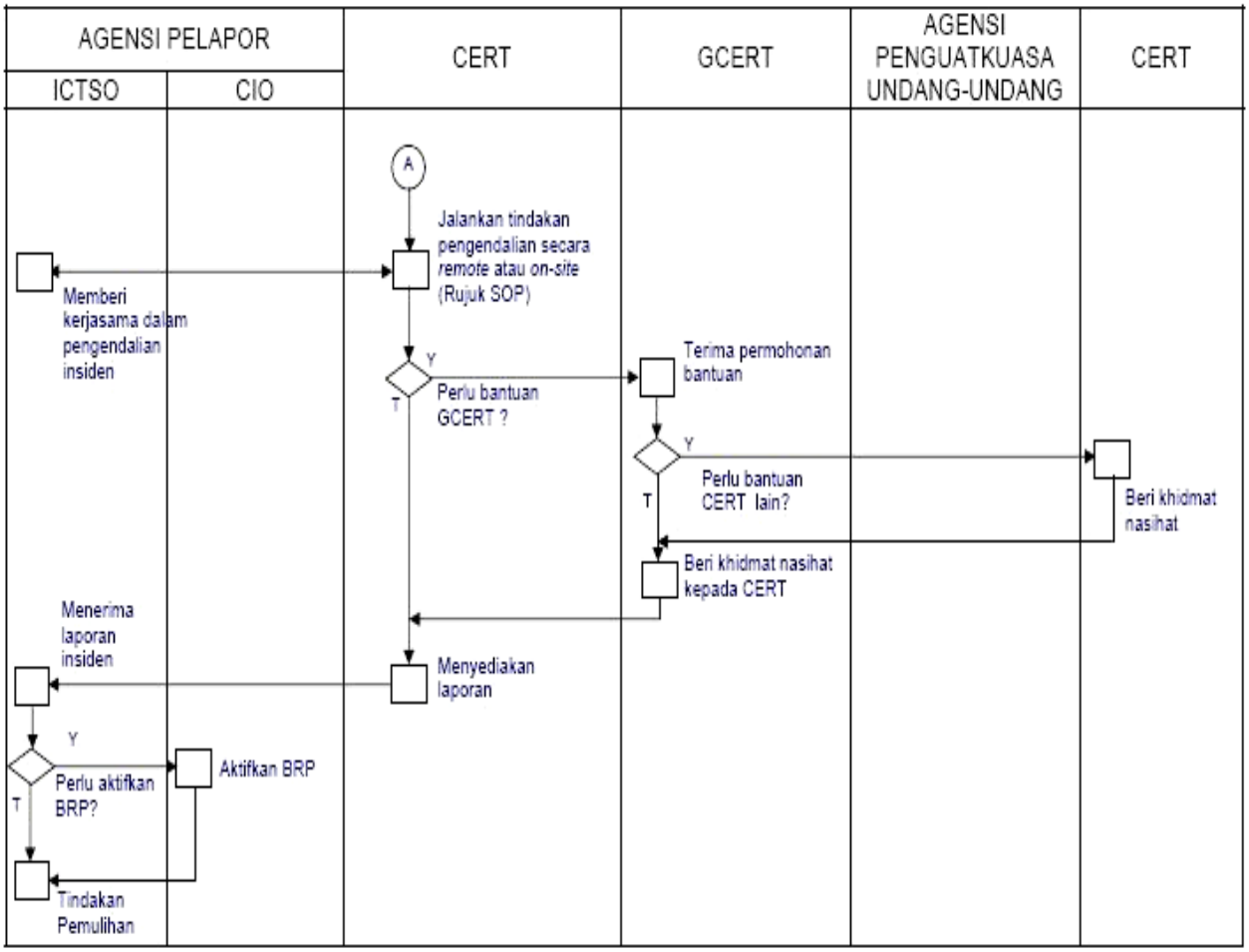


Lampiran 2

Rajah 1 : Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT
DOA



Rajah 2: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT DOA



Lampiran 3

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT JABATAN PERTANIAN

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan dan Gred Perkhidmatan : .....

Bahagian : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya juga telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT DOA; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....
(Tandatangan)
Nama :
Alamat Pejabat Penempatan :

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....
(Tandatangan Pegawai Keselamatan ICT)
b.p Ketua Pengarah Pertanian

Tarikh : .....