PENGENALAN

Dasar Keselamatan ICT (DKICT) Jabatan Perkhidmatan Veterinar Malaysia (DVS) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna di DVS, Institut dan Pusat di bawah DVS mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT di DVS, 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 (*malicious codes*) 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 DVS diwujudkan untuk menjamin kesinambungan urusan DVS dengan meminimumkan kesan insiden keselamatan ICT.

Objektif utama Dasar Keselamatan ICT DVS adalah seperti berikut:-

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

(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.

PERNYATAAN DASAR

Dasar Keselamatan ICT DVS 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.

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.

SKOP

Dasar Keselamatan ICT DVS 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.

Dasar Keselamatan ICT DVS 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 DVS. 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, perisi an sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada DVS;

(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 DVS. Contoh: sistem dokumentasi, prosedur operasi, rekod-rekod DVS, 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 DVS bagi mencapai misi dan objektif DVS. 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 DVS perlu dilaksanakan secara konsisten dengan undang-undang dan peraturan yang sedia ada.

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

PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT DVS 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 samada 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, mengemaskini, 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. Bagi 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 DVS 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

(iii) 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 DVS dan perundangan yang berkaitan.		
DM-0101	**Perlaksanaan Dasar**	
	Pelaksanaan dasar ini dijalankan oleh Ketua Pengarah Perkhidmatan Veterinar dibantu oleh Jawatankuasa Keselamatan ICT DVS .	Ketua Pengarah Perkhidmatan – Veterinar
DM-0102	**Penyebaran Dasar**	
	Dasar ini perlu disebarkan kepada semua warga Jabatan Perkhidmatan Veterinar.	ICTSO, STM
DM-0103	**Penyelenggaraan Dasar**	
	Dasar Keselamatan ICT DVS 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 DVS: 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 Perkhidmatan Veterinar; c. perubahan yang telah dipersetujui oleh JKICT Jabatan Perkhidmatan Veterinar 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 DVS adalah terpakai kepada semua pengguna ICT Jabatan Perkhidmatan Veterinar dan tiada pengecualian diberikan.	Warga DVS/ Pengguna Sistem

PERKARA 02 KESELAMATAN ORGANISASI

Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT DVS.		
DM-0201	**Infrastruktur Organisasi Dalaman**	
DM-020101	**Ketua Pengarah Perkhidmatan Veterinar**	
	Peranan dan tanggungjawab Ketua Pengarah Perkhidmatan Veterinar adalah seperti berikut: a. memahami dan mematuhi Dasar Keselamatan ICT DVS; b. memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT DVS; c. memastikan semua pengguna mematuhi Dasar Keselamatan ICT DVS; 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 DVS.	Ketua Pengarah Perkhidmatan Veterinar (KPPV)
DM-020102	**Ketua Pegawai Maklumat (CIO)**	
	Ketua Pengarah Perkhidmatan Veterinar boleh melantik dirinya atau Timbalan Ketua Pengarah Perkhidmatan Veterinar sebagai Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab beliau adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DVS; b. bertanggungjawab ke atas perkara – perkara yang berkaitan dengan keselamatan ICT DVS; c. membantu Ketua Pengarah Perkhidmatan	CIO

	Veterinar 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 DVS dan pengauditan; f. mempengerusikan Jawatankuasa Pemandu ICT (JPICT).	
DM-020103	**Pegawai Keselamatan ICT (ICTSO)**	
	Jawatan ICTSO bagi DVS adalah merupakan Pegawai Teknologi Maklumat (PTM) yang berperanan dan bertanggungjawab seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DVS; b. Mengurus keseluruhan program-program keselamatan ICT DVS; c. menguatkuasakan pelaksanaan Dasar Keselamatan ICT DVS; d. memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT DVS kepada semua pengguna; e. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT DVS; f. menjalankan pengurusan risiko; g. menjalankan audit, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya ; h. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; i. melaporkan insiden keselamatan ICT kepada	ICTSO

	Pasukan Tindak balas Insiden Keselamatan ICT (CERT) MOA dan memaklumkannya kepada CIO; j. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; k. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT DVS; dan l. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	
DM-020104	**Pengurus ICT**	
	Ketua Seksyen Teknologi Maklumat (STM) adalah merupakan Pengurus ICT DVS. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. memahami dan mematuhi Dasar Keselamatan ICT DVS; b. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan DVS; c. menentukan kawalan akses semua pengguna terhadap aset ICT DVS; d. melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; e. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT DVS. f. memastikan semua pengguna mematuhi Dasar Keselamatan ICT DVS;	Pengurus ICT
DM-020105	**Pentadbir Sistem Aplikasi**	
	Tanggungjawab Pentadbir Sistem adalah seperti berikut:	Pentadbir Sistem ICT

	a. Menandatangani Surat Lantikan Pentadbir Sistem oleh CIO/Pengarah Bahagian melalui Borang Lantikan Pentadbir Sistem b. Memahami dan mematuhi Dasar Keselamatan ICT DVS; c. Mengemaskini dengan segera apabila dimaklumkan mengenai kakitangan yang bersara, berhenti, dipecat atau berlaku perubahan dalam bidang tugas termasuk yang dikenakan tindakan tatatertib; d. menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT DVS; e. memantau aktiviti capaian harian pengguna; f. bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan baik; g. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatal atau memberhentikannya dengan serta-merta; h. menyimpan dan menganalisis rekod jejak audit; i. menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala. j. Melaporkan sebarang insiden atau berlaku kecurigaan kepada pentadbir sistem ICT	
DM-020106	**Pentadbir Sistem ICT**	
	Tanggungjawab Pentadbir Sistem adalah seperti berikut: a. Memahami dan mematuhi Dasar Keselamatan ICT DVS; b. Mengemaskini dengan segera apabila dimaklumkan mengenai kakitangan yang	Pentadbir Sistem ICT

	bersara, berhenti, dipecat atau berlaku perubahan dalam bidang tugas termasuk yang dikenakan tindakan tatatertib; c. menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT DVS; 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.	
DM-020107	**Pengguna**	
	Pengguna adalah Warga DVS atau mana-mana individu yang diberi hak capaian ke atas sistem aplikasi DVS. Peranan dan tanggungjawab pengguna adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DVS; b. mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; d. mematuhi prinsip-prinsip Dasar Keselamatan	Pengguna Sistem

	ICT DVS dan menjaga kerahsiaan maklumat DVS; e. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; f. menghadiri program-program kesedaran mengenai keselamatan ICT sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; dan g. menandatangani "Surat Akuan Pematuhan" (Lampiran 3) bagi mematuhi Dasar Keselamatan ICT DVS.	
DM-020108	**Jawatankuasa Pemandu ICT DVS**	
	Jawatankuasa Pemandu ICT (JPICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT DVS. Keanggotaan DVS adalah seperti berikut: **Pengerusi** : KP / CIO **Ahli** : i. ICTSO DVS ii. Semua Pengarah Bahagian IPPV iii. Ketua Unit Undang-Undang iv. Pengurus ICT **Urus Setia** :STM Carta struktur organisasi DVS seperti di Lampiran 1. **Bidang kuasa** : a. Menyelenggara dokumen DKICT DVS; 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 DVS;	JPICT DVS

	e. menyemak semula sistem ICT supaya sentiasa mematuhi keperluan keselamatan dari semasa ke semasa; f. menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; g. memastikan DKICT DVS selaras dengan dasar-dasar ICT kerajaan semasa; dan h. menyediakan dan mengemukakan laporan keselamatan ICT kepada JPICT, dan membincangkan serta menyelesaikan isu-isu berbangkit.	
DM-020109	**Pasukan Keselamatan ICT DVS**	
	Pasukan Keselamatan ICT DVS bertanggungjawab menghalang dan menangani ancaman keselamatan ICT DVS. Keanggotaan pasukan kecil ini adalah seperti berikut: **Pengerusi** : Pengurus ICT **Ahli** : Seksyen ICT **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 DVS mengambil tindakan	CERT DVS

	pemulihan dan pengukuhan dengan kerjasama bersama CERT MOA; f. menyebarkan makluman berkaitan dengan DVS 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.	
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 DVS; 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 ICT

Objektif : Untuk memberi perlindungan keselamatan yang bersesuaian ke atas semua aset ICT Jabatan Perkhidmatan Veterinar Malaysia.		
DM-0301	**Akauntabiliti Aset ICT**	
DM-030101	**Inventori Aset ICT**	
	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 diuruskan oleh pegawai aset dan dikendalikan oleh pengguna yang dibenarkan sahaja; c. memastikan penggunaan aset gunasama direkodkan dalam buku daftar pengguna (log book) dan pegawai aset mesti memastikan aset tersebut berada di dalam keadaan yang baik selepas penggunaan. d. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di DVS; dan e. peraturan penggunaan dan pengendalian aset hendaklah dikenal pasti, di dokumen dan dilaksanakan.	Pegawai Aset, Pengguna Aset, STM, Pentadbir Sistem
DM-0302	**Pengelasan dan Pengendalian Maklumat**	
Objektif: Memastikan setiap maklumat mempunyai tahap keselamatan yang bersesuaian.		
DM-030201	**Pengelasan Maklumat**	
	Maklumat hendaklah dikelaskan sewajarnya oleh Pegawai yang diberi kuasa. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di	Warga DVS

	dalam dokumen Arahan Keselamatan seperti berikut: a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	
DM-0302012	**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.	Warga DVS

PERKARA 04 PENGURUSAN SUMBER MANUSIA

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

DM-0401	**Keselamatan ICT Dalam Tugas Harian**	
DM-040101	**Sebelum Perkhidmatan ICT**	
	Ini bertujuan memastikan pegawai dan kakitangan DVS, 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 DVS, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dalam menjamin keselamatan aset ICT sebelum perkhidmatan; b. Mengenalpasti, menilai prestasi dan menjalankan tapisan keselamatan pembekal, pakar runding dan pihak-pihak lain yang berkepentingan; dan c. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan. d. Mematuhi bahawa aset ICT yang ditawarkan hanya boleh digunakan dengan tujuan yang dibenarkan.	Warga DVS

DM-040102	**Dalam Perkhidmatan ICT**	
	Ini bertujuan memastikan pegawai dan kakitangan DVS, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong dasar keselamatan ICT DVS dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan pegawai dan kakitangan DVS, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh DVS; b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT DVS secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari masa ke semasa; c. memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan DVS, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sekiranya berlaku perlanggaran perundangan dan peraturan yang ditetapkan oleh DVS; 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 Latihan dan Pembangunan Kerjaya, DVS.	CIO, ICTSO, pegawai dan kakitangan DVS, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan

DM-040103	**Bertukar Atau Tamat Perkhidmatan ICT**	
	Ini bertujuan memastikan pertukaran atau tamat perkhidmatan pegawai dan kakitangan DVS, 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 DVS 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 DVS dan/atau terma perkhidmatan.	Warga DVS

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif : Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan dan ancaman.		
DM-0501	**Keselamatan Kawasan**	
DM050101	**Kawalan Kawasan 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 DVS adalah Pejabat Ketua Pengarah, Pejabat Timbalan Ketua Pengarah, Pejabat Pengarah Bahagian, bilik sulit, bilik Server dan Pusat Data (Data Centre) DVS. 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, Pegawai Keselamatan Jabatan, Pegawai Keselamatan Gunasama, Pentadbir Rangkaian dan STM
DM050102	**Kawalan Kawasan**	
	Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat DVS.	Pegawai Keselamatan Bangunan Gunasama,

	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 dan sebarang bencana alam 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.	Pegawai Keselamatan Jabatan DVS, CIO, ICTSO dan pengguna
DM-050103	**Kawalan Masuk Fizikal**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya. b. Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat sekiranya ada dan mesti mematuhi peraturan setempat yang berkaitan. c. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau mengguna aset ICT DVS.	Warga DVS dan Pelawat

DM – 0502	**Keselamatan Peralatan**	
DM – 050201	**Peralatan ICT**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna hendaklah memeriksa semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Penggunaan kata laluan pentadbir sistem dan pengguna 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; d. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan tanpa kebenaran pegawai STM; e. pengguna dilarang sama sekali memindahkan sebarang perkakasan ICT ke bahagian lain kecuali dengan kebenaran pegawai aset bahagian dan ICT; f. pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; g. 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; h. semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna; i. setiap pengguna adalah bertanggungjawab melaporkan ke atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya kepada pegawai bertanggungjawab;	Warga DVS

	j. peralatan-peralatan kritikal seperti server perlu disokong oleh Uninterruptable Power Supply (UPS); k. semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. l. semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin atau mempunyai pengudaraan (*air ventilation*) yang sesuai; m. peralatan ICT yang hendak dibawa keluar dari premis DVS, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan; n. peralatan ICT yang hilang semasa di dalam dan di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden; o. pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa; p. pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ianya ditempatkan tanpa kebenaran Pentadbir Sistem ICT; 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 (statik) juga tidak dibenarkan diubah daripada alamat IP yang telah ditetapkan oleh unit ICT; s. pengguna dilarang sama sekali mengubah *password administrator* dan membuang akaun *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 suis ditutup atau plug dicabut daripada suis utama selepas hari bekerja bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku sebarang kejadian seperti petir, kilat dan sebagainya.	
DM-050202	**Media Storan**	
	Media storan merupakan peralatan yang digunakan untuk menyimpan data dan maklumat seperti cakera padat, pen drive/thumb drive, external hard disk 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 kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja;	Warga DVS

	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. i. Media storan yang mengandungi data terperingkat mestilah dilengkapi sistem keselamatan. j. Penggunaan media storan atas talian DVS adalah digalakkan berbanding penggunaan media storan luar kawasan DVS.	
DM 050203	**Media Tandatangan Digital**	
	Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah-langkah berikut: a. Sebarang media yang digunakan hendaklah mempunyai sistem keselamatan. b. pegawai hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; c. tidak boleh dipindah-milik atau dipinjamkan; dan d. sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Warga DVS
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 pemilik sistem atau Pengurus ICT;	pemilik sistem , Pengurus ICT ICTSO

	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.	
DM – 050205	**Penyelenggaraan**	
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil 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. Memeriksa dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan e. Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Warga DVS dan Pegawai Aset
DM – 050206	**Pengendalian Peminjaman Perkakasan ICT 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:	Warga DVS

	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. c. Sebarang kehilangan perkakasan hendaklah diuruskan mengikut Pekeliling Perbendaharaan K.P 1.1/2013	
DM-050207	**Pengendalian Keselamatan Perkakasan ICT di Luar Pejabat**	
	Perkakasan yang dibawa keluar dari premis DVS 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.	Warga DVS
DM-050208	**Pelupusan Peralatan ICT**	
	Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh DVS ataupun tidak dan ditempatkan di DVS sendiri. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan DVS. 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, *grinding*, *degauzing* atau pembakaran; b. Sekiranya maklumat perlu disimpan, maka	Warga DVS, Pegawai Aset dan STM

	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 ICT DVS.	

	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.(dibwh larangan atau tidak)	
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. Semua komputer akan dibekalkan dengan *password screen saver* atau *logout* apabila meninggalkan komputer dan pengguna tidak dibenarkan ******* 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 faksimili dan mesin fotostat.	Warga DVS
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) atau mana-mana pihak berkuasa keselamatan yang berkaitan. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil :	Warga DVS

	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; 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 secara berkala. 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 iii. 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 c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	STM, ICTSO, Warga DVS
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.	Warga DVS 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	Warga DVS

	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.	

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.	STM, ICTSO
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 ;	Warga DVS

	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.	
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; c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d. Mengemas kini antivirus dengan versi (perisian) 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.	Warga DVS

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 backup bergantung pada tahap kritikal maklumat; e. DVS hendaklah menyimpan sekurang-kurangnya dua (2) generasi backup; dan f. Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat.	Warga DVS
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	Pentadbir Sistem ICT

	seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah dilaporkan kepada ICTSO dan CIO.	
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 dilokasi 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 kontraktor penyelenggara dan diselia oleh Pentadbir Sistem. e. Semua trafik keluar dan masuk Ibu Pejabat Jabatan Perkhidmatan Veterinar hendaklah melalui *firewall* di bawah kawalan DVS; 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 DVS; h. Memasang *Web Content Filter* pada Internet Gateway untuk menyekat aktiviti kemasukan	STM, ICTSO

	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 DVS hendaklah mendapat kebenaran ICTSO; j. Semua pengguna hanya dibenarkan menggunakan rangkaian DVS sahaja di mana penggunaan modem/broadband adalah dilarang sama sekali ; dan k. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.	
DM-0606	**Pengurusan Media**	
DM060601	**Penghantaran dan Pemindahan**	
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Warga DVS
DM060602	**Prosedur Pengendalian Media**	
	Prosedur-prosedur pengendalian media termasuk: a. Melabelkan semua media mengikut tahap keselamatan sesuatu maklumat; b. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; 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.	Warga DVS

	g. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	
DM-060603	**Keselamatan Sistem Komunikasi**	
	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.	Warga DVS
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.	Warga DVS
DM-0607	**Pengurusan Pertukaran Maklumat**	
	Pengurusan Pertukaran Maklumat bertujuan untuk memastikan keselamatan pertukaran maklumat dan perisian antara DVS 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;	Warga DVS

	b. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara DVS dengan pihak luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari DVS; 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 DVS.	
DM-0608	**Pengurusan Mel Elektronik (E-mel)**	
	Penggunaan e-mel di DVS 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 Agensi Kerajaan " dan mana-mana undang-undang bertulis yang berkuat kuasa: Di antara langkah-langkah pengendalian mel elektronik termasuk: a. Menghadkan 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 (10MB) 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	Warga DVS

	diketahui atau diragui; e. Penghantaran lampiran dalam format/ extension " *.exe, *.bat " dan " *.com " tidak dibenarkan; f. Hanya kakitangan DVS sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi DVS; 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 DVS) 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 pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	
DM-06010	**Pengurusan Perkhidmatan Penyampaian 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, STM

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 diwujud 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; e. Kesalahan, kesilapan dan/atau penyalahgunaan perlu dilog, dianalisis dan diambil tindakan sewajarnya; dan f. Masa yang berkaitan dengan sistem pemprosesan maklumat dalam DVS atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.	Pentadbir Sistem ICT, ICTSO, STM

PERKARA 07 KAWALAN CAPAIAN

Objektif: Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT DVS.		
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.	STM, ICTSO, Pentadbir Sistem
DM-0702	**Pengurusan Capaian Pengguna**	
Objektif : Mengawal capaian pengguna ke atas aset ICT DVS.		
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;	Warga DVS, Pentadbir Sistem ICT

	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. Akaun hendaklah ditarik balik jika: i) penggunaannya melanggar peraturan; ii) Bersara; atau iii) Ditamatkan perkhidmatan 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 satu(1) bulan tanpa sebarang capaian ii) Bertukar bidang tugas kerja; iii) Bertukar ke agensi lain;	
DM-070202	**Hak Capaian**	
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Warga DVS
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 DVS seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;	Warga DVS

	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 windows 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 kata laluan diset semula; h. kata laluan hendaklah berlainan daripada pengenalan identiti pengguna. i. Kata laluan hendaklah ditukar selepas 180 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 Khidmat Pengurusan. b. Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain.	Warga DVS

	c. Perkongsian kad pintar untuk sebarang capaian system 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 Khidmat Pengurusan.	
DM-0703	**Capaian Sistem Pengoperasian**	
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam system 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 laluan digunakan, kualiti kata laluan perlu mendapat pengesahan. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; b. mewujudkan jejak audit ke atas semua capaian system 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.	Pentadbir Sistem ICT, ICTSO

	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 DVS 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. menghadkan 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 Acces*** mestilah menggunakan kaedah penyulitan (*encryption*). b. Lokasi bagi akses ke sistem ICT DVS hendaklah dipastikan selamat. c. Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada CIO. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	Warga DVS
DM-0706	**Capaian Internet**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Penggunaan Internet di DVS 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	Pentadbir Rangkaian, Pengurus ICT

	rangkaian DVS. 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. 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/broadband 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 DVS; k. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walaubagaimanapun, 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.	
DM-0707	**Pengauditan dan Forensik ICT**	
	ICTSO mestilah bertanggungjawab merekod dan menganalisa perkara-perkara berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT DVS; 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;	ICTSO

	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.	
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	Pentadbir Sistem ICT

	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.	

PERKARA 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Objektif: Memastikan sistem yang dibangunkan oleh Jabatan atau pihak lain mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

DM-0801	**Keselamatan dalam Membangunkan Sistem Aplikasi**	
DM-080101	**Keperluan Keselamatan Sistem Maklumat**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem aplikasi 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 data input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan samada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; c. Sistem aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d. Semua sistem aplikasi yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan. e. Semua sistem yang dibangunkan hendaklah mempunyai dokumentasi yang lengkap. f. Semua sistem yang dibangunkan hendaklah dipastikan *source code* menjadi hak milik	Pemilik Sistem, Pentadbir Sistem ICT, ICTSO

	jabatan.	
DM-080102	**Pengesahan Data Input**	
	Data input bagi sistem aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.	Pentadbir Sistem / Pemilik Sistem
DM-080103	**Kawalan Prosesan**	
	Kawalan prosesan perlu ada dalam sistem 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 sistem aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pentadbir Sistem / Pemilik Sistem
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 daripada pendedahan dan penyelewengan maklumat berlaku.	Warga DVS
DM-080202	**Tandatangan Digital**	
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Warga DVS
DM-080203	**Pengurusan Infrastruktur Kunci Awam (PKI)**	
	Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Warga DVS

DM-0803	**Keselamatan *file system***	
	File system perlu dikawal dan dikendalikan dengan baik dan selamat. Antara kawalan dan pengendalian tersebut adalah: a. Proses pengemaskini *file system* sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan. b. Kod atau aturcara sistem aplikasi yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan e. Mengaktifkan log audit bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem ICT
DM-0804	**Pembangunan dan Sokongan Sistem**	
Objektif: Memastikan keselamatan sistem aplikasi dan maklumat dikawal supaya selamat dalam semua keadaan.		
DM-080401	**Perubahan Prosedur**	
	Perubahan atau pengubahsuaian ke atas sistem aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum digunapakai. Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut: a. Mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan yang formal; b. Mengkaji semula dan menguji sistem aplikasi kritikal semasa melaksanakan perubahan ke atas sistem aplikasi yang sedang beroperasi untuk memastikan tiada impak negatif ke atas	Pemilik Sistem, Pentadbir Sistem ICT

	keselamatan atau operasi DVS; 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.	
DM-080402	**Pembangunan Secara *Outsource***	
	Pembangunan sistem aplikasi secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code*) bagi semua sistem aplikasi adalah menjadi hak milik DVS.	STM, 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, STM, ICTSO

PERKARA 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

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

DM-0901	**Mekanisme Pelaporan Insiden Keselamatan ICT**	
	Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan serta merta: a. Maklumat didapati hilang, didedahkan kepada pihak- pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberikuasa; b. Sistem aplikasi digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses: i. disyaki hilang, dicuri atau didedahkan; ii. hilang, dicuri atau didedahkan d. Berlaku kejadian keadaan sistem aplikasi yang mencurigakan 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 atau pegawai yang diberi kuasa. ICTSO akan melaporkan kepada CERT MOA untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak- pihak yang di benarkan.	Warga DVS Warga DVS

	b. **CERT MOA** Pasukan Keselamatan Kecil DVS / CERT MOA akan bertindak menghubungi dan GCERT MAMPU sama ada sebagai input atau untuk tindakan seterusnya.	Pasukan keselamatan Kecil DVS/ CERT DVS CERT MOA
	c. **Tanggungjawab Pengguna dan pihak lain** Semua pengguna kakitangan, pembekal, pakar runding dan pihak-pihak lain yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri. Pengguna dan pihak lain mesti melaporkan dengan segera sebarang kejadian insiden keselamatan ICT kepada ICTSO. *Vulnerabality* yang diperhatikan atau disyaki yang terdapat dalam sistem maklumat hendaklah dilaporkan menerusi mekanisme pelaporan. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan menceroboh.	Pengguna/Pihak lain
	d. **Tindakan Dalam Keadaan Berisiko Tinggi** Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan dalam tempoh yang ditetapkan 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 CERT DVS 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. CERT DVS akan menerima aduan atau laporan daripada pengguna, laporan yang dikesan dari perisian atau perkakasan keselamatan rangkaian jabatan atau laporan daripada jabatan atau agensi lain yang berkaitan. 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 penguatkuasa undang-undang. CERT DVS 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. 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 (PKP) perlu diaktifkan atau sebaliknya. Pengesahan akan dihantar kepada CIO bagi mengaktifkan PKP. Laporan insiden yang tidak memerlukan PKP akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan. Carta lengkap mengenai perjalanan laporan insiden seperti di Lampiran 2.	ICTSO

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 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 JPICT DVS 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. Mengenalpasti sistem aplikasi mempunyai backup; dan f. menguji dan mengemaskini pelan sekurang-kurangnya tiga tahun sekali atau mengikut keperluan semasa.	Pengurus ICT CERT DVS

DM-1002	**Pengurusan Kesinambungan Perkhidmatan**	
	Pengurusan Kesinambungan Perkhidmatan adalah mekanisme bagi mengurus dan memastikan kepentingan stakeholder sistem penyampaian perkhidmatan dilindungi dan imej DVS terpelihara. Ini dilakukan dengan tindakan proaktif untuk memastikan operasi sistem penyampaian perkhidmatan disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT DVS.	CIO, Pengurus ICT, ICTSO

PERKARA 11 PEMATUHAN

Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT DVS.		
DM-1101	**Pematuhan dan Keperluan Perundangan**	
	Setiap pengguna di DVS hendaklah membaca, memahami, menandatangani surat akuan pematuhan dan mematuhi Dasar Keselamatan ICT DVS serta undang- undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Semua aset ICT di DVS adalah hak milik Kerajaan. Ketua Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT DVS selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber DVS.	Warga DVS
DM-1102	**Pematuhan Dengan Dasar, Piawaian dan Keperluan Teknikal**	
	ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas pengguna aset ICT di DVS mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi piawaian pelaksanaan keselamatan ICT. ICTSO hendaklah menyediakan Dasar Keselamatan ICT DVS serta undang-undang atau peraturan-peraturan lain yang berkaitan untuk diakses.	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.	Warga DVS
DM-1104	**Keperluan Perundangan**	
	Berikut adalah keperluan perundangan atau peraturan- peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di DVS: a. Arahan Keselamatan b. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam; c. Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam (2009); d. Surat Arahan KSN Bil.KPKK(R)200/55 Klt.8(2) bertarikh 31 Januari 2007 – Langkah-langkah Keselamatan Perlindungan untuk Larangan Penggunaan Telefon Bimbit atau lain-lain Peralatan Komunikasi ICT Tanpa Kebenaran atau Kuasa yang Sah Di Agensi-agensi Kerajaan; e. Surat Arahan MAMPU Bil.MAMPU.702-1/1/7 Jld.3(48) bertarikh 23 Mac 2009 – Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT Di Agensi-agensi Kerajaan; f. Garis Panduan Pembangunan Kandungan Sektor Awam bertarikh 11 September 2009 g. Pekeliling Am Bilangan 1 Tahun 2006 – Pengurusan Laman Web/Portal Sektor Awam; h. Surat Arahan MAMPU Bil. MAMPU.BDPICT(S)700-6/1/3(21) bertarikh 19 November 2009 – Penggunaan Media Jaringan Sosial Di Sektor Awam; i. Surat Arahan MAMPU Bil.	Warga DVS

	UPTMS(S)159/05/648/1(33) bertarikh 17 Julai 2009 – Garis Panduan Pelaksanaan Blog Bagi Agensi Sektor Awam; j. Surat Arahan MAMPU Bil. MAMPU.BDPICT(S)700-6/1/3(7) bertarikh 15 September 2009 – Penggunaan Smartphone, Personel Digital Assistant dan Alat Komunikasi Mudah Alih Sebagai Saluran Komunikasi Tambahan; k. Pekeliling Kemajuan Pentadbiran Awam Bil.3 Tahun 2008 – Panduan Menambahbaik Sistem Penyampaian Perkhidmatan Kerajaan Menerusi Perkhidmatan Pesanan Ringkas (SMS); l. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan; m. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS); n. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); o. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan; p. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; q. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; r. 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; s. Surat Arahan Ketua Pengarah MAMPU - Langkah- langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan yang bertarikh 1 Jun 2007; t. Surat Arahan Ketua Pengarah MAMPU - Langkah-langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-agensi Kerajaan yang bertarikh 23 November 2007; u. Surat Pekeliling Am Bilangan 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di Bawah	

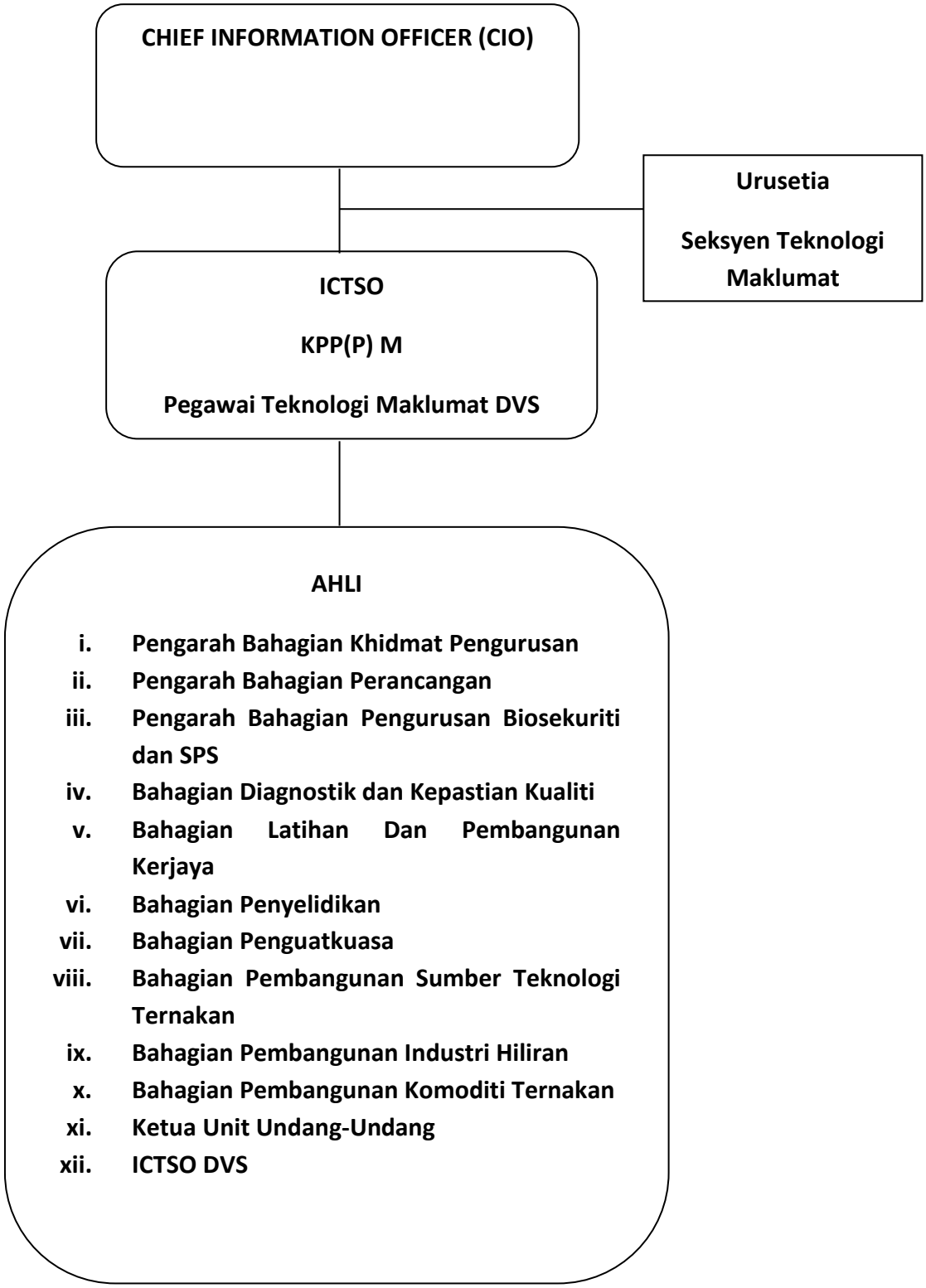
	Jawatankuasa IT dan Internet Kerajaan (JITIK); v. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender; w. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan; x. Akta Tandatangan Digital 1997; y. Akta Rahsia Rasmi 1972; z. Akta Jenayah Komputer 1997; aa. Akta Hak cipta (Pindaan) Tahun 1997; bb. Akta Komunikasi dan Multimedia 1998; cc. Perintah-perintah Am; dd. Arahan Perbendaharaan; ee. Arahan Teknologi Maklumat 2007; ff. Akta Aktiviti Kerajaan Elektronik 2007	
DM-1105	**Pelanggaran Dasar**	
	Pelanggaran Dasar Keselamatan ICT DVS boleh dikenakan tindakan tatatertib.	Warga DVS

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 komunikas (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CERT DVS	Organisasi yang ditubuhkan untuk membantu DVS mengurus pengendalian insiden keselamatan ICT di DVS masing-masing dan DVS di bawah kawalannya.
CIO	Chief Information Officer Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan 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 Pencerobohann Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada

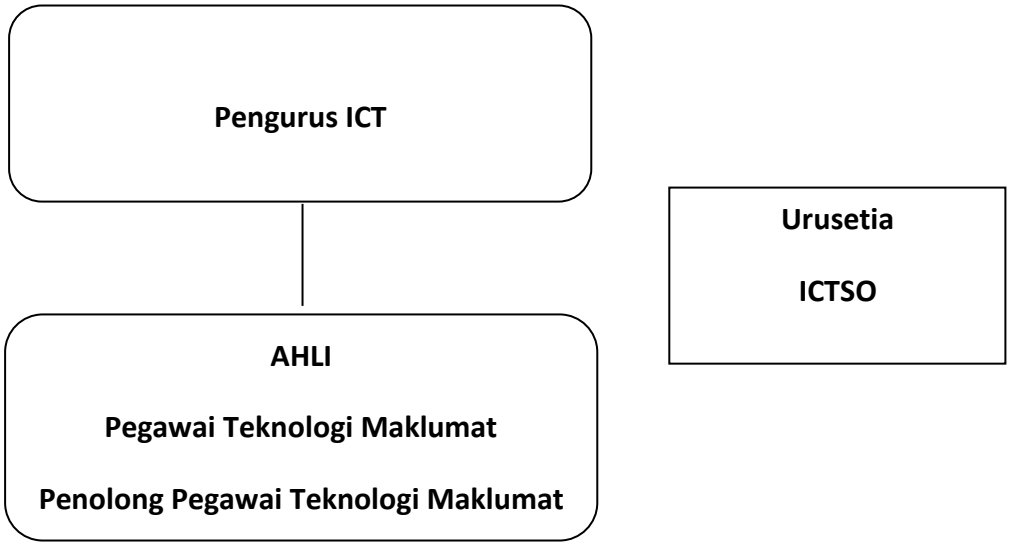
	lebih bersifat host atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau 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.
Maklumat rasmi	Maklumat yang dikutip/dijana dan diproses atas urusan rasmi jabatan
Warga DVS	Pegawai dan kakitangan di semua peringkat yang berkhidmat di DVS

Lampiran 1

Carta 1 (a): Struktur Organisasi Jawatankuasa Pemandu ICT DVS

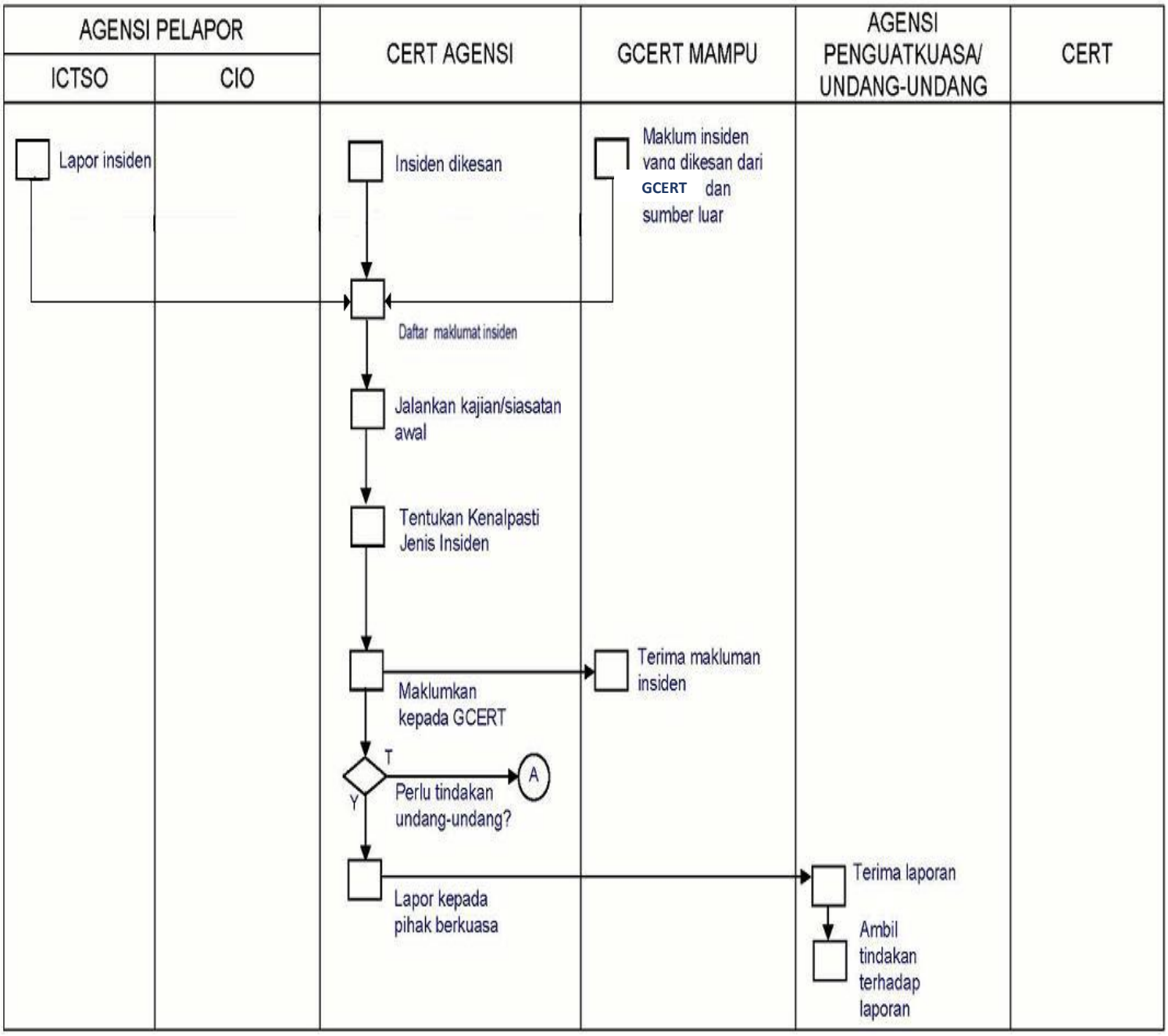


Carta 1 (b): Struktur Organisasi Pasukan Kecil Keselamatan ICT DVS (CERT DVS)

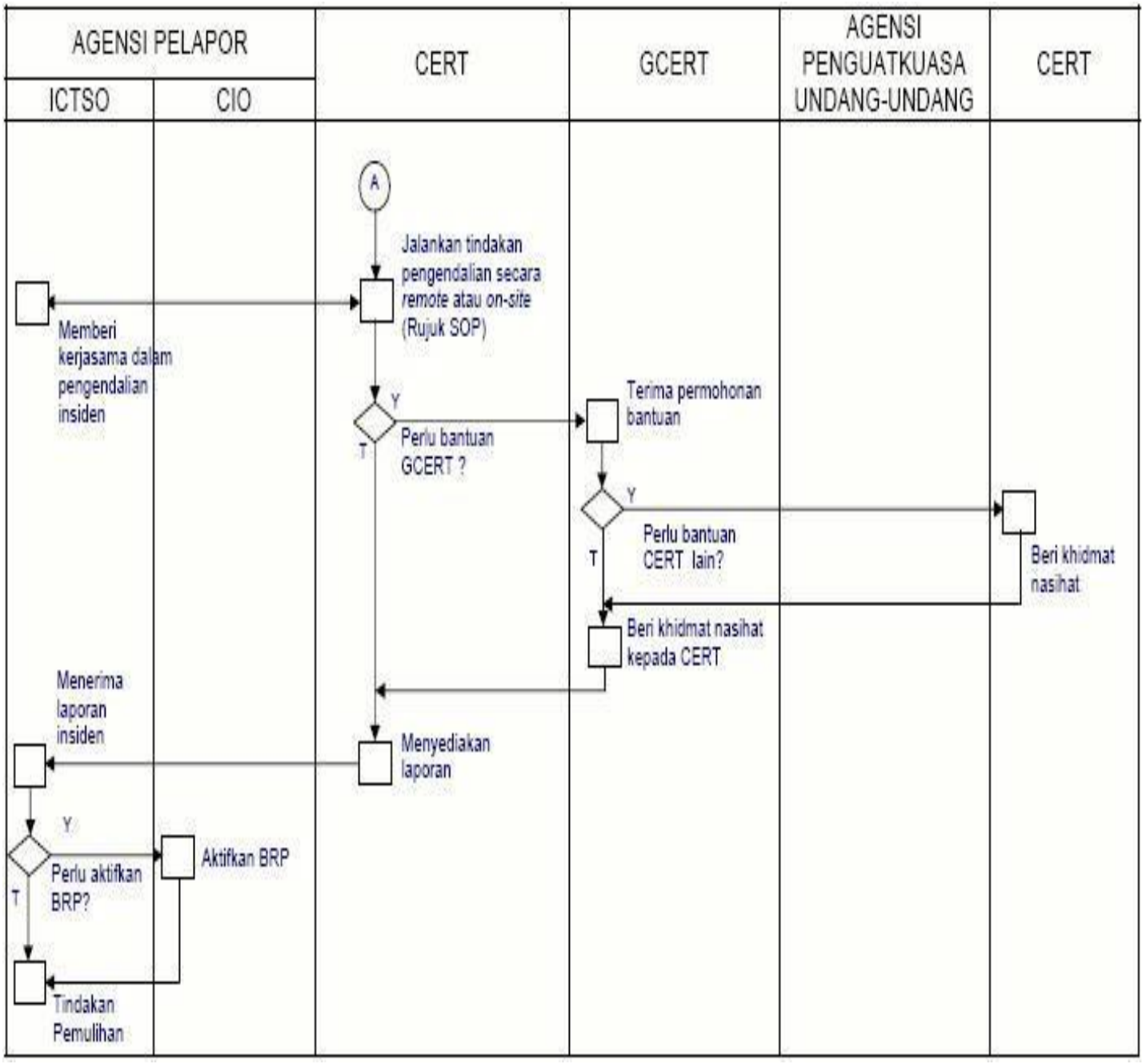


Lampiran 2

Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT DVS



Rajah 2: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT DVS



Lampiran 3

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT JABATAN PERKHIDMATAN VETERINAR

Nama (Huruf Besar) : ……..

No. Kad Pengenalan : ……..

Jawatan dan Gred Perkhidmatan : ……..

Jabatan / Agensi : ……..

Bahagian / Seksyen : ……..

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 DVS; dan

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

…….

(Tandatangan)

Nama :

Alamat Pejabat Penempatan :