Dasar Keselamatan ICT

Jabatan Perikanan Malaysia (DOFM)

Kementerian Pertanian dan Industri Asas Tani

November 2009

Versi 1.0

KANDUNGAN

PENGENALAN

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

RASIONAL

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

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

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

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

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

OBJEKTIF

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

Objektif utama Dasar Keselamatan ICT DOFM adalah seperti berikut:-

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

(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 kesemalatan ICT kepada para kakitangan, pengguna dan pembekal;

(f) Memperkemaskan pengurusan risiko; dan

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

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

PERNYATAAN DASAR

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

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

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

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

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

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

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

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

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

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

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

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

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

SKOP

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

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

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

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

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

Bagi menentukan Sistem ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT DOFM ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran, dan yang dibuat salinan keselamatan ke dalam semua aset ICT, Ini akan

dilakukan melalui 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 DOFM. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) **Perisian**

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada DOFM;

(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 DOFM. Contoh: sistem dokumentasi, prosedur operasi, rekod-rekod DOFM, 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 DOFM bagi mencapai misi dan objektif DOFM. 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 DOFM ini adalah juga saling lengkap-melengkapi dan perlu dilaksanakan secara konsisten dengan undang-undang dan peraturan yang sedia ada.

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

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT DOFM 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 yang dinyatakan dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

(b) **Hak Akses Minimum**

Hak akses kepada pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas adalah diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu data atau maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

(c) **Akauntabiliti**

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:-

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

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

(iii) Menentukan maklumat sedia untuk digunakan;

(iv) Menjaga kerahsiaan kata laluan;

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

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

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

(d) **Pengasingan**

Ttugas-tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat, di manipulasi dan seterusnya, mengenalkan integriti dan kebolehsediaan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

(e) **Pengauditan**

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*.

(f) **Pematuhan**

Dasar Keselamatan ICT DOFM hendaklah dibaca, difahami dan dipatuhi. Pematuhan adalah merupakan prinsip penting dalam menghindar dan mengesan sebarang perlanggaran Dasar yang boleh membawa ancaman kepada keselamatan ICT.

(g) **Pemulihan**

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian bagi meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan dan ketidakbolehcapaian. Pemulihan boleh dilakukan melalui proses penduaan (*backup*) dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan (BPR).

(h) **Saling Bergantung**

Setiap prinsip adalah saling lengkap-melengkapi dan bergantung antara satu dengan lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

KAWALAN 01 DASAR KESELAMATAN ICT

Dasar Keselamatan ICT		
Objektif : DKICT DOFM ini diwujudkan untuk melindungi aset ICT bagi memastikan kelancaran operasi Jabatan Perikanan secara berterusan, meminimumkan kerosakan atau kemusnahan aset-aset ICT melalui usaha pencegahan atau mengurangkan kesan kejadian yang tidak diingini berdasarkan kepada ciri-ciri keselamatan iaitu kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan.		
K/0101	**Pelaksanaan Dasar**	
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah Jabatan Perikanan dibantu oleh Jawatankuasa Pemandu ICT DOFM, kesemua Pengarah Bahagian, Pengarah Pejabat Perikanan Negeri, Ketua Institut dan Ketua Pusat.	Ketua Pengarah
K/0102	**Penyebaran Dasar**	
	Dasar ini perlu disebarkan kepada semua pengguna Jabatan Perikanan dan agensi di bawahnya (termasuk kakitangan, pembekal, pakar runding dll.)	ICTSO
K/0103	**Penyelenggaraan Dasar**	
	Dasar Keselamatan ICT DOFM 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 DOFM: a. kenal pasti dan tentukan perubahan yang diperlukan; b. kemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Jawatankuasa Pemandu ICT (JPICT) Jabatan Perikanan; c. perubahan yang telah dipersetujui oleh JPICT Jabatan Perikanan dimaklumkan kepada semua pihak iaitu kakitangan, pengguna dan pembekal; dan	ICTSO

	d. dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	
K/0104	**Pengecualian Dasar**	
	Dasar Keselamatan ICT DOFM adalah terpakai kepada semua pengguna ICT Jabatan Perikanan dan tiada pengecualian diberikan.	Semua

KAWALAN 02 KESELAMATAN ORGANISANI

Infrastruktur Keselamatan Organisasi		
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT DOFM.		
K/0201	**Infrastruktur Organisasi Dalaman**	
K/020101	**Ketua Pengarah**	
	Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOFM; b. memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT DOFM; c. memastikan semua pengguna mematuhi Dasar Keselamatan ICT DOFM; d. memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; e. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT DOFM; dan f. menandatangani “Surat Akuan Pematuhan” (Lampiran 1) bagi mematuhi Dasar Keselamatan ICT DOFM.	Ketua Pengarah
K/020102	**Ketua Pegawai Maklumat (CIO)**	
	Timbalan Ketua Pengarah (Operasi) Jabatan Perikanan adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggung jawab beliau adalah seperti berikut:	CIO

	a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOFM; b. membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; c. menentukan keperluan keselamatan ICT; d. menentukan tindakan tatatertib yang perlu diambil ke atas pengguna yang telah melanggar DKICT DOFM; dan e. menandatangani "Surat Akuan Pematuhan" (Lampiran 1) bagi mematuhi Dasar Keselamatan ICT DOFM.	
K/020103	**Pegawai Keselamatan ICT (ICTSO)**	
	Jawatan ICTSO bagi DOFM adalah disandang oleh Ketua Unit Pentadbir Sistem dan Rangkaian Komunikasi yang merupakan Pegawai Teknologi Maklumat (PTM). Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOFM; b. menguatkuasakan pelaksanaan Dasar Keselamatan ICT DOFM di semua Bahagian di DOFM; c. memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT DOFM kepada semua pengguna; d. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT DOFM; e. menjalankan *Security Posture Assessment* (SPA) sekurang-kurangnya dua tahun sekali dan merumus tindak balas pengurusan berdasarkan hasil penemuan serta menyediakan laporan mengenainya; f. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta	ICTSO

	menyediakan langkah-langkah perlindungan yang bersesuaian; g. melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (CERT) MOA dan memaklumkannya kepada CIO; h. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; i. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT DOFM; j. memastikan Dasar Keselamatan ICT DOFM dikemas kini sesuai dengan perubahan teknologi, arahan Jabatan dan ancaman-ancaman dari semasa ke semasa; k. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan l. menandatangani "Surat Akuan Pematuhan" (Lampiran 1) bagi mematuhi Dasar Keselamatan ICT DOFM.	
K/020104	**Pengurus ICT**	
	Dalam konteks DKICT ini, peranan Pengurus ICT di Ibu Pejabat disandang oleh dua wakil iaitu Pengarah Bahagian Pengurusan Maklumat Perikanan (PMP) dan Ketua Cawangan Teknologi Maklumat (CTM), manakala peranan Pengurus ICT di negeri ialah *Super User* di Pejabat Perikanan Negeri/ Institut/Pusat. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOFM; b. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan DOFM; c. menentukan kawalan akses pengguna terhadap aset ICT DOFM di Pusat Data; d. melaporkan sebarang perkara atau penemuan mengenai	Pengurus ICT

	keselamatan ICT kepada ICTSO; dan e. menandatangani "Surat akuan Pematuhan" (Lampiran 1) bagi mematuhi Dasar Keselamatan ICT DOFM.	
K/020105	***Super User***	
	Peranan dan tanggungjawab Super User adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOFM; b. mengkaji semula dan melaksanakan kawalan keselamatan ICT di negeri selaras dengan keperluan DOFM; c. menentukan kawalan akses pengguna terhadap aset ICT DOFM di negeri; d. melaporkan mengenai kakitangan yang berhenti dan bertukar dengan mengembalikan Borang Pengurusan Aset dan Penggunaan Sistem Aplikasi ICT (BICT-01) seperti di Lampiran 4; e. melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan f. menandatangani "Surat akuan Pematuhan" (Lampiran 1) bagi mematuhi Dasar Keselamatan ICT DOFM.	*Super User*
K/020106	**Pentadbir Sistem**	
	Pegawai setiap unit di Cawangan Teknologi Maklumat adalah merupakan Pentadbir Sistem DOFM dan tanggungjawab Pentadbir Sistem adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOFM; b. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; c. menentukan ketepatan dan kesempurnaan sesuatu tahap	Pentadbir Sistem

	capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT DOFM; d. memantau aktiviti capaian harian sistem aplikasi pengguna; e. menentukan kawalan akses pengguna terhadap sistem aplikasi DOFM; g. melaksanakan prinsip-prinsip DKICT dan menjaga kerahsiaan maklumat DOFM; h. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatal atau memberhentikannya dengan serta merta; i. menyimpan dan menganalisis rekod jejak audit; dan j. menandatangani "Surat Akuan Pematuhan" (Lampiran 1) bagi mematuhi Dasar Keselamatan ICT DOFM.	
K/020107	**Pengguna**	
	Peranan dan tanggungjawab pengguna adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOFM; b. mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. lulus tapisan keselamatan; d. melaksanakan prinsip-prinsip Dasar Keselamatan ICT DOFM dan menjaga kerahsiaan maklumat DOFM; e. melaksanakan langkah-langkah perlindungan seperti berikut :- i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. menentukan maklumat sedia untuk digunakan;	Pengguna

	iv. menjaga kerahsiaan kata laluan; v. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; g. menghadiri program-program kesedaran mengenai keselamatan ICT; dan h. menandatangani "Surat Akuan Pematuhan" (Lampiran 1) bagi mematuhi Dasar Keselamatan ICT DOFM.	
K/020108	**Jawatankuasa Pemandu ICT DOFM**	
	Jawatankuasa Pemandu ICT (JPICT) DOFM adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT DOFM. Keanggotaan JPICT DOFM adalah seperti berikut: **Pengerusi**: CIO **Ahli**: i. Wakil Bahagian Pentadbiran dan Kewangan ii. Wakil Bahagian Perancangan dan Antarabangsa iii. Wakil Bahagian Pembangunan dan Perundingan Khidmat Teknikal iv. Wakil Bahagian Pelesenan dan Pengurusan Sumber v. Wakil Bahagian Perlindungan Sumber vi. Wakil Bahagian Kejuruteraan vii. Wakil Bahagian Pembangunan Akuakultur viii. Wakil Bahagian Pembangunan Sumber Manusia ix. Wakil Bahagian Pengembangan Perikanan x. Wakil Bahagian Biosekuriti Perikanan xi. Wakil Cawangan Perundangan dan Pendakwaan xii. Wakil Jabatan Perikanan Laut Sarawak JPLS	CIO

	xiii. Wakil Departmen Penyelidikan dan Pengurusan Sumber Wakil Marin, SEAFDEC xiv. Wakil Institut Penyelidikan Perikanan, IPP xv. Wakil Institut Perikanan Malaysia, IPM xvi. ICTSO DOFM **Urusetia**: Bahagian Pengurusan Maklumat Perikanan Carta struktur organisasi DOFM seperti di Lampiran 2. **Bidang kuasa**: a. memperakukan/meluluskan dokumen DKICT DOFM; b. memantau tahap pematuhan keselamatan ICT; c. menilai aspek teknikal keselamatan projek-projek ICT; d. memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam jabatan yang mematuhi keperluan DKICT DOFM; 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 DOFM selaras dengan dasar-dasar ICT kerajaan semasa; dan h. menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; i. membincangkan tindakan yang melibatkan pelanggaran Dasar Kesemalatan ICT DOFM; dan j. membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	

K/ 0202	Pihak Luar/ Asing	
K/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. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOFM; b. mengenalpasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c. mengenalpasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak luar/asing; d. 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 DOFM; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. e. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT DOFM sebagaimana Lampiran 1.	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem dan Pihak Luar/ Asing

KAWALAN 03 PENGURUSAN ASET

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

K/030101	**Inventori Aset**	
	Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: a. Memastikan semua aset dikenal pasti dan maklumat aset di rekod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini; b. memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c. memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di DOFM; d. peraturan bagi pengendalian aset hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan e. setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pentadbir Sistem, Semua
K/0302	**Pengelasan dan Pengendalian Maklumat**	
Objektif : Memastikan setiap maklumat diberikan tahap perlindungan yang bersesuaian.		
K/030201	**Pengelasan Maklumat**	
	Maklumat hendaklah dikelas dan dilabelkan sewajarnya oleh Pegawai	Semua

	yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	
K/030202	**Pengendalian Maklumat**	
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, pertukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan berikut : a. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. menentukan maklumat sedia untuk digunakan; d. menjaga kerahsiaan kata laluan; e. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. memberi perhatian kepada maklumat terperingkat terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua

KAWALAN 04 KESELAMATAN SUMBER MANUSIA

K/0401	Keselamatan ICT Dalam Tugas Harian	
Objektif : Untuk memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan DOFM, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga DOFM hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuatkuasa.		
K/040101	**Sebelum Perkhidmatan**	
	Ini bertujuan memastikan pegawai dan kakitangan DOFM, 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 DOFM, pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan DOFM, pembekal, pakar runding dan pihak-pihak lain yang terlibat selaras dengan keperluan perkhidmatan; dan c. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua
K/040102	**Semasa Perkhidmatan**	
	Ini bertujuan memastikan pegawai dan kakitangan DOFM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong dasar keselamatan ICT DOFM dan	Semua

	meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan pegawai dan kakitangan DOFM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh DOFM; b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT DOFM secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa; c. Melengkapkan Borang Pengurusan Aset dan Penggunaan Sistem Aplikasi ICT (BICT-01) seperti di Lampiran 4; d. memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan DOFM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh DOFM; dan e. memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pihak pengguna boleh merujuk kepada Bahagian Pembangunan Sumber Manusia, DOFM.	
K/040103	**Bertukar Atau Tamat Perkhidmatan**	
	Ini bertujuan memastikan pertukaran atau tamat perkhidmatan pegawai dan kakitangan DOFM, 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 DOFM	Semua

	mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; b. Melengkapkan Borang Pengurusan Aset dan Penggunaan Sistem Aplikasi ICT (BICT-01) seperti di Lampiran 4; dan c. membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan DOFM dan/atau terma perkhidmatan.	

KAWALAN 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

K/0501	Keselamatan Fizikal dan Persekitaran	
Objektif : Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan dan ancaman.		
K/050101	**Kawasan Larangan Lokasi ICT**	
	Kawasan larangan lokasi ICT bagi DOFM ditakrifkan sebagai kawasan yang dihadkan kemasukkan pegawai-pegawai yang tertentu sahaja Ini bertujuan untuk menghalang capaian, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat DOFM. Kawasan larangan lokasi ICT DOFM adalah Pusat Data. Kawasan ini mestikan dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke premis tersebut adalah seperti berikut: a. sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; b. akses adalah terhad kepada pegawai yang telah diberikan kuasa sahaja dan dipantau pada setiap masa; c. pemataauan dibuat menggunakan Closed-Circuit Television (CCTV) kamera atau lain-lain peralatan yang sesuai; d. pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; e. lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan dan laluan awam; f. memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal keselamtan; g. melengkapkan Borang Pengurusan Aset dan Penggunaan Sistem	Pentadbir Pusat Data, Pentadbir Sistem

	Aplikasi ICT (BICT-01) seperti di Lampiran 4; h. memperkukuhkan dinding dan siling; dan i. mengehadkan jalan keluar masuk.	
K/0502	**Keselamatan Peralatan**	
K/050201	**Peralatan ICT**	
	Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; b. pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; d. 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; e. semua peralatan sokongan ICT termasuk *thumbdrive*, hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna; f. setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; g. peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); h. semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci, kecuali untuk kegunaan individu;	Semua

	i. semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan *(air ventilation)* yang sesuai; j. peralatan ICT yang hendak dibawa keluar dari premis DOFM, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan; k. peralatan ICT yang hilang semasa di waktu pejabat dan luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden; l. pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa; m. 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; n. konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal; o. pengguna dilarang sama sekali mengubah *password administrator* yang telah ditetapkan oleh pihak ICT; p. pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat dibawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi Jabatan sahaja; dan q. pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "OFF" apabila meninggalkan pejabat.	
K/050202	**Media Storan**	
	Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *USB flash drive*, CDROM dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik,	Semua

	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. Setakat yang boleh, katalaluan perlu digunakan termasuk untuk media storan *USB flash drive*; 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. akses dan pergerakan kepada media storan perlu direkodkan dengan menggunakan Borang Pengurusan Aset dan Penggunaan Sistem Aplikasi ICT (BICT-01) seperti di Lampiran 4; dan e. sebarang kehilangan media storan yang berlaku hendaklah dilaporkan mengikut Prosedur Pelaporan Insiden.	
K/050203	**Media Tandatangan Digital**	
	Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah-langkah berikut: a. pegawai hendaklah bertanggunjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyelahgunaan dan pengklonan; b. tidak boleh dipindah-milik atau dipinjamkan; dan c. sebarang insiden kehilangan yang berlaku hendaklah dilaporkan mengikut Prosedur Pelaporan Insiden.	Semua
K/050204	**Media Perisian dan Aplikasi**	
	Sebarang media yang digunakan sebagai media perisian dan aplikasi hendaklah mematuhi langkah-langkah berikut:	Pengurus ICT, Pegawai Aset, Pentadbir Sistem

	a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan Jabatan; b. Sistem aplikasi dalaman tidak dibenarkan diagih/ didemontrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c. Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada CD-ROM, disk atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; d. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan; dan e. Sistem-sistem aplikasi yang dibangunkan di Ibu Pejabat Perikanan dan Pejabat Perikanan Negeri perlu mendapat kelulusan teknikal dari JPICT Jabatan Perikanan. Sementara sistem-sistem aplikasi yang dibangunkan di Institut/Pusat perlu mendapatkan pengesahan dari Unit Teknologi Maklumat di Institut/Pusat masing-masing dahulu sebelum dikemukakan untuk kelulusan teknikal JPICT Jabatan Perikanan.	
K/050205	**Perkakasan Tanpa Penyeliaan (*Unattended Equipment)***	
	Pengguna perlu memastikan mana-mana perkakasan yang ditinggalkan tanpa penyeliaan mematuhi ciri-ciri keselamatan seperti mempunyai kata laluan dan sebagainya. Perkakasan hendaklah disenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.	Semua
K/050206	**Penyelenggaraan**	
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan 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;	Pegawai Aset Bahagian/ Institut/ Pusat

	b. Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; c. Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; dan d. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan.	
K/050207	**Pelupusan**	
	Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh DOFM ataupun tidak dan ditempatkan di agensi sendiri. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan DOFM. Langkah-langkah seperti berikut hendaklah diambil: a. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; b. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; c. peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; d. pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; e. 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, Hardisk, Motherboard dan sebagainya.	Pegawai Aset Bahagian/ Institut/ Pusat

	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 dibawah tanggungjawab bahagian/ pusat/ institut. v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau thumbdrive sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
K/050208	**Clear Desk dan Clear Screen**	
	Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Clear Desk bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja warga atau di paparan skrin apabila warga tidak berada di tempatnya. Langkah-langkah perlu diambil termasuklah seperti berikut: a. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; b. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci; dan c. Dokumen yang mengandungi bahan-bahan sensitif hendaklah diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	Semua
K/0503	**Keselamatan Persekitaran**	
K/050301	**Kawalan Persekitaran**	

	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil : 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 perkomputeran 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 perkomputeran; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; dan f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer.	Semua
K/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; dan b. Peralatan sokongan seperti UPS (*Uniterruptible Power Supply*)	Semua Pentadbir Pusat

	dan penjana (*generator*) boleh digunakan bagi perkhidmatan kiritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan.	Data
K/0504	**Keselamatan Dokumen dan Sistem Dokumentasi**	
K/050401	**Dokumen**	
	Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi: a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi ICT sedia ada dengan melengkapkan Borang Pengurusan Aset dan Penggunaan Sistem Aplikasi ICT (BICT-01) seperti di Lampiran 4; c. Setiap dokumen hendaklah difail 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.	Pentadbir Sistem, Pentadbir Fail

KAWALAN 06 PENGURUSAN OPERASI DAN KOMUNIKASI

Objektif :

Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

K/0601	**Pengurusan Prosedur dan Operasi**	
K/060101	**Pengendalian Prosedur**	
	a. Semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumentasikan, disimpan dan dikawal; b. Setiap prosedur berkenaan 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 berkenaan hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua
K/060102	**Pengurusan Perubahan**	
	a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua

K/060103	**Pengasingan Tugas dan Tanggungjawab**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut dengan syarat cadangan penambahan kakitangan dalam ISP Jabatan Perikanan Tahun 2007 – 2011 dipenuhi: a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan c. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pengurus ICT , ICTSO
K/0602	**Pengurusan Penyampaian Perkhidmatan Pihak Ketiga**	
K/060201	**Perkhidmatan Penyampaian**	
	Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi dilaksanakan dan diselenggarakan oleh pihak ketiga; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Pentadbir Sistem
K/0603	**Perancangan dan Penerimaan Sistem**	
K/060301	**Perancangan Kapasiti**	
	a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan	Pentadbir Sistem, ICTSO

	bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b. 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.	
K/060302	**Penerimaan Sistem**	
	Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem, ICTSO
K/0604	**Perisian Berbahaya**	
K/060401	**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 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 berkuatkuasa; c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d. Mengemas kini *antivirus* dengan *pattern* dari semasa ke semasa; 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	Pentadbir Sistem

	yang telah ditawarkan kepada pembekal perisian. Klausa ini akan digunakan sekiranya perisian tersebut mengandungi program berbahaya; dan h. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
K/0605	***Housekeeping***	
K/060501	***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 salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat salinan *backup* ke atas semua data dan maklumat mengikut kesesuaian operasi; c. Menguji sistem *backup* 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; dan e. DOFM hendaklah menyimpan sekurang-kurangnya tiga (3) generasi *backup*.	Pentadbir Sistem, Pentadbir Pusat Data
K/060502	**Sistem Log**	
	Pentadbir Sistem 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	Pentadbir Sistem

	membaik pulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada ICTSO dan CIO dengan menggunakan IRH1.0 seperti di Lampiran 5.	
K/0606	**Pengurusan Rangkaian**	
K/060601	**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. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; c. *Firewall* hendaklah dipasang di Ibu Pejabat, antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh kontraktor penyelenggara dan diselia oleh Pentadbir Sistem; d. Semua trafik keluar dan masuk Ibu Pejabat Perikanan hendaklah melalui *firewall* di bawah kawalan DOFM; e. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer peribadi kecuali mendapat kebenaran ICTSO; f. Memasang perisian *Intrusion Detection System* (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat DOFM; g. Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti kemasukan dari atau capaian pada laman web/Internet yang mengandungi maklumat atau unsur-unsur tidak	Pentadbir Rangkaian dan *Super User*

	sihat dan berbahaya yang boleh menjejaskan integriti kakitangan, sistem dan maklumat; h. Sebarang penyambungan rangkaian yang bukan di bawah kawalan DOFM adalah tidak dibenarkan; i. Semua pengguna di Ibu Pejabat hanya dibenarkan menggunakan rangkaian DOFM sahaja di mana penggunaan modem adalah dilarang sama sekali; dan j. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan di semua premis pejabat.	
K/0607	**Pengurusan Media**	
K/060701	**Penghantaran dan Pemindahan**	
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Semua
K/060702	**Prosedur Pengendalian Media**	
	Di antara prosedur-prosedur pengendalian media termasuk: a. Melabelkan semua media mengikut tahap keselamatan sesuatu maklumat; b. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; 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.	Semua

K/0608	**Pengurusan Pertukaran Maklumat**	
	Pengurusan Pertukaran Maklumat bertujuan untuk memastikan keselamatan pertukaran maklumat dan perisian dalam DOFM dan mana-mana entiti 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; b. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara DOFM dengan pihak luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari DOFM; 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 DOFM.	Pentadbir Sistem
K/0609	**Pengurusan Mel Elektronik (E-mel)**	
	Penggunaan e-mel di DOFM 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-agensi Kerajaan” dan mana-mana undang-undang bertulis yang berkuatkuasa: 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;* b. Penghantaran dokumen rasmi hendaklah menggunakan e-mel rasmi jabatan sahaja;	Semua

	c. Penggunaan e-mel jabatan bagi tujuan peribadi adalah tidak dibenarkan; d. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, streamyx.com, gmail.com dsb) tidak boleh digunakan untuk tujuan rasmi; e. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; f. Pentadbir e-mel perlu menetapkan had maxima bagi kuota *mailbox;* g. Pembersihan e-mel akan dibuat oleh Pentadbir Sistem sekiranya *mailbox* didapati tidak aktif selama dua (2) bulan atau melebihi kuota dan had masa yang ditetapkan; h. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi boleh dihapuskan; i. Penghantaran lampiran dalam format/*extension " *.exe, *.bat "* dan " **.com"* tidak dibenarkan; j. Mengambil tindakan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; k. Hanya kakitangan DOFM sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi DOFM; l. Pihak Cawangan Personel, B(PnK) dan B(PSM) perlu memaklumkan sebarang status personel (bertukar jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke DOFM) di pejabat-pejabat berkenaan bagi tujuan pengemaskinian e-mel yang terlibat; dan m. Pengguna adalah mewakili diri sendiri dan bertanggungjawab ke atas maklumat yang dikeluarkan dalam setiap perhubungan yang dibuat secara elektronik.	
K/0610	**Pemantauan**	
	Ianya bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, di antaranya seperti berikut:	Pentadbir Sistem

	a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b. Maklumat log perlu dilindungi daripada diubahsuai serta sebarang capaian yang tidak dibenarkan; c. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu di wujud dan hasilnya perlu dipantau secara berkala; d. Kesalahan, kesilapan dan / atau penyalahgunaan perlu dilog, dianalisis dan diambil tindakan sewajarnya; e. Aktiviti pentadbiran dan operator sistem perlu direkodkan dengan melengkapkan Borang Pengurusan Aset dan Penggunaan Sistem Aplikasi ICT (BICT-01) seperti di Lampiran 4; dan f. Masa yang berkaitan dengan sistem pemprosesan maklumat dalam DOFM atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.	

KAWALAN 07 Kawalan Capaian

Dasar Kawalan Capaian		
Objektif : Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT DOFM.		
K/0701	**Kawalan Capaian**	
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkod, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	Pentadbir Sistem
K/0702	**Pengurusan Capaian Pengguna**	
Objektif : Mengawal capaian pengguna ke atas aset ICT DOFM.		
K/070201	**Akaun Pengguna**	
	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 yang boleh digunakan; b. akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. akaun pengguna yang diwujud 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 boleh ditarik balik jika penggunaannya melanggar peraturan; e. penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan	Pentadbir Sistem, Pengguna

	f. Pentadbir Sistem boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut; i) Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi sebulan; ii) Bertukar bidang tugas kerja; iii) Bertukar ke agensi lain; iv) Bersara; atau v) Ditamatkan perkhidmatan.	
K/070202	**Hak Capaian**	
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem
K/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 DOFM seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c. panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf dan nombor (alphanumerik); d. kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. kata laluan sistem pengoperasian seperti w*indows* dan juga *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama; 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	Pentadbir Sistem, Pengguna

	selepas *login* kali pertama atau selepas kata laluan diset semula; h. kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i. kata kaluan ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan j. mengelakkan penggunaan semula kata laluan yang baru digunakan.	
K/070204	**Kad Pintar**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan kad pintar kerajaan elekronik (Kad EG) hendaklah digunakan bagi capaian sistem kerajaan elektronik yg dikhususkan. Proses permohonan kad pintar hendaklah dibuat melalui Cawangan Kewangan, B (P&K) DOFM. b. Kad pintar hendaklah disimpan ditempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain. c. Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat. d. Sebarang kehilangan, kerosakan dan katalaluan disekat terhadap kad pintar perlu dimaklumkan kepada pihak Cawangan Kewangan, B (P&K) DOFM.	Semua
K/0703	**Capaian Sistem Pengoperasian**	
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan b. merekodkan capaian yang berjaya dan gagal.	Pentadbir Sistem, ICTSO

	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 sistem pengoperasian terutama pengguna bertaraf *super user;* dan c. menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi termasuk berikut: a. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; dan 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.	
K/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 DOFM adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah 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, ICTSO

	c. mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; d. memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e. capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
K/0705	**Capaian Jarak Jauh**	
	a. Penghantaran maklumat yang menggunakan capaian jarak jauh menggunakan kaedah ***Remote Access*** mestilah menggunakan kaedah penyulitan (*encryption*). b. Lokasi bagi akses ke sistem ICT DOFM hendaklah dipastikan selamat. c. Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pengurus ICT. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	Pentadbir Rangkaian, Pentadbir Sistem
K/0706	**Capaian Internet**	
	a. Penggunaan Internet di DOFM hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code,* virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian DOFM. 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*	Pentadbir Rangkaian Pengurus ICT

	conferencing, *video streaming, chat, downloading*) adalah dicadangkan bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan. e. Penggunaan modem telefon untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali. f. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang fail atau aplikasi seperti permainan elektronik, video, gambar, lagu yang boleh menjejaskan tahap capaian internet. ii. Menyedia, memuat naik, memuat turun dan menyimpan bahan-bahan, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah ataupun hasutan terhadap Kerajaan.	
K/0707	**Pengauditan dan Forensik ICT**	
	Wakil DOFM yang menjadi ahli CERT MOA di DOFM mestilah bertanggungjawab merekod dan menganalisa: a. Sebarang percubaan pencerobohan kepada sistem ICT DOFM; 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;	CERT MOA, ICTSO, Pentadbir Sistem, Pentadbir Rangkaian

	g. aktiviti penyalahgunaan akaun e-mel; dan h. aktiviti penukaran *IP address* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian. 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.	
K/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 ciri-ciri 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

	Pentadbir Sistem hendaklah menyemak catatan jejak audit dari masa 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.	

KAWALAN 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

Objektif : Memastikan sistem yang dibangunkan atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.		
K/0801	**Keselamatan Dalam Membangunkan Sistem dan Aplikasi**	
K/080101	**Kawalan Prosesan Aplikasi**	
	a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; dan c. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pentadbir Sistem, ICTSO
K/080102	**Pengesahan Data Input**	
	Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.	Pentadbir Sistem
K/080103	**Kawalan Prosesan**	
	Kawalan prosesan perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan.	Pentadbir Sistem
K/080104	**Pengesahan Data Output**	
	Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat	Pentadbir Sistem

	yang dihasilkan adalah tepat.	
K/0802	**Kawalan Kriptografi**	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui teknik kriptografi.		
K/080201	**Penyulitan**	
	Setiap pengguna hendaklah membuat penyulitan/ enkripsi (*encryption*) ke atas sistem yang melibatkan maklumat sensitif atau kritikal atau maklumat rahsia rasmi bagi mengelakkan dari pendedahan dan penyelewengan maklumat berlaku.	Semua
K/080202	**Tandatangan Digital**	
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna kewangan yang menggunakan aplikasi eSPKB khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
K/0803	**Keselamatan Sistem Fail**	
Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.		
	Fail sistem perlu dikawal dan dikendalikan dengan baik dan selamat. Antara kawalan dan pengendalian tersebut adalah: a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;	Pentadbir Sistem

	d. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan e. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemas kinian untuk tujuan statistik, pemulihan dan keselamatan.	
K/0804	**Pembangunan dan Sokongan Sistem**	
Objektif : Memastikan keselamatan perisian sistem aplikasi dan maklumat dikawal supaya selamat dalam semua keadaan.		
K/080401	**Perubahan Prosedur**	
	Perubahan atau pengubah suaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum diguna pakai.	Pentadbir Sistem
K/080402	**Pembangunan Secara *Outsource***	
	Pembangunan perisian aplikasi secara *outsource* perlu dipantau oleh DOFM dan agensi di bawah DOFM. *Source code* adalah menjadi hak milik DOFM sekiranya ia adalah jenis perisian aplikasi *customized* untuk DOFM.	Pentadbir Sistem
K/080403	**Kawalan dari Ancaman Teknikal**	
	Maklumat mengenai ancaman teknikal sistem maklumat yang digunakan perlu diperolehi. Pendedahan organisasi kepada ancaman teknikal perlu dinilai bagi mengenalpasti tahap risiko yang bakal dihadapi.	Pentadbir Sistem

KAWALAN 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

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

K/0901	Mekanisme Pelaporan Insiden Keselamatan ICT	
	Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak –pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisma kawalan akses: i. hilang, dicuri atau didedahkan; atau ii. disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar;dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Sekiranya berlaku insiden keselamatan ICT, maka mekanisme pelaporan adalah seperti berikut: a. **Pelaporan**	Semua

	Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO dan wakil DOFM yang menjadi ahli CERT MOA untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan.	
	b. **CERT MOA** Wakil DOFM yang menjadi ahli dalam pasukan CERT MOA akan bertindak menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai *input* atau untuk tindakan seterusnya.	
	c. **Tanggungjawab Pengguna** Semua kakitangan, pembekal, pakar runding dan pihak-pihak lain yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden keselamatan ICT kepada ICTSO, kerentanan (*vulnerabality*) yang diperhatikan atau disyaki terdapat dalam sistem maklumat menerusi mekanisme pelaporan ini. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan menceroboh.	Semua
	d. **Tindakan Dalam Keadaan Berisiko Tinggi** Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak.	ICTSO, CERT MOA
	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	Semua
	Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di DOFM adalah sepertimana di Lampiran 3.	CIO, ICTSO
K/0902	**Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT**	
	Semua pegawai pasukan pengendali insiden keselamatan ICT di DOFM	ICTSO, MOA CERT

	atau CERT MOA perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur operasi standard keselamatan CERT MOA dan GCERT. Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak tinggi kepada DOFM.	

KAWALAN 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

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

K/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 DOFM dan perkara-perkara berikut perlu diberi perhatian: a. mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut akibat terhadap keselamatan ICT; c. melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; d. mendokumentasikan proses dan prosedur yang telah dipersetujui; e. membuat *backup*; dan f. menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	ICTSO

KAWALAN 11 PEMATUHAN

Objektif : Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT DOFM.		
K/1101	**Pematuhan dan Keperluan Perundangan**	
	Setiap pengguna di DOFM hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT DOFM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Semua aset ICT di DOFM termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Pengarah DOFM berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Semua
K/1102	**Pematuhan Dengan Dasar, Piawaian dan Keperluan Teknikal**	
	ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu melalui pemeriksaan secara berkala mengikut keperluan semasa bagi mematuhi standard pelaksanaan keselamatan.	ICTSO
K/1103	**Keperluan Perundangan**	
	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di DOFM: a. Arahan Keselamatan; b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”; c. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS); d. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet	Semua

	dan Mel Elektronik di DOFM-DOFM Kerajaan"; f. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; g. Surat Pekeliling Am Bil. 4 Tahun 2006 – "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam"; h. Surat Pekeliling Perbendaharaan Bil.2 Tahun 1995 (Tambahan pertama)- "Tatacara Penyediaan, Penilaian dan Penerimaan Tender"; i. Surat Pekeliling Perbendaharaan Bil. 3 Tahun 1995 -"Peraturan Perolehan Perkhidmatan Perundingan"; j. Akta Tandatangan Digital 1997; k. Akta Rahsia Rasmi 1972; l. Akta Jenayah Komputer 1997; m. Akta Hak cipta (Pindaan) Tahun 1997; n. Akta Komunikasi dan Multimedia 1998; o. Perintah-Perintah Am; p. Arahan Teknologi Maklumat 2007; q. Surat Akujanji; r. MPK Jabatan Perikanan Malaysia; s. Fail Meja Kakitangan; dan t. Arahan Perbendaharaan.	
K/1104	**Pelanggaran Dasar**	
	Pelanggaran Dasar Keselamatan ICT DOFM boleh dikenakan tindakan undang-undang dan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaian, kelalaian dan perlanggaran keselamatan yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 dan akta lain yang berkaitan.	Semua

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasa, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CCTV	*Closed-Circuit Television System* Sistem TV yang digunakan secara komersial di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
CERT MOA	Organisasi yang ditubuhkan untuk membantu MOA khususnya dan agensi di bawah MOA mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawabkan terhadap ICT dan sistem maklum menyokong arahtuju 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 direkabentuk 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 emel 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. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
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 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.

GLOSARI	
	Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindakbalas 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.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
Media	Peralatan yang digunakan untuk menyimpan dan menghantar maklumat atau data, seperti external *hard disk*, *thumbdrive*, CD/DVD, *flash memory*, *floppy* disk dll.
MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perrkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan

GLOSARI	
	rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense Multiple Access/Collision Detection (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Aturcara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran 1

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

Nama : .....

No. Kad Pengenalan : .....

Jawatan : .....

Kementerian/Jabatan : .....

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 DOFM; dan

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

.....
(Tandatangan Pegawai)
Nama :
Jawatan dan Gred Perkhidmatan :
Alamat Pejabat Penempatan :

Cop rasmi :
Tarikh : .....

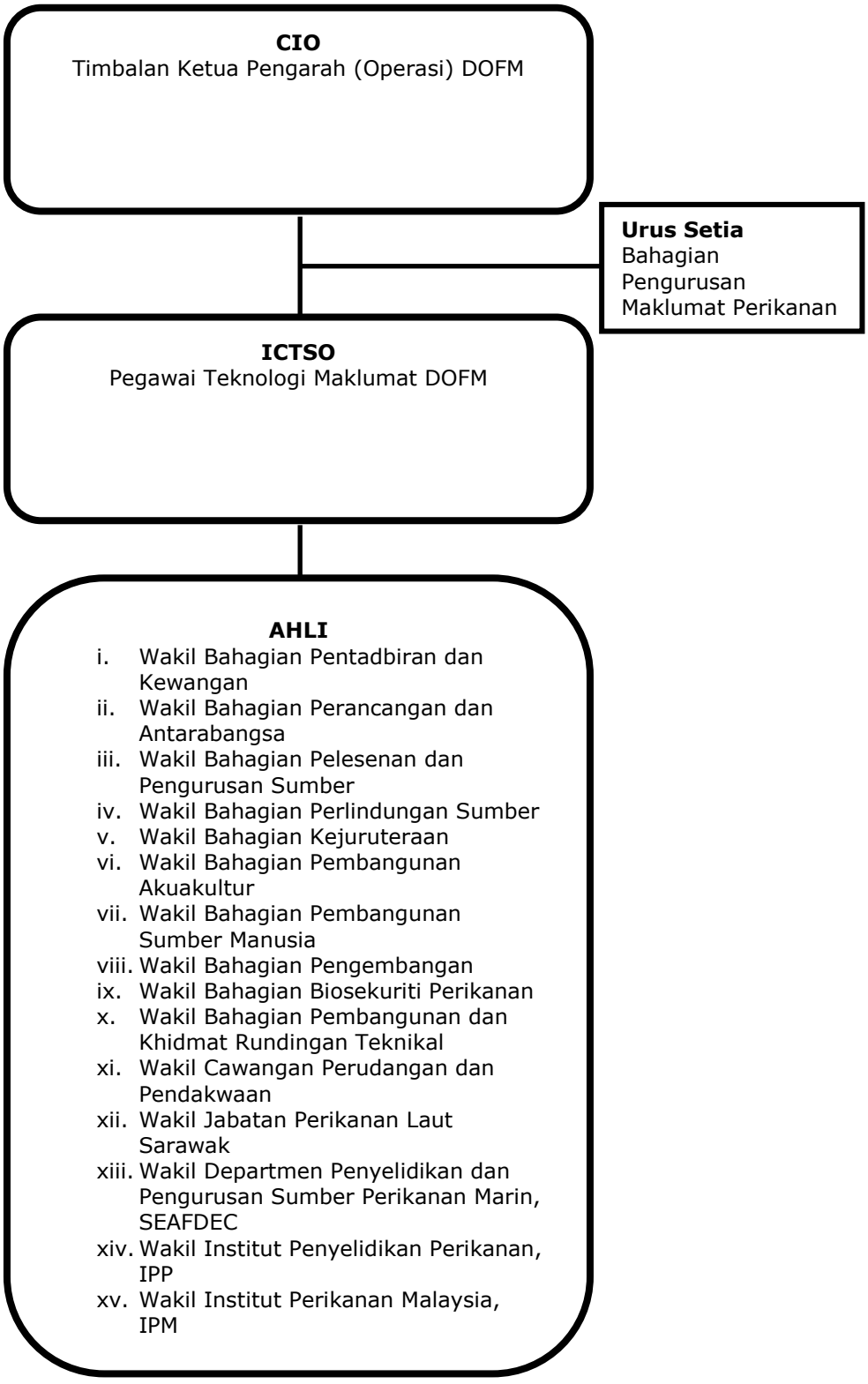
Pengesahan Pegawai Keselamatan ICT

.....
(Tandatangan Pegawai Keselamatan ICT)
b.p Ketua Pengarah Kementerian / Jabatan

Nama :
Jawatan dan Gred Perkhidmatan :
Cop rasmi :
Tarikh : .....

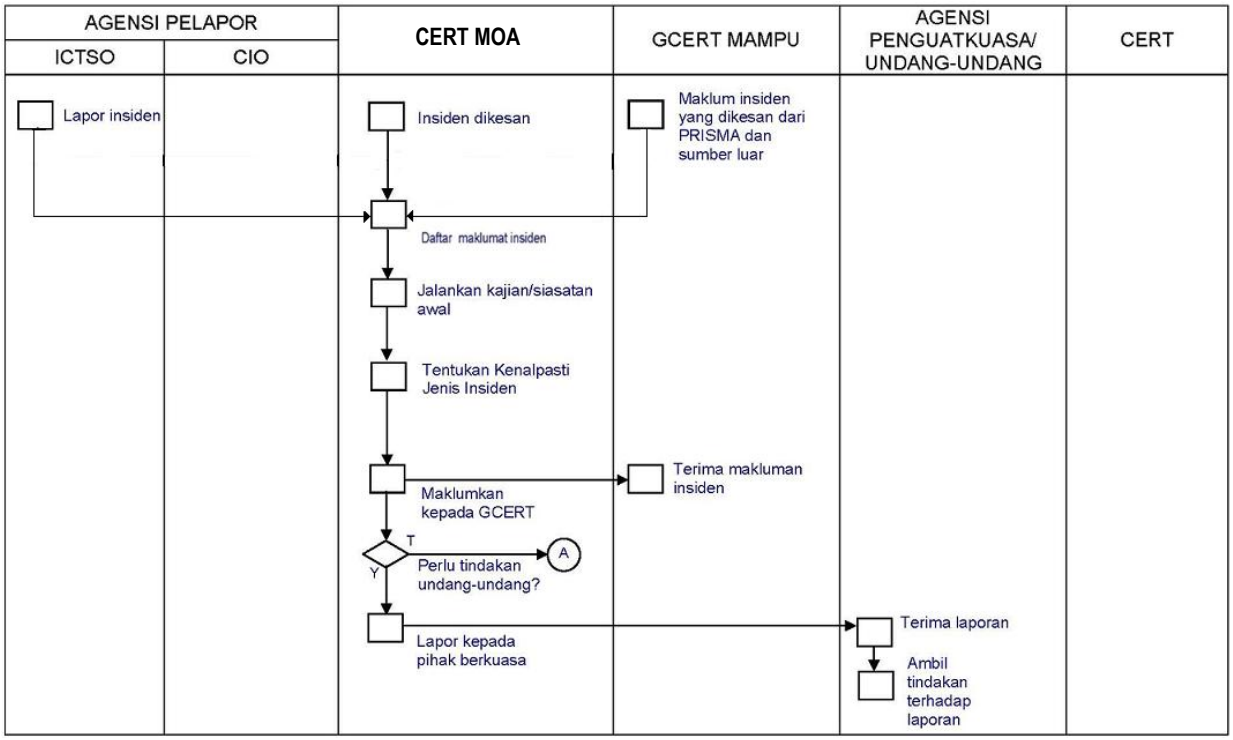
Lampiran 2

Carta 1 : Struktur Organisasi Jawatankuasa Pemandu ICT DOFM

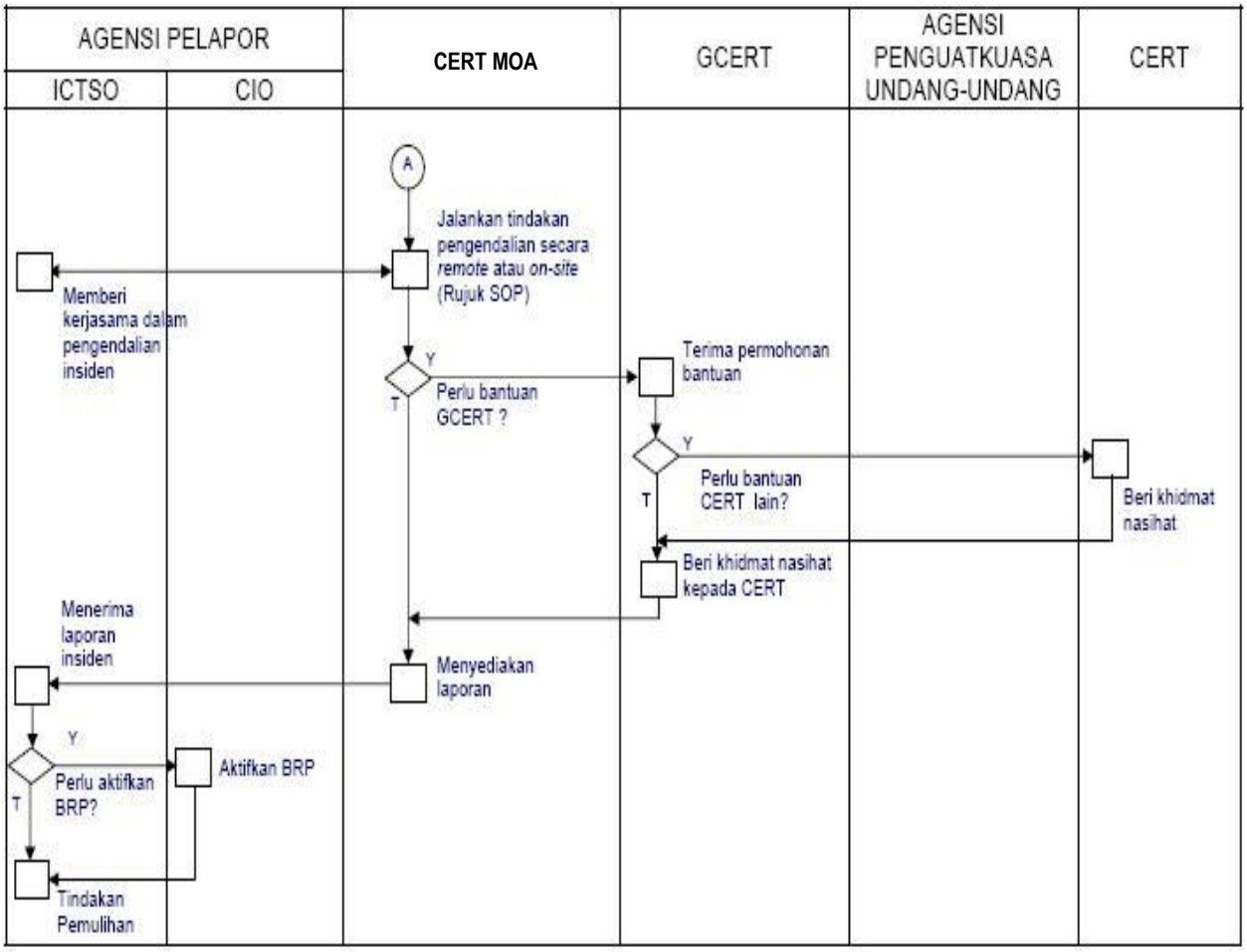


Lampiran 3

Rajah 1 : Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT DOFM



Rajah 2: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT DOFM



Penunjuk :

SOP - *Standard Operating Procedure*

BRP - *Business Recovery Procedure*

Lampiran 4

Borang Pengurusan Aset dan Penggunaan Sistem Aplikasi ICT (BICT-01)

BORANG PENGURUSAN ASET DAN SISTEM APLIKASI ICT [BICT-01]

PERHATIAN :

Sila lengkapkan maklumat di bawah di mana berkenaan.

Borang boleh difaks ke 03-8889 2498 (u.p: Pn. Faziella bt. Nat Jemi, Bahagian Pengurusan Maklumat Perikanan).

Sekiranya keterangan lanjut diperlukan, sila hubungi: En. Haszilan (03-88704311)
En. Asmadi (03-88704310)
Pn. Rafidah (03-88704312) atau
Cik Nurul Aini (03-88704314)

TUJUAN :

Sila tandakan (/) pada tujuan yang berkenaan :-

- ☐ Permohonan / Penamatan Akaun Emel
- ☐ Permohonan / Penamatan Akaun Sistem Aplikasi
- ☐ Permohonan Pinjaman Peralatan/Perisian ICT
- ☐ Permohonan Pinjaman/Akses Dokumen ICT
- ☐ Permohonan Akses Ke Pusat Data
- ☐ Akuan Penerimaan Aset ICT
- ☐ Aduan Teknikal

I: MAKLUMAT PENGGUNA/PEMOHONAN

Nama : _____ No KP Baru/Lama : _____

No. Tel : _____ No. Fax: _____ Emel _____

Kategori ☐ Warga DOF : Bahagian/Pejabat/Pusat/Institut : _____

☐ Nama Syarikat/Agensi Kerajaan : _____

Alamat : _____

II: PENERIMAAN HARDWARE/SOFTWARE

Item (nyatakan)	Bilangan	Harga Perolehan perunit	No. Pesanan Kerajaan	Nama Pembekal	Serial Numbet

III: PINJAMAN PERALATAN/PERISIAN

Aset Yang Dipinjam [Nyatakan Bilangan]

☐ PC ☐ Printer ☐ LCD Projector ☐ Lain-lain (Nyatakan) _____

Sebab diperlukan	Tempoh Pinjaman	Lokasi Penggunaan :

Rujukan	Versi	Tarikh	Mukasurat
BICT-01	1.0	1 Januari 2009	1/2

	Dari :	Sehingga :	

IV: AKAUN EMEL / SISTEM APLIKASI

Emel DOF	
ID Pengguna	:
Sebab permohonan / penamatan	:

Sistem Aplikasi (nyatakan)	ID Pengguna		Sebab permohonan / penamatan
	Pengguna Biasa	Pentadbir Sistem	

I: PINJAMAN/AKSES DOKUMEN ICT

Nama Dokumen (nyatakan)	Media/Bilangan			
	Hardcopy	Disket	CD	Alamat Emel

VI: ADUAN TEKNIKAL

Media Aduan :	☐ Lisan	☐ Emel	☐ Fax	☐ Telefon	☐ Surat
Jenis Aduan	☐ Rangkaian	☐ PC	☐ Printer	☐ Sistem Aplikasi	☐ Emel
Keterangan Aduan					

VII: AKSES PUSAT DATA

Tarikh (dari – hingga)	Masa Mula	Masa Tamat	Cara akses (Remote / On-site)	Sebab diperlukan

PENGESAHAN

Pemohon / Penerima	Cawangan Teknologi Maklumat
(Tandatangan)	(Tandatangan)
Nama :	Nama :
Jawatan :	Jawatan :
Bahagian/Pejabat /Institut/Pusat :	Catatan/ Status :
Tarikh :	Tarikh :

Rujukan	Versi	Tarikh	Mukasurat
BICT-01	1.0	1 Januari 2009	2/2

Lampiran 5

Borang Pelaporan Insiden Keselamatan

SULIT

Borang IRH 1.0 - Maklumat Pengendalian Insiden Keselamatan ICT

Tarikh dan Masa : Pengendalian

***Government Computer Emergency Response Team* (GCERT)**	
*No. Insiden	Tahun/Bulan/Kod Kategori/Bil insiden dalam tahun semasa **(Diisi oleh GCERT)**
*Tarikh & Masa Dikesan	**(Diisi oleh GCERT)**
Maklumat Organisasi/Agensi	
ICTSO 1. Nama 2. E-mel 3. Jawatan dan Gred 4. No. Telefon Pejabat 5. No. Telefon Bimbit	
Pentadbir Sistem 1. Nama 2. E-mel 3. Jawatan dan Gred 4. No. Telefon Pejabat 5. No. Telefon Bimbit	
Pegawai Perhubungan 1. Nama 2. E-mel 3. Jawatan dan Gred 4. No. Telefon Pejabat 5. No. Telefon Bimbit	
Alamat Penuh Agensi	
Bahagian/Unit Yang Melapor	
No. Telefon Agensi	
No. Faks	
Maklumat Perkakasan dan Perisian Yang Terlibat	
Hostname	
Domain	
DNS	
Alamat IP	

SULIT

SULIT

1. Internal 2. External	
Sistem Pengoperasian 1. Jenis 2. Versi 3. Service pack	
Kapasiti Disk	
Jenis *Hard Disk*	
Sistem Aplikasi / Perkhidmatan lain	
Maklumat Insiden	
Alamat IP Penyerang	
Jenis Insiden	e.g. unauthorized access, malicious code
Jenis Serangan	
Tindakan Yang Diambil Oleh GCERT	

Government Computer Emergency Response Team (GCERT)
Bahagian Pematuhan ICT, MAMPU, Aras 5, Blok B1, Parcel B,
Kompleks JPM, Pusat Pentadbiran Kerajaan Persekutuan, Putrajaya
Tel : +603-8872 5128 ; H/P : +012-3312205 ;
Faks : +603-8888 3286
Email : gcert@mampu.gov.my

SULIT

Jabatan Perikanan Malaysia
Bahagian Pengurusan Maklumat Perikanan (PMP)
Wisma Tani, Aras 3, Lot 4G2
No. 30, Persiaran Perdana, Presint 4
Pusat Pentadbiran Kerajaan Persekutuan
62628 Putrajaya
Laman Web Rasmi: www.dof.gov.my
E-mel: hqhelp@dof.gov.my
Telefon: 03-8870 4000
Faks (Ketua Pengarah): 03-8889 2460
Faks (PMP): 03-8889 2498