



Dasar Keselamatan ICT

**Jabatan Perikanan Malaysia (DOFM)
Kementerian Pertanian dan Industri Asas Tani**

November 2009

Versi 1.0

KANDUNGAN

PENGENALAN	6
RASIONAL	7
OBJEKTIF	8
PERNYATAAN DASAR.....	9
SKOP	11
PRINSIP-PRINSIP	14
KAWALAN 01 DASAR KESELAMATAN ICT.....	17
K/0101 Pelaksanaan Dasar.....	17
K/0102 Penyebaran Dasar.....	17
K/0103 Penyelenggaraan Dasar	17
K/0104 Pengecualian Dasar.....	18
KAWALAN 02 KESELAMATAN ORGANISANI	19
Infrastruktur Keselamatan Organisasi.....	19
K/0201 Infrastruktur Organisasi Dalaman	19
K/020101 Ketua Pengarah	19
K/020102 Ketua Pegawai Maklumat (CIO).....	19
K/020103 Pegawai Keselamatan ICT (ICTSO)	20
K/020104 Pengurus ICT.....	21
K/020105 <i>Super User</i>	22
K/020106 Pentadbir Sistem.....	22
K/020107 Pengguna.....	23
K/020108 Jawatankuasa Pemandu ICT DOFM	24
K/ 0202 Pihak Luar/ Asing	26
K/020201 Keperluan Keselamatan Kontrak Dengan Pihak Luar/ Asing	26
KAWALAN 03 PENGURUSAN ASET	27
K/030101 Inventori Aset.....	27
K/0302 Pengelasan dan Pengendalian Maklumat	27
K/030201 Pengelasan Maklumat	27
K/030202 Pengendalian Maklumat	28
KAWALAN 04 KESELAMATAN SUMBER MANUSIA.....	29
K/0401 Keselamatan ICT Dalam Tugas Harian	29
K/040101 Sebelum Perkhidmatan.....	29
K/040102 Semasa Perkhidmatan.....	29
K/040103 Bertukar Atau Tamat Perkhidmatan	30
KAWALAN 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN	32
K/0501 Keselamatan Fizikal dan Persekitaran.....	32
K/050101 Kawasan Larangan Lokasi ICT	32

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	2 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

K/0502	Keselamatan Peralatan	33
K/050201	Peralatan ICT	33
K/050202	Media Storan.....	34
K/050203	Media Tandatangan Digital.....	35
K/050204	Media Perisian dan Aplikasi	35
K/050205	Perkakasan Tanpa Penyeliaan (<i>Unattended Equipment</i>)	36
K/050206	Penyelenggaraan.....	36
K/050207	Pelupusan	37
K/050208	Clear Desk dan Clear Screen.....	38
K/0503	Keselamatan Persekitaran	38
K/050301	Kawalan Persekitaran.....	38
K/050302	Bekalan Kuasa	39
K/0504	Keselamatan Dokumen dan Sistem Dokumentasi.....	40
K/050401	Dokumen	40
KAWALAN 06	PENGURUSAN OPERASI DAN KOMUNIKASI	41
K/0601	Pengurusan Prosedur dan Operasi	41
K/060101	Pengendalian Prosedur	41
K/060102	Pengurusan Perubahan	41
K/060103	Pengasingan Tugas dan Tanggungjawab	42
K/0602	Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	42
K/060201	Perkhidmatan Penyampaian.....	42
K/0603	Perancangan dan Penerimaan Sistem	42
K/060301	Perancangan Kapasiti	42
K/060302	Penerimaan Sistem	43
K/0604	Perisian Berbahaya	43
K/060401	Perlindungan dari Perisian Berbahaya.....	43
K/0605	Housekeeping	44
K/060501	<i>Backup</i>	44
K/060502	Sistem Log.....	44
K/0606	Pengurusan Rangkaian	45
K/060601	Kawalan Infrastruktur Rangkaian	45
K/0607	Pengurusan Media.....	46
K/060701	Penghantaran dan Pemindahan	46
K/060702	Prosedur Pengendalian Media.....	46
K/0608	Pengurusan Pertukaran Maklumat	47
K/0609	Pengurusan Mel Elektronik (E-mel).....	47
K/0610	Pemantauan.....	48
KAWALAN 07	KAWALAN CAPAIAN.....	50
Dasar Kawalan Capaian	50	
K/0701	Kawalan Capaian	50
K/0702	Pengurusan Capaian Pengguna	50
K/070201	Akaun Pengguna	50
K/070202	Hak Capaian	51
K/070203	Pengurusan Kata Laluan.....	51

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	3 dari 78

K/070204	Kad Pintar	52
K/0703	Capaian Sistem Pengoperasian	52
K/0704	Capaian Aplikasi dan Maklumat.....	53
K/0705	Capaian Jarak Jauh	54
K/0706	Capaian Internet.....	54
K/0707	Pengauditan dan Forensik ICT	55
K/0708	Jejak Audit.....	56
KAWALAN 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT		58
K/0801	Keselamatan Dalam Membangunkan Sistem dan Aplikasi	58
K/080101	Kawalan Prosesan Aplikasi.....	58
K/080102	Pengesahan Data Input.....	58
K/080103	Kawalan Prosesan	58
K/080104	Pengesahan Data Output.....	58
K/0802	Kawalan Kriptografi	59
K/080201	Penyulitan.....	59
K/080202	Tandatangan Digital.....	59
K/0803	Keselamatan Sistem Fail	59
K/0804	Pembangunan dan Sokongan Sistem	60
K/080401	Perubahan Prosedur	60
K/080402	Pembangunan Secara <i>Outsource</i>	60
K/080403	Kawalan dari Ancaman Teknikal	60
KAWALAN 09	PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT .61	
K/0901	Mekanisme Pelaporan Insiden Keselamatan ICT.....	61
K/0902	Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT	62
KAWALAN 10	PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	64
K/1001	Pelan Kesinambungan Perkhidmatan	64
KAWALAN 11	PEMATUHAN	65
K/1101	Pematuhan dan Keperluan Perundangan	65
K/1102	Pematuhan Dengan Dasar, Piawaian dan Keperluan Teknikal	65
K/1103	Keperluan Perundangan.....	65
K/1104	Pelanggaran Dasar.....	66
LAMPIRAN 1		70
	SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA	70
LAMPIRAN 2		71

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	4 dari 78

Carta 1 : Struktur Organisasi Jawatankuasa Pemandu ICT DOFM..... 71

LAMPIRAN 3 72

Rajah 1 : Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT DOFM..... 72

Rajah 2: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT DOFM..... 73

LAMPIRAN 4 74

Borang Pengurusan Aset dan Penggunaan Sistem Aplikasi ICT (BICT-01) 74

LAMPIRAN 5 76

Borang Pelaporan Insiden Keselamatan 76

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	5 dari 78

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.

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	6 dari 78

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.

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	7 dari 78

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 keselamatan ICT kepada para kakitangan, pengguna dan pembekal;
- (f) Memperkemaskan pengurusan risiko; dan
- (g) Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal.

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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	8 dari 78

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;

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	9 dari 78

- (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.

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	10 dari 78

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 bergantung 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, diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran, dan yang dibuat salinan keselamatan ke dalam semua aset ICT, Ini akan

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	11 dari 78

dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:-

(a) **Perkakasan**

Semua aset yang digunakan untuk menyokong pemrosesan 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 pemrosesan 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.

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	12 dari 78

(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 pelanggaran 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, menyediakan, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT Jabatan Perikanan Malaysia.

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	13 dari 78

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 mewujudkan, 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;

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	14 dari 78

- (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 terperinci terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
- (vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari di ketahui umum.

(d) **Pengasingan**

Tugas-tugas mewujudkan, memadam, mengemas kini, mengubah dan mengesahkan data diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperinci, 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**

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	15 dari 78

Dasar Keselamatan ICT DOFM hendaklah dibaca, difahami dan dipatuhi. Pematuhan adalah merupakan prinsip penting dalam menghindar dan mengesan sebarang pelanggaran 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.

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	16 dari 78

KAWALAN 01 DASAR KESELAMATAN ICT

Dasar Keselamatan ICT		
<p>Objektif :</p> <p>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.</p>		
K/0101 Pelaksanaan Dasar		
	<p>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.</p>	Ketua Pengarah
K/0102 Penyebaran Dasar		
	<p>Dasar ini perlu disebar kepada semua pengguna Jabatan Perikanan dan agensi di bawahnya (termasuk kakitangan, pembekal, pakar runding dll.)</p>	ICTSO
K/0103 Penyelenggaraan Dasar		
	<p>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:</p> <ol style="list-style-type: none"> 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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	17 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	18 dari 78

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

	<p>Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut:</p> <ul style="list-style-type: none"> 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. 	<p>Ketua Pengarah</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------

K/020102 Ketua Pegawai Maklumat (CIO)

	<p>Timbalan Ketua Pengarah (Operasi) Jabatan Perikanan adalah merupakan Ketua Pegawai Maklumat (CIO).</p> <p>Peranan dan tanggung jawab beliau adalah seperti berikut:</p>	<p>CIO</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	19 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<ul style="list-style-type: none"> 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 tata tertib 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)

	<p>Jawatan ICTSO bagi DOFM adalah disandang oleh Ketua Unit Pentadbir Sistem dan Rangkaian Komunikasi yang merupakan Pegawai Teknologi Maklumat (PTM).</p> <p>Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:</p> <ul style="list-style-type: none"> 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 <i>Security Posture Assessment</i> (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
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	20 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>menyediakan langkah-langkah perlindungan yang bersesuaian;</p> <p>g. melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (CERT) MOA dan memaklukkannya kepada CIO;</p> <p>h. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;</p> <p>i. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT DOFM;</p> <p>j. memastikan Dasar Keselamatan ICT DOFM dikemas kini sesuai dengan perubahan teknologi, arahan Jabatan dan ancaman-ancaman dari semasa ke semasa;</p> <p>k. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan</p> <p>l. menandatangani “Surat Akuan Pematuhan” (Lampiran 1) bagi mematuhi Dasar Keselamatan ICT DOFM.</p>	
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

K/020104 **Pengurus ICT**

	<p>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 <i>Super User</i> di Pejabat Perikanan Negeri/ Institut/Pusat.</p> <p>Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:</p> <p>a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOFM;</p> <p>b. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan DOFM;</p> <p>c. menentukan kawalan akses pengguna terhadap aset ICT DOFM di Pusat Data;</p> <p>d. melaporkan sebarang perkara atau penemuan mengenai</p>	<p>Pengurus ICT</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	21 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	22 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT DOFM;</p> <p>d. memantau aktiviti capaian harian sistem aplikasi pengguna;</p> <p>e. menentukan kawalan akses pengguna terhadap sistem aplikasi DOFM;</p> <p>g. melaksanakan prinsip-prinsip DKICT dan menjaga kerahsiaan maklumat DOFM;</p> <p>h. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;</p> <p>i. menyimpan dan menganalisis rekod jejak audit; dan</p> <p>j. menandatangani “Surat Akuan Pematuhan” (Lampiran 1) bagi mematuhi Dasar Keselamatan ICT DOFM.</p>	
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

K/020107 Pengguna

	<p>Peranan dan tanggungjawab pengguna adalah seperti berikut:</p> <p>a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOFM;</p> <p>b. mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;</p> <p>c. lulus tapisan keselamatan;</p> <p>d. melaksanakan prinsip-prinsip Dasar Keselamatan ICT DOFM dan menjaga kerahsiaan maklumat DOFM;</p> <p>e. melaksanakan langkah-langkah perlindungan seperti berikut :-</p> <p>i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;</p> <p>ii. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;</p> <p>iii. menentukan maklumat sedia untuk digunakan;</p>	Pengguna
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	23 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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

	<p>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:</p> <p>Pengerusi: CIO</p> <p>Ahli:</p> <ul style="list-style-type: none"> 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
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	24 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

- 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 Keselamatan ICT DOFM; dan
- j. membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	25 dari 78

K/ 0202 Pihak Luar/ Asing	
K/020201 Keperluan Keselamatan Kontrak Dengan Pihak Luar/ Asing	
	<p>Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak luar/ asing dikawal.</p> <p>Perkara yang perlu dipatuhi termasuk yang berikut:</p> <ol style="list-style-type: none"> a. membaca, memahami dan mematuhi Dasar Keselamatan ICT DOFM; b. mengenalpasti risiko keselamatan maklumat dan kemudahan pemrosesan 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. <p>Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai.</p> <ol style="list-style-type: none"> i. Dasar Keselamatan ICT DOFM; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. <p>e. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT DOFM sebagaimana Lampiran 1.</p>
	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem dan Pihak Luar/ Asing

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	26 dari 78

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.

Pentadbir Sistem,
Semua

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.

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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	27 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>yang diberi kuasa mengikut dokumen Arahan Keselamatan.</p> <p>Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut:</p> <ol style="list-style-type: none"> a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad. 	
<p>K/030202 Pengendalian Maklumat</p>		
	<p>Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, pertukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan berikut :</p> <ol style="list-style-type: none"> 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. 	<p>Semua</p>

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	28 dari 78

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

	<p>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 kesusilaan, kecurian, penipuan dan penyalahgunaan aset ICT.</p> <p>Perkara-perkara yang mesti dipatuhi termasuk yang berikut:</p> <ol style="list-style-type: none"> 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

	<p>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</p>	Semua
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	29 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>meminimumkan risiko kesilapan, kecuaiian, kecurian, penipuan dan penyalahgunaan aset ICT.</p> <p>Perkara-perkara yang perlu dipatuhi termasuk yang berikut:</p> <ol style="list-style-type: none"> 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; 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; Melengkapkan Borang Pengurusan Aset dan Penggunaan Sistem Aplikasi ICT (BICT-01) seperti di Lampiran 4; 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 pelanggaran dengan perundangan dan peraturan ditetapkan oleh DOFM; dan 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

	<p>Ini bertujuan memastikan pertukaran atau tamat perkhidmatan pegawai dan kakitangan DOFM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan diurus dengan teratur.</p> <p>Perkara-perkara yang perlu dipatuhi termasuk yang berikut:</p> <ol style="list-style-type: none"> Memastikan semua aset ICT dikembalikan kepada DOFM 	Semua
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	30 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	31 dari 78

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

	<p>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.</p> <p>Kawasan ini mestikan dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke premis tersebut adalah seperti berikut:</p> <ol style="list-style-type: none"> 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; akses adalah terhad kepada pegawai yang telah diberikan kuasa sahaja dan dipantau pada setiap masa; pemantauan dibuat menggunakan Closed-Circuit Television (CCTV) kamera atau lain-lain peralatan yang sesuai; pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemungahan dan laluan awam; memperkuhkan tingkap dan pintu serta dikunci untuk mengawal keselamatan; melengkapkan Borang Pengurusan Aset dan Penggunaan Sistem 	<p>Pentadbir Pusat Data, Pentadbir Sistem</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	32 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	33 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<ul style="list-style-type: none"> i. semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (<i>air ventilation</i>) 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 <i>password administrator</i> 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

	<p>Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, <i>optical disk</i>, <i>USB flash drive</i>, CDROM dan media storan lain.</p> <p>Media-media storan perlu dipastikan berada dalam keadaan yang baik,</p>	Semua
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	34 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.</p> <p>Bagi menjamin keselamatan, langkah-langkah berikut perlu diambil:</p> <ol style="list-style-type: none"> 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 <i>USB flash drive</i>; bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu; semua media storan data yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat; 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 sebarang kehilangan media storan yang berlaku hendaklah dilaporkan mengikut Prosedur Pelaporan Insiden. 	
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

K/050203 Media Tandatangan Digital

	<p>Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah-langkah berikut:</p> <ol style="list-style-type: none"> pegawai hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; tidak boleh dipindah-milik atau dipinjamkan; dan sebarang insiden kehilangan yang berlaku hendaklah dilaporkan mengikut Prosedur Pelaporan Insiden. 	Semua
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

K/050204 Media Perisian dan Aplikasi

	<p>Sebarang media yang digunakan sebagai media perisian dan aplikasi hendaklah mematuhi langkah-langkah berikut:</p>	Pengurus ICT, Pegawai Aset, Pentadbir Sistem
--	----------------------------------------------------------------------------------------------------------------------	----------------------------------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	35 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<ul style="list-style-type: none"> a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan Jabatan; b. Sistem aplikasi dalaman tidak dibenarkan diagih/ didemonstrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c. Lesen perisian (<i>registration code, serials, CD-keys</i>) perlu disimpan berasingan daripada CD-ROM, disk atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; d. <i>Source code</i> 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*)

	<p>Pengguna perlu memastikan mana-mana perkakasan yang ditinggalkan tanpa penyeliaan mematuhi ciri-ciri keselamatan seperti mempunyai kata laluan dan sebagainya.</p> <p>Perkakasan hendaklah disenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.</p>	Semua
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

K/050206 Penyelenggaraan

	<p>Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti.</p> <p>Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:</p> <ul style="list-style-type: none"> a. Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; 	Pegawai Aset Bahagian/ Institut/ Pusat
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	36 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<ul style="list-style-type: none"> 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

	<p>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.</p> <p>Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan DOFM.</p> <p>Langkah-langkah seperti berikut hendaklah diambil:</p> <ul style="list-style-type: none"> 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 dikhasakan 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:- <ul style="list-style-type: none"> 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. 	<p>Pegawai Aset Bahagian/ Institut/ Pusat</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	37 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<ul style="list-style-type: none"> 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

	<p>Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.</p> <p>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.</p> <p>Langkah-langkah perlu diambil termasuklah seperti berikut:</p> <ul style="list-style-type: none"> a. Menggunakan kemudahan <i>password screen saver</i> atau <i>logout</i> 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

--	--	--

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	38 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>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).</p> <p>Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil :</p> <ol style="list-style-type: none"> Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; 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; Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan perkomputeran; Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; dan Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer. 	Semua
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

K/050302 Bekalan Kuasa

	<p>Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.</p> <p>Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa:</p> <ol style="list-style-type: none"> Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; dan Peralatan sokongan seperti UPS (<i>Uninterruptible Power Supply</i>) 	<p>Semua</p> <p>Pentadbir Pusat</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	39 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	dan penjana (<i>generator</i>) 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	
	<p>Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi:</p> <ol style="list-style-type: none"> Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; 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; Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; Pelupusan dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan Menggunakan penyulitan (<i>encryption</i>) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik. 	Pentadbir Sistem, Pentadbir Fail

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	40 dari 78

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

	<ul style="list-style-type: none"> a. Semua prosedur keselamatan ICT yang diwujudkan, 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

	<ul style="list-style-type: none"> 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
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	41 dari 78

K/060103 Pengasingan Tugas dan Tanggungjawab		
	<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut dengan syarat cadangan penambahan kakitangan dalam ISP Jabatan Perikanan Tahun 2007 – 2011 dipenuhi:</p> <ol style="list-style-type: none"> Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; Tugas mewujudkan, 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 Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai <i>production</i>. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. 	Pengurus ICT , ICTSO
K/0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga		
K/060201 Perkhidmatan Penyampaian		
	<p>Perkara-perkara yang mesti dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi dilaksanakan dan diselenggarakan oleh pihak ketiga; Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan 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		
	<ol style="list-style-type: none"> Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan 	Pentadbir Sistem, ICTSO

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	42 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan</p> <p>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.</p>	
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

K/060302 Penerimaan Sistem

	<p>Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.</p>	<p>Pentadbir Sistem, ICTSO</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------

K/0604 Perisian Berbahaya

K/060401 Perlindungan dari Perisian Berbahaya

	<p>Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT dari perisian berbahaya:</p> <p>a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti <i>antivirus</i> dan <i>Intrusion Detection System (IDS)</i> dan mengikut prosedur penggunaan yang betul dan selamat;</p> <p>b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa;</p> <p>c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;</p> <p>d. Mengemas kini <i>antivirus</i> dengan <i>pattern</i> dari semasa ke semasa;</p> <p>e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;</p> <p>f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;</p> <p>g. Memasukkan klausa tanggungan di dalam mana-mana kontrak</p>	<p>Pentadbir Sistem</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	43 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>yang telah ditawarkan kepada pembekal perisian. Klausula ini akan digunakan sekiranya perisian tersebut mengandungi program berbahaya; dan</p> <p>h. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.</p>	
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

K/0605 Housekeeping

K/060501 Backup

	<p>Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan backup seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan <i>backup</i> hendaklah direkodkan dan disimpan di <i>offsite</i>.</p> <p>a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;</p> <p>b. Membuat salinan <i>backup</i> ke atas semua data dan maklumat mengikut kesesuaian operasi;</p> <p>c. Menguji sistem <i>backup</i> sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.</p> <p>d. <i>Backup</i> hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan <i>backup</i> bergantung pada tahap kritikal maklumat; dan</p> <p>e. DOFM hendaklah menyimpan sekurang-kurangnya tiga (3) generasi <i>backup</i>.</p>	<p>Pentadbir Sistem, Pentadbir Pusat Data</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------

K/060502 Sistem Log

	<p>Pentadbir Sistem hendaklah melaksanakan perkara-perkara seperti berikut:</p> <p>a. Mewujudkan sistem log bagi merekod semua aktiviti harian pengguna;</p> <p>b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan</p>	<p>Pentadbir Sistem</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	44 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>membaik pulih dengan segera; dan</p> <p>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.</p>	
K/0606 Pengurusan Rangkaian		
K/060601 Kawalan Infrastruktur Rangkaian		
	<p>Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.</p> <p>Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut :-</p> <p>a. Semua tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;</p> <p>b. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;</p> <p>c. <i>Firewall</i> hendaklah dipasang di Ibu Pejabat, antara rangkaian dalaman dan sistem yang melibatkan maklumat rasmi Kerajaan serta dikonfigurasi oleh kontraktor penyelenggara dan diselua oleh Pentadbir Sistem;</p> <p>d. Semua trafik keluar dan masuk Ibu Pejabat Perikanan hendaklah melalui <i>firewall</i> di bawah kawalan DOFM;</p> <p>e. Semua perisian <i>sniffer</i> atau <i>network analyser</i> adalah dilarang dipasang pada komputer peribadi kecuali mendapat kebenaran ICTSO;</p> <p>f. Memasang perisian <i>Intrusion Detection System (IDS)</i> bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat DOFM;</p> <p>g. Memasang <i>Web Content Filter</i> pada <i>Internet Gateway</i> untuk menyekat aktiviti kemasukan dari atau capaian pada laman web/Internet yang mengandungi maklumat atau unsur-unsur tidak</p>	<p>Pentadbir Rangkaian dan <i>Super User</i></p>

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	45 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>sihat dan berbahaya yang boleh menjejaskan integriti kakitangan, sistem dan maklumat;</p> <p>h. Sebarang penyambungan rangkaian yang bukan di bawah kawalan DOFM adalah tidak dibenarkan;</p> <p>i. Semua pengguna di Ibu Pejabat hanya dibenarkan menggunakan rangkaian DOFM sahaja di mana penggunaan modem adalah dilarang sama sekali; dan</p> <p>j. Kemudahan bagi <i>wireless</i> LAN perlu dipastikan kawalan keselamatan di semua premis pejabat.</p>	
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		
	<p>Di antara prosedur-prosedur pengendalian media termasuk:</p> <p>a. Melabelkan semua media mengikut tahap keselamatan sesuatu maklumat;</p> <p>b. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;</p> <p>c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;</p> <p>d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;</p> <p>e. Menyimpan semua media di tempat yang selamat; dan</p> <p>f. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.</p>	Semua

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	46 dari 78

K/0608 Pengurusan Pertukaran Maklumat	
	<p>Pengurusan Pertukaran Maklumat bertujuan untuk memastikan keselamatan pertukaran maklumat dan perisian dalam DOFM dan mana-mana entiti luar terjamin.</p> <p>Langkah-langkah bagi Pengurusan Pertukaran Maklumat adalah seperti berikut:</p> <ol style="list-style-type: none"> 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)	
	<p>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:</p> <p>Di antara langkah-langkah pengendalian mel elektronik termasuk:</p> <ol style="list-style-type: none"> a. Menghadkan jenis dan saiz fail lampiran bagi tujuan mengelakkan jangkitan virus dan serangan e-mel <i>bombing</i>; b. Penghantaran dokumen rasmi hendaklah menggunakan e-mel rasmi jabatan sahaja;
	Semua

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	47 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	48 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<ul style="list-style-type: none"> 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. 	
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	49 dari 78

KAWALAN 07 Kawalan Capaian

Dasar Kawalan Capaian

Objektif :

Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT DOFM.

K/0701 Kawalan Capaian

	<p>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.</p>	<p>Pentadbir Sistem</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------

K/0702 Pengurusan Capaian Pengguna

Objektif :

Mengawal capaian pengguna ke atas aset ICT DOFM.

K/070201 Akaun Pengguna

	<p>Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi:</p> <ul style="list-style-type: none"> a. akaun yang diperuntukkan oleh jabatan sahaja yang boleh digunakan; b. akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. akaun pengguna yang diwujudkan 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 	<p>Pentadbir Sistem, Pengguna</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	50 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>f. Pentadbir Sistem boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut;</p> <ul style="list-style-type: none"> 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	
	<p>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:</p> <ul style="list-style-type: none"> 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 (alphanumeric); d. kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. kata laluan sistem pengoperasian seperti <i>windows</i> dan juga <i>screen saver</i> 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 <i>login</i> kali pertama atau 	Pentadbir Sistem, Pengguna

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	51 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>selepas <i>login</i> kali pertama atau selepas kata laluan diset semula;</p> <p>h. kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;</p> <p>i. kata laluan ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan</p> <p>j. mengelakkan penggunaan semula kata laluan yang baru digunakan.</p>	
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

K/070204 Kad Pintar

	<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a. Penggunaan kad pintar kerajaan elektronik (Kad EG) hendaklah digunakan bagi capaian sistem kerajaan elektronik yg dikhususkan. Proses permohonan kad pintar hendaklah dibuat melalui Cawangan Kewangan, B (P&K) DOFM.</p> <p>b. Kad pintar hendaklah disimpan ditempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain.</p> <p>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.</p> <p>d. Sebarang kehilangan, kerosakan dan katalaluan disekat terhadap kad pintar perlu dimaklumkan kepada pihak Cawangan Kewangan, B (P&K) DOFM.</p>	Semua
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

K/0703 Capaian Sistem Pengoperasian

	<p>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:</p> <p>a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan</p> <p>b. merekodkan capaian yang berjaya dan gagal.</p>	Pentadbir Sistem, ICTSO
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	52 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:</p> <ol style="list-style-type: none"> Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf <i>super user</i>; dan menjana amaran (<i>alert</i>) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem. <p>Perkara-perkara yang perlu dipatuhi termasuk berikut:</p> <ol style="list-style-type: none"> Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur <i>log on</i> yang terjamin; dan 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

	<p>Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.</p> <p>Capaian sistem dan aplikasi di DOFM adalah terhad kepada pengguna dan tujuan yang dibenarkan.</p> <p>Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi:</p> <ol style="list-style-type: none"> Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log) bagi mengesan aktiviti-aktiviti yang tidak diingini; 	<p>Pentadbir Sistem, ICTSO</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	53 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>c. menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;</p> <p>d. memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan</p> <p>e. capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.</p>	
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

K/0705 Capaian Jarak Jauh

	<p>a. Penghantaran maklumat yang menggunakan capaian jarak jauh menggunakan kaedah Remote Access mestilah menggunakan kaedah penyulitan (<i>encryption</i>).</p> <p>b. Lokasi bagi akses ke sistem ICT DOFM hendaklah dipastikan selamat.</p> <p>c. Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pengurus ICT. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.</p>	<p>Pentadbir Rangkaian, Pentadbir Sistem</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------

K/0706 Capaian Internet

	<p>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 <i>malicious code</i>, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian DOFM.</p> <p>b. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya.</p> <p>c. Kaedah <i>Content Filtering</i> mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan.</p> <p>d. Penggunaan teknologi (<i>packet shaper</i>) untuk mengawal aktiviti (<i>video</i></p>	<p>Pentadbir Rangkaian</p> <p>Pengurus ICT</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	54 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p><i>conferencing, video streaming, chat, downloading</i>) adalah dicadangkan bagi menguruskan penggunaan <i>bandwidth</i> yang maksimum dan lebih berkesan.</p> <p>e. Penggunaan modem telefon untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali.</p> <p>f. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:</p> <p>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.</p> <p>ii. Menyedia, memuat naik, memuat turun dan menyimpan bahan-bahan, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah ataupun hasutan terhadap Kerajaan.</p>	
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

K/0707 Pengauditan dan Forensik ICT

	<p>Wakil DOFM yang menjadi ahli CERT MOA di DOFM mestilah bertanggungjawab merekod dan menganalisa:</p> <p>a. Sebarang percubaan pencerobohan kepada sistem ICT DOFM;</p> <p>b. serangan kod perosak (<i>malicious code</i>), halangan pemberian perkhidmatan (<i>denial of service</i>), <i>spam</i>, pemalsuan (<i>forgery, phishing</i>), pencerobohan (<i>intrusion</i>) ancaman (<i>threats</i>) dan kehilangan fizikal (<i>physical loss</i>);</p> <p>c. pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;</p> <p>d. aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;</p> <p>e. aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;</p> <p>f. aktiviti instalasi dan penggunaan perisian yang membebankan <i>bandwidth</i> rangkaian;</p>	<p>CERT MOA, ICTSO, Pentadbir Sistem, Pentadbir Rangkaian</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	55 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>g. aktiviti penyalahgunaan akaun e-mel; dan</p> <p>h. aktiviti penukaran <i>IP address</i> selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian.</p> <p>Langkah-langkah yang perlu diambil adalah seperti berikut:</p> <p>a. ICTSO akan menentukan prosedur pengumpulan bahan bukti (<i>hard disk/media storan</i>) yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan.</p> <p>b. Proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat.</p> <p>c. Sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, laporan khas perlu disediakan.</p> <p>Semua proses dan hasil siasatan adalah SULIT.</p>	
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

K/0708 Jejak Audit

	<p>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.</p> <p>Jejak audit hendaklah mengandungi ciri-ciri berikut:</p> <p>a. Rekod setiap aktiviti transaksi;</p> <p>b. maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;</p> <p>c. aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan</p> <p>d. maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.</p> <p>Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara.</p>	<p>Pentadbir Sistem</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	56 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>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.</p>	
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	57 dari 78

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

	<p>a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemrosesan dan ketepatan maklumat;</p> <p>b. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemrosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; dan</p> <p>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.</p>	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 <i>output</i> daripada aplikasi perlu disahkan bagi memastikan maklumat	Pentadbir Sistem
--	------------------------------------------------------------------------------	------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	58 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	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 (<i>encryption</i>) 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: <ul style="list-style-type: none"> 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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	59 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	60 dari 78

**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

	<p>Insiden keselamatan ICT bermaksud musibah (<i>adverse event</i>) 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.</p> <p>Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. <p>Sekiranya berlaku insiden keselamatan ICT, maka mekanisme pelaporan adalah seperti berikut:</p> <p>a. Pelaporan</p>	Semua
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	61 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

	<p>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.</p> <p>b. CERT MOA</p> <p>Wakil DOFM yang menjadi ahli dalam pasukan CERT MOA akan bertindak menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai <i>input</i> atau untuk tindakan seterusnya.</p> <p>c. Tanggungjawab Pengguna</p> <p>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 (<i>vulnerability</i>) 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.</p> <p>d. Tindakan Dalam Keadaan Berisiko Tinggi</p> <p>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.</p> <p>Prosedur pelaporan insiden keselamatan ICT berdasarkan:</p> <p>a. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan</p> <p>b. Surat Pekeliling Am Bilangan 4 tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam</p> <p>Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di DOFM adalah sepertimana di Lampiran 3.</p>	<p>Semua</p> <p>ICTSO, CERT MOA</p> <p>Semua</p> <p>CIO, ICTSO</p>
K/0902 Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT		
	<p>Semua pegawai pasukan pengendali insiden keselamatan ICT di DOFM</p>	<p>ICTSO, MOA CERT</p>

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	62 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

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.

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	63 dari 78

KAWALAN 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Objektif :

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

K/1001 Pelan Kesinambungan Perkhidmatan

	<p>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:</p> <ul style="list-style-type: none"> 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 <i>backup</i>; dan f. menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. 	ICTSO
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	64 dari 78

KAWALAN 11 PEMATUHAN

Objektif :

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT DOFM.

K/1101 Pematuhan dan Keperluan Perundangan

	<p>Setiap pengguna di DOFM hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT DOFM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa.</p> <p>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.</p>	Semua
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

K/1102 Pematuhan Dengan Dasar, Piawaian dan Keperluan Teknikal

	<p>ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.</p> <p>Sistem maklumat perlu melalui pemeriksaan secara berkala mengikut keperluan semasa bagi mematuhi standard pelaksanaan keselamatan.</p>	ICTSO
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

K/1103 Keperluan Perundangan

	<p>Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di DOFM:</p> <ul style="list-style-type: none"> a. Arahan Keselamatan; b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”; c. <i>Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)</i>; 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
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	65 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	66 dari 78

GLOSARI

<i>Antivirus</i>	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, <i>optical disk</i> , <i>flash disk</i> , CDROM untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasa, perisian, perkhidmatan, data atau maklumat dan manusia.
<i>Backup</i>	Proses penduaan sesuatu dokumen atau maklumat.
<i>Bandwidth</i>	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
<i>CCTV</i>	<i>Closed-Circuit Television System</i> 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	<i>Chief Information Officer</i> Ketua Pegawai Maklumat yang bertanggungjawabkan terhadap ICT dan sistem maklumat menyokong arahnya sesebuah organisasi.
<i>Denial of service</i>	Halangan pemberian perkhidmatan.
<i>Downloading</i>	Aktiviti muat-turun sesuatu perisian.
<i>Encryption</i>	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
<i>Firewall</i>	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.
<i>Forgery</i>	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (<i>information theft / espionage</i>), penipuan(<i>hoaxes</i>).
GCERT	<i>Government Computer Emergency Response Team</i> 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.
<i>Hard disk</i>	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
<i>Hub</i>	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bus berbentuk bintang dan menyiarkan (<i>broadcast</i>) data yang diterima daripada sesuatu <i>port</i> kepada semua <i>port</i> yang lain.
ICT	<i>Information and Communication Technology</i> .(Teknologi Maklumat dan Komunikasi).
ICTSO	<i>ICT Security Officer</i> Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (<i>server</i>) atau komputer lain.
<i>Internet Gateway</i>	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain.

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	67 dari 78

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.
<i>Intrusion Detection System (IDS)</i>	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 <i>host</i> atau rangkaian.
<i>Intrusion Prevention System (IPS)</i>	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 <i>malicious code</i> . Contohnya: <i>Network-based IPS</i> yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	<i>Local Area Network</i> Rangkaian Kawasan Setempat yang menghubungkan komputer.
<i>Logout</i>	<i>Log-out</i> komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
<i>Malicious Code</i>	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, <i>trojan horse</i> , <i>worm</i> , <i>spyware</i> dan sebagainya.
Media	Peralatan yang digunakan untuk menyimpan dan menghantar maklumat atau data, seperti external <i>hard disk</i> , <i>thumbdrive</i> , CD/DVD, <i>flash memory</i> , <i>floppy disk</i> 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.
<i>Outsource</i>	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 <i>spreadsheet</i> dan <i>word processing</i> ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
<i>Public-Key Infrastructure (PKI)</i>	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
<i>Router</i>	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
<i>Screen saver</i>	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
<i>Server</i>	Pelayan komputer
<i>Switches</i>	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	68 dari 78

GLOSARI

	rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense Multiple Access/Collision Detection (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan pelanggaran yang berlaku.
<i>Threat</i>	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
<i>Uninterruptible Power Supply (UPS)</i>	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
<i>Video Conference</i>	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
<i>Video Streaming</i>	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.
<i>Wireless LAN</i>	Jaringan komputer yang terhubung tanpa melalui kabel.

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	69 dari 78

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 :

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	70 dari 78

Lampiran 2

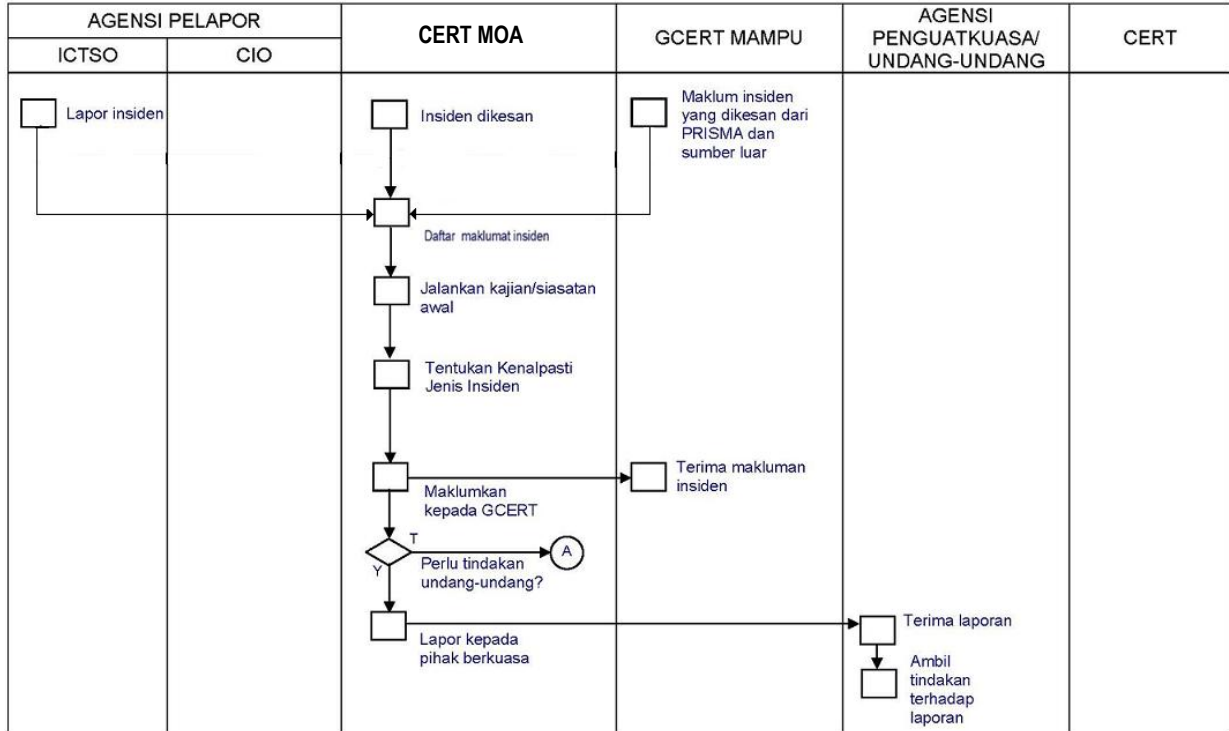
Carta 1 : Struktur Organisasi Jawatankuasa Pemandu ICT DOFM



RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	71 dari 78

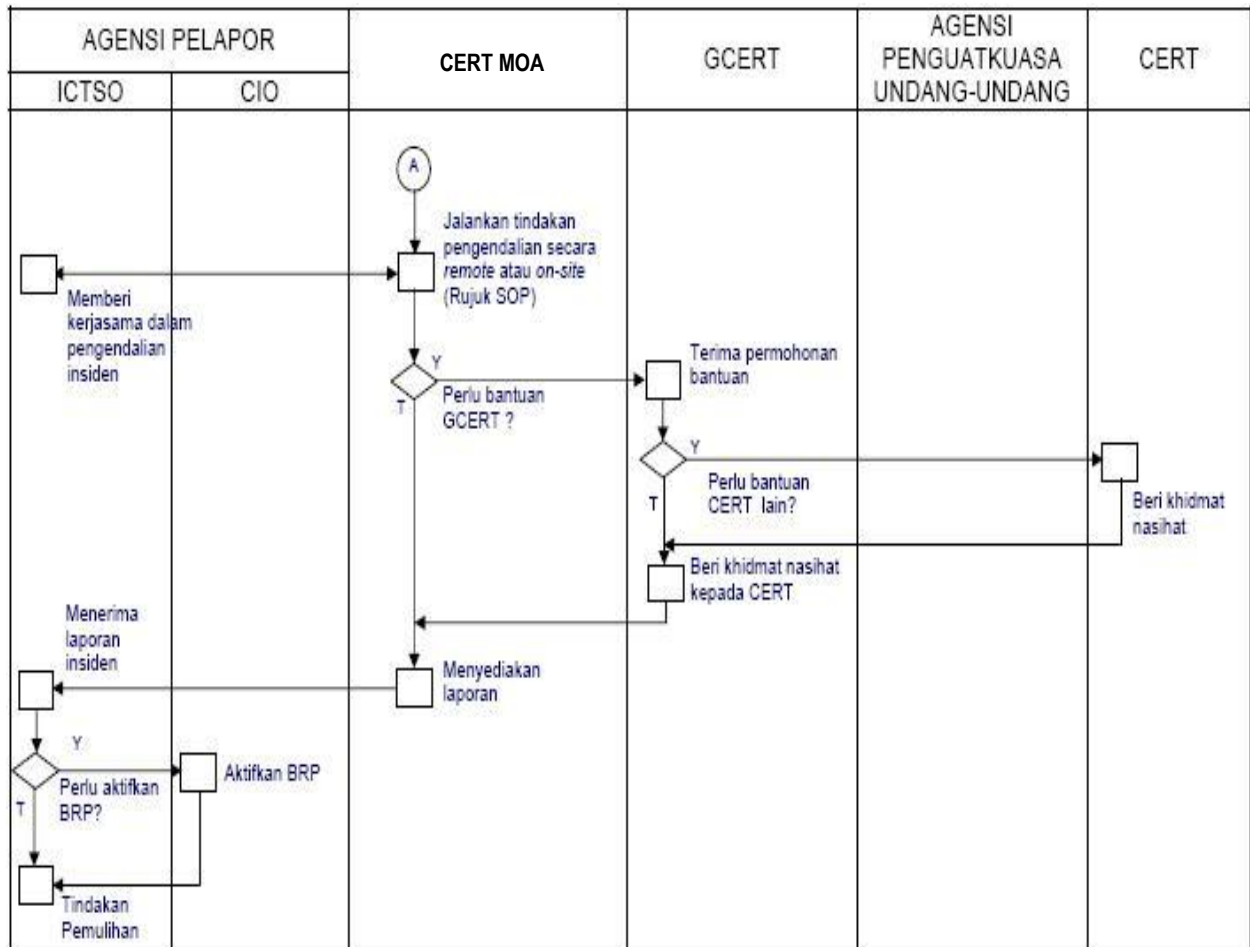
Lampiran 3

Rajah 1 : Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT DOFM



RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	72 dari 78

Rajah 2: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT DOFM



Penunjuk :



SOP - *Standard Operating Procedure*

BRP - *Business Recovery Procedure*

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	73 dari 78

Lampiran 4

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

	BORANG PENGURUSAN ASET DAN SISTEM APLIKASI ICT [BICT-01]									
<p>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)</p>										
<p>TUJUAN : Sila tandakan (/) pada tujuan yang berkenaan :-</p> <table style="width: 100%;"> <tr> <td><input type="checkbox"/> Permohonan / Penamatan Akaun Emel</td> <td><input type="checkbox"/> Permohonan Akses Ke Pusat Data</td> </tr> <tr> <td><input type="checkbox"/> Permohonan / Penamatan Akaun Sistem Aplikasi</td> <td><input type="checkbox"/> Akaun Penerimaan Aset ICT</td> </tr> <tr> <td><input type="checkbox"/> Permohonan Pinjaman Peralatan/Perisian ICT</td> <td><input type="checkbox"/> Aduan Teknikal</td> </tr> <tr> <td><input type="checkbox"/> Permohonan Pinjaman/Akses Dokumen ICT</td> <td></td> </tr> </table>			<input type="checkbox"/> Permohonan / Penamatan Akaun Emel	<input type="checkbox"/> Permohonan Akses Ke Pusat Data	<input type="checkbox"/> Permohonan / Penamatan Akaun Sistem Aplikasi	<input type="checkbox"/> Akaun Penerimaan Aset ICT	<input type="checkbox"/> Permohonan Pinjaman Peralatan/Perisian ICT	<input type="checkbox"/> Aduan Teknikal	<input type="checkbox"/> Permohonan Pinjaman/Akses Dokumen ICT	
<input type="checkbox"/> Permohonan / Penamatan Akaun Emel	<input type="checkbox"/> Permohonan Akses Ke Pusat Data									
<input type="checkbox"/> Permohonan / Penamatan Akaun Sistem Aplikasi	<input type="checkbox"/> Akaun Penerimaan Aset ICT									
<input type="checkbox"/> Permohonan Pinjaman Peralatan/Perisian ICT	<input type="checkbox"/> Aduan Teknikal									
<input type="checkbox"/> Permohonan Pinjaman/Akses Dokumen ICT										
I: MAKLUMAT PENGGUNA/PEMOHONAN										
Nama : _____ No KP Baru/Lama : _____ No. Tel : _____ No. Fax: _____ Emel _____ Kategori <input type="checkbox"/> Warga DOF : Bahagian/Pejabat/Pusat/Institut : _____ <input type="checkbox"/> 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]										
<input type="checkbox"/> PC <input type="checkbox"/> Printer <input type="checkbox"/> LCD Projector <input type="checkbox"/> Lain-lain (Nyatakan) _____										
Sebab diperlukan		Tempoh Pinjaman		Lokasi Penggunaan :						

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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	74 dari 78

DASAR KESELAMATAN ICT JABATAN PERIKANAN MALAYSIA

		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 :	<input type="checkbox"/> Lisan	<input type="checkbox"/> Emel	<input type="checkbox"/> Fax	<input type="checkbox"/> Telepon	<input type="checkbox"/> Surat
Jenis Aduan	<input type="checkbox"/> Rangkaian	<input type="checkbox"/> PC	<input type="checkbox"/> Printer	<input type="checkbox"/> Sistem Aplikasi	<input type="checkbox"/> 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 :			Catatan/Status :		
//Institut/Pusat					
Tarikh :			Tarikh :		

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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	75 dari 78

Lampiran 5

Borang Pelaporan Insiden Keselamatan

SULIT



**Borang IRH 1.0 - Maklumat Pengendalian
Insiden Keselamatan ICT**

**Tarikh dan Masa :
Pengendalian**

<i>Government Computer Emergency Response Team (GCERT)</i>	
*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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	76 dari 78

SULIT

1. Internal 2. External
Sistem Pengoperasian 1. Jenis 2. Versi 3. Service pack
Kapasiti Disk
Jenis <i>Hard Disk</i>
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 Pemuatnahan 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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	77 dari 78

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

RUJUKAN	REVISI	TARIKH	M/SURAT
DKICT DOFM	Versi 1.0	09/11/2009	78 dari 78