DASAR KESELAMATAN ICT
JABATAN PEMBANGUNAN PERINDUSTRIAN DAN PENYELIDIKAN
(DKICT DIDR) 2012

Versi 1.0

Disediakan oleh :

KSIT DIDR

Tarikh Kemaskini Terakhir : 1HB Julai 2012

ISI KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT (DKICT) Jabatan Pembangunan Perindustrian Dan Penyelidikan (DIDR) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT Kerajaan Negeri.

OBJEKTIF

Dasar Keselamatan ICT DIDR diwujudkan untuk mencapai tahap keselamatan ICT yang menyeluruh demi menjamin kesinambungan urusan Kerajaan Negeri dengan melindungi kepentingan strategik Negeri dan aset-asetnya serta meminimumkan kesan insiden keselamatan ICT.

Objektif utama Dasar Keselamatan ICT DIDR ialah seperti berikut :

(a) Menghebahkan pendirian pihak pengurusan untuk mendukung pelaksanaan keselamatan ICT.

(b) Menyediakan Dasar Keselamatan ICT yang komprehensif, selamat, berkesan, stabil dan boleh dipercayai (reliable).

(c) Menjamin kesinambungan operasi Kerajaan Negeri dan meminimumkan kerosakan atau kemusnahan.

(d) Mencegah salah guna atau kecurian aset ICT Kerajaan.

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

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 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 DIDR 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 di biarkan di akses tanpa kebenaran;
(b)	**Integriti**	Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan;
(c)	**Tidak Boleh disangkal**	Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
(d)	**Kesahihan**	Data dan maklumat hendaklah dijamin kesahihannya; dan
(e)	**Ketersediaan**	Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

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

Aset ICT DIDR terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT DIDR menetapkan keperluan-keperluan asas berikut :

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

(ii) 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.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT DIDR ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini adalah dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut :

(a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan Jabatan/Agensi Negeri. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) Perisian

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

(c) Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contohnya :

1. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
2. Sistem halangan akses seperti sistem kad akses; dan
3. Perkhidmatan sokongan seperti kemudahan elektrik. Penghawa dingin, sistem pencegah kebakaran dan lain-lain.

(d) Data dan Maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif Jabatan. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod Jabatan, 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 Jabatan bagi mencapai misi dan objektif Jabatan. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

(f) Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a)-(e) di atas.

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

PRINSIP- PRINSIP KESELAMATAN ICT

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

(a) Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifikasi 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 untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen "**Arahan Keselamatan Kerajaan**" iaitu **Rahsia Besar, Rahsia, Sulit dan Terhad.**

Penggunaan encryption, tandatangan digital atau sebarang mekanisma lain yang boleh melindungi maklumat mestilah juga dipertimbangkan. Dasar klasifikasi ke atas sistem aplikasi juga hendaklah mengikut klasifikasi maklumat yang sama.

(b) Hak akses minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu data atau maklumat elektronik. 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 sensitivity 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 merangkumi perkara berikut :

i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

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

iii) Menentukan maklumat sedia untuk digunakan;

iv) Menjaga kerahsiaan kata laluan;

v) Mematuhi piawaian, 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.

(d) Pengasingan Fungsi

Tugas mewujud, memadam, kemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan fungsi perlu diadakan di antara pentadbir dan pengguna. Pengasingan fungsi juga hendaklah dilakukan di antara pentadbir sistem dan pentadbir rangkaian.

(e) Pengauditan Keselamatan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Pentadbir Sistem perlu memastikan semua log/audit trail yang dijanakan oleh aset ICT berkaitan keselamatan disimpan sekurang-kurangnya setahun (1). Rekod audit hendaklah dilindungi dan tersedia untuk penilaian apabila diperlukan. Penggunaan perisian tambahan perlu dipertimbangkan bagi menentukan ketepatan dan kesahikan log/audit trail.

Dengan itu, aset ICT seperti komputer, pelayan, router, firewall dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau audit trail.

1 MAMPU, Arahan Teknologi Maklumat : Jabatan Perdana Menteri, 2007.

(f) Pematuhan

Dasar Keselamatan ICT DIDR hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT. Pelaksanaan program pengawasan dan pematuhan keselamatan maklumat secara berterusan hendaklah dilaksanakan oleh setiap perkhidmatan di kawasan tanggungjawab masing-masing. JPKN berperanan melaksanakan pengawasan dan pemantauan menyeluruh terhadap keselamatan maklumat pada aset-aset ICT di Jabatan berkaitan.

(g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui tindakan berikut :-

i) Pelan Pemulihan Bencana (DRP) Sistem ICT hendaklah diuji sekurang-kurangnya sekali setahun. Ketua Jabatan / Agensi dikehendaki menentukan perkara ini dilaksanakan;

ii) Pentadbir sistem dikehendaki melaksanakan sokongan (backup) setiap hari bagi sistem ICT; dan

iii) Semua pengguna dikehendaki mencegah kemasukan virus, mengamalkan langkah-langkah pencegahan kebakaran dan amalan ‘clear desk’ mengikut arahan semasa Jabatan.

(h) Integriti

Data dan maklumat hendaklah tepat, lengkap dan sentiasa terkini. Sebarang perubahan terhadap data hendaklah dilaksanakan oleh staf yang diberi kebenaran sahaja.

(i) Perimeter Keselamatan Fizikal

Perimeter merujuk kepada keadaan persekitaran fizikal di mana aset-aset ICT dilindungi. Perimeter tersebut hendaklah dijaga dengan rapi bagi mengelakkan sebarang pencerobohan.

(j) Saling Bergantungan

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan memperlbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamim keselamatan yang maksimum.

PERKARA 01 : PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101 Dasar Keselamatan ICT

Objektif :

Menerangkan halatuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Jabatan dan perundangan yang berkaitan.

Kenyataan		Tanggungjawab
010101	Penyebaran Dasar	
	Dasar ini perlu disebarkan kepada semua pengguna Jabatan (termasuk kakitangan, pembekal, pakar runding dan lain-lain)	ICTSO
010102	Penyelenggara Dasar	
	Dasar Keselamatan ICT DIDR ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan social. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar ICT DIDR : • Kenalpasti dan tentukan perubahan yang	ICTSO

	diperlukan; • Kemuka cadangan pindaan secara bertulis kepada ICTSO masing-masing untuk dibentangkan kepada JPKN selaku urus setia bagi mendapatkan persetujuan Mesyuarat Jawatankuasa Kerja Keselamatan ICT Kerajaan Negeri; • Maklumkan kepada semua pengguna perubahan yang telah dipersetujui oleh Jawatankuasa Kerja Keselamatan ICT Kerajaan Negeri; dan • Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	
010103	Pengecualian Dasar	
	Dasar Keselamatan ICT DIDR adalah terpakai kepada semua pengguna ICT DIDR dan tiada pengecualian diberikan.	Semua

PERKARA 02 : ORGANISASI KESELAMATAN

0201 Organisasi Dalaman

020101	**Ketua Pegawai Maklumat (CIO)**	
	Peranan dan tanggungjawab Ketua Pegawai Maklumat (CIO) DIDR adalah seperti berikut : a) Menentukan keperluan keselamatan ICT Jabatan; b) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT; c) Memastikan setiap pegawai dan kakitangan memahami kandungan dan menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT DIDR. d) Mengambil tindakah tatatertib ke atas anggota yang melanggar Dasar Keselamatn ICT DIDR; dan e) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT DIDR.	CIO

020102	Ketua Keselamatan ICT (ICTSO)	
	Peranan dan tanggungjawab adalah seperti berikut : a) Mengurus program-program keselamatan ICT Jabatan; b) Menguatkuasa dan memantau pelaksanaan Dasar Keselamatan ICT DIDR; c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT DIDR kepada semua pengguna; d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT DIDR; e) Menjalankan pengurusan risiko; f) Menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan Jabatan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h) Melaporkan insiden keselamatan ICT kepada SgCERT, dan memaklumkannya kepada CIO; i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; j) Mengesyorkan proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT DIDR; dan k) Menyedia, menyelaras dan melaksana program-program kesedaran dan latihan mengenai keselamatan ICT.	**ICTSO**

020103	**Pentadbir Sistem ICT**	
	Peranan dan tanggungjawab Pentadbir Sistem ICT di Jabatan adalah seperti berikut : a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; b) Mementukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT DIDR; c) Memantau aktiviti capaian harian sistem aplikasi pengguna; d) Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e) Menyimpan dan menganalisis rekod jejak audit (audit trail) f) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	Pentadbir Sistem ICT

020104	Pengguna	
	Peranan dan tanggungjawab pengguna adalah seperti berikut : a) Membaca dan memahami dan mematuhi Dasar Keselamatan ICT DIDR; b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c) Lulus tapisan keselamatan; d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT DIDR dan menjaga kerahsiaan maklumat Jabatan; e) Melaksanakan langkah-langkah perlindungan seperti berikut : i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan katalaluan; v. Mematuhi 'standard, prosedur', langkah dan garis panduan keselamatan yang ditetapkan dan dikeluarkan dari semasa ke semasa; vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; g) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan h) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT DIDR. (Lampiran 1)	Pengguna

0202 Pihak Ketiga

Objektif :

Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).

020201	**Keperluan Keselamatan Kontrak Dengan Pihak Ketiga**	
	Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Berikut adalah perkara yang perlu dipatuhi: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT DIDR; b) Mengenalpasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c) Mengenalpasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d) Akses kepada aset ICT Jabatan perlu berlandaskan kepada perjanjian kontrak; e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. Dasar Keselamatan ICT DIDR; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. f) Sistem aplikasi online yang dibangunkan secara outsource hendaklah melulusi 'vulnerability test' terhadap tahap keselamatan yang dikendalikan oleh SgCERT sebelum dilaksanakan. g) Menandatangani Surat Akuan Pematuhan bagi mematuhi Dasar Keselamatan ICT DIDR. (Lampiran 1)	

PERKARA 03 : PENGURUSAN ASET

O3O1 Akauntabiliti Aset

Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Jabatan.

030101	**Inventori Aset ICT**	
	Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut : a. Memastikan semua aset ICT dikenalpasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemaskini; b. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di Jabatan; d. Peraturan bagi pengendalian aset ICT hendaklah dikenalpasti, didokumenkan dan dilaksanakan; dan e. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pentadbir Sistem ICT dan Pegawai Aset

0302 Pengelasan dan Pengendalian Maklumat

Objektif :

Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

030201	**Pengelasan Maklumat**	
	Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut : a) Rahsia Besar; b) Rahsia; c) Sulit; atau d) Terhad. Ketua jabatan/Agensi dipertanggungjawabkan mengeluarkan Arahan Khas jika perlu untuk dilaksanakan di Bahagian masing-masing.	Semua
030202	**Pengendalian Maklumat**	
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan seperti berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f) Memberi perhatian kepada maklumat terperingkat terutama	Semua

	semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	

PERKARA 04 : KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif :

Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan Jabatan Pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua kakitangan Jabatan hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

040101	**Terma dan Syarat Perkhidmatan**	
	a) Semua kakitangan yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa. b) Semua kakitangan yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Semua
040102	**Sebelum Perkhidmatan**	
	Semua pengguna mestilah memahami tanggungjawab masing-masing ke atas keselamatan aset ICT Jabatan bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang mesti dipatuhi termasuk yang berikut : a) Menyatakan dengan lengkap dan jelas peranan kakitangan Jabatan serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan b) Menjalankan tapisan keselamatan untuk kakitangan Jabatan serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras	Semua

	dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	
040103	**Dalam Perkhidmatan**	
	Semua Pengguna hendaklah faham dan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong Dasar Keselamatan ICT DIDR dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi termasuk yang berikut : a) Memastikan kakitangan Jabatan serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Jabatan; b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT Jabatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; c) Memastikan adanya proses tindakan disiplin dan /atau undang-undang ke atas pegawai dan kakitangan Jabatan serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan yang ditetapkan dalam Dasar Keselamatan ICT DIDR; dan d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Latihan/Pembangunan Sumber Manusia Jabatan.	Semua

040104	**Bertukar Atau Tamat Perkhidmatan**	
	Memastikan semua pengguna di Jabatan diuruskan dengan teratur apabila tamat perkhidmatan atau bertukar dari Jabatan. Perkara-perkara yang perlu dipatuhi termasuk yang berikut : a) Memastikan semua aset ICT dikembalikan kepada Jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh Jabatan dan/atau terma perkhidmatan.	Semua

PERKARA 05 : KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 Keselamatan Kawasan

Objektif :

Mencegah akses yang tidak dibenarkan, sebarang bentuk pencerobohan, ancaman dan kerosakan kepada premis dan maklumat.

050101	**Kawalan Kawasan**	
	Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat Jabatan. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut : a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c) Memasang alat penggera atau kamera jika terdapat keperluan; d) Menghadkan jalan keluar masuk; e) Mengadakan kaunter kawalan; f) Menyediakan tempat atau bilik khas untk pelawat-pelawat; g) Mewujudkan perkhidmatan kawalan keselamatan; h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;	CIO dan ICTSO

	i) Merekabentuk dan melaksanakan keselamatan fizikal di dalam Pejabat Ketua pejabat, bilik dan kemudahan; j) Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir , letupan, kacau-bilau dan bencana; k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
050102	**Kawasan Masuk FIzikal**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut : a) Setiap pengguna Jabatan hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b) Semua pas keselamatan hendaklah diserahkan balik kepada Jabatan apabila pengguna berhenti atau bersara; c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan. d) Kehilangan pas mestilah dilaporkan dengan segera; dan e) Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT Jabatan.	Semua

0502 Keselamatan Peralatan

Objektif :

Melindungi peralatan ICT Jabatan dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

050201	**Peralatan ICT**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (activated) akan dikemaskini di samping melakukan imbasan ke atas media storan yang digunakan seperti hard disk, disket, thumb drive	Semua

	dan external hard disk; g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; i) Peralatan-peralatan kritikal perlu disokong oleh Uninterruptable Power Supply (UPS); j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti switches, hub, router dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai; l) Peralatan ICT yang hendak dibawa keluar dari premis Jabatan, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan; m) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan/atau Pentadbir Sistem dengan segera; n) Pengendalian peralatan ICT hendaklah mematuhi peraturan semasa yang berkuat kuasa; o) Pengguna tidak dibenarkan mengubah kedudukan	

	komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT; p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk di baik pulih; q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; s) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaanya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; t) Pengguna hendaklah memastikan semua perkakasan komputer pencetak dan pengimbas dalam keadaan 'OFF" apabila meningglkan pejabat; u) Memastikan suis kuasa elektrik (Power Switch) dimatikan bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir dan sebagainya; dan v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.	
050202	**Media Storan**	
	Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetic, optical disk, thumb drive, external hard disk dan media storan lain.	

	Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integrity dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; b) Bagi media storan yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu dengan teratur dan selamat; c) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; d) Media storan dan peralatan backup hendaklah disimpan di lokasi yang berasingan yang dikategorikan selamat. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; e) Akses dan pergerakan kepada media storan perlu direkodkan; f) Perkakasan backup hendaklah diletakkan di tempat yang terkawal; g) Mengadakan salinan atau penduaan (data backup) pada media storan kedua bagi tujuan keselamatan	Semua

	dan bagi mengelakkan kehilangan data; dan h) Pengguna adalah bertanggungjawab terhadap keselamatan maklumat dalam storan mudah alih seperti thumb drive atau external hard disk.	
050203	**Media Perisian dan Aplikasi**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan di Jabatan. b) Sistem aplikasi dalaman tidak dibenarkan di demo atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT/Ketua Jabatan; c) Lesen perisian (registration code, serials, CD-keys) perlu disimpan berasingan daripada media storan berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua
050204	**Penyelenggaraan Perkakasan**	
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh	

	pengedar; b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT/Ketua Jabatan	Pentadbir Sistem ICT dan Pegawai Aset
050205	**Peminjaman Perkakasan Untuk Kegunaan Di Luar Premis**	
	Perkakasan yang dipinjam untuk kegunaan di luar premis Jabatan adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mendapatkan kelulusan Pentadbir Sistem ICT Jabatan bagi membawa keluar peralatan atau maklumat tertakluk kepada tujuan yang dibenarkan; dan b) Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan bagi tujuan pemantauan.	Semua
050206	**Pengendalian Peralatan Luar Yang Dibawa Masuk/Keluar**	

	Bagi peralatan yang dibawa masuk/keluar pejabat, langkah-langkah keselamatan yang perlu diambil adalah seperti berikut : a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh Jabatan bagi membawa masuk/keluar peralatan dan; b) Memastikan peralatan yang dibawa masuk tidak mengancam keselamatan ICT Jabatan.	Semua
050207	**Pelupusan Perkakasan**	
	Pelupusan melibatkan semua peralatan ICT yang telah rosak usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh Jabatan dan ditempatkan di Jabatan. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur perlupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Jabatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; b) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih	Semua, pegawai Aset dan Pentadbir Sistem ICT

	dahulu sebelum pelupusan sama ada melalui *shredding*, *grinding*, *degauzing* atau pembakaran; c) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; d) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; e) Pegawai Aset hendaklah mengenalpasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; f) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai cirri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; g) Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam sistem inventori SISPHANS; h) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut : i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan komponen dalaman CPU seperti RAM, hardisk, motherboard dan sebagainya; ii. Menyimpan dan memindahkan	

	perkakasan tambahan komputer seperti AVT, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di Jabatan. iii. Memindah keluar dari Jabatan mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja perlupusan di bawah tanggungjawab Jabatan; v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket, thumb drive atau external hard disk sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; dan vi. Pelupusan peralatan ICT hendaklah dilakukan dengan mengambil kira kepentingan perlindungan alam sekitar.	

0503 Keselamatan Persekitaran

Objektif :

Melindungi aset ICT Jabatan dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

050301	**Kawalan Persekitaran**	
	Bagi mengelakkan kerosakan terhadap pejabat dan aset ICT Jabatan, semua cadangan berkaitan pejabat samada urusan perolehan, penyewaan atau pengubahsuaian hendaklah dirujuk terlebih dahulu kepada pegawai yang berkenaan. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil :- a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data /bilik server, bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya dengan teliti; b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e) Semua bahan cecair hendaklah diletakkan di	Semua

	tempat yang bersesuaian dan berjauhan dari aset ICT; f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua(2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	
050302	**Keselamatan Pusat Data / Bilik Server**	
	Kawasan yang menempatkan pusat data / bilik server hendaklah mempunyai kawalan persekitaran seperti berikut: i. Susunatur hendaklah dirancang dengan teliti dan mengambil kira ancaman yang akan dihadapi. ii. Mempunyai alat penghawa dingin yang mempunyai keupayaan mengawal kelembapan udara bagi mengelakkan kerosakan komponen elektronik pada perkakasan komputer berkenaan. Pemeriksaan hendaklah dilaksanakan setiap 6 bulan bagi menentukan keberkesanannya. iii. Menyediakan sistem pengudaraan (ventilation) yang mencukupi. iv. Penggunaan lantai bertingkat (raised floor) dalam pusat data/bilik server.	ICTSO

	v. Penggunaan CCTV boleh dilaksanakan bagi meningkatkan kawalan keselamatan. Kawasan yang menempatkan pusat data / bilik server hendaklah menentukan cirri-ciri keselamatan seperti berikut : i. Bekalan kuasa elektrik mesti dari punca yang berasingan dan berkemampuan menampung semua beban termasuk server, alat penghawa dingin, alat penggera dan lain-lain. ii. 'Centralized Uninterruptable Power Supply' (UPS) dan atau janakuasa sokongan (back-up) hendaklah disediakan dan diuji setiap 3 bulan bagi menentukan bekalan kuasa berterusan. iii. Sistem pengaliran air yang sempurna bagi mengelakkan banjir. Pemeriksaan terhadap kawasan yang berkenaan hendaklah dilaksanakan setiap 6 bulan oleh pihak yang bertauliah atau dilantik.	
050303	**Bekalan Kuasa**	
	Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;	Pengurus ICT dan ICTSO

	b) Peralatan sokongan seperti Uninterruptable Power Supply (UPS) dan penjana (generator) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	
050304	**Kabel**	
	Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut : a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Semua kabel rangkaian yang digunakan hendaklah mempunyai salutan (coating) yang tebal dan sukar untuk pecah serta dimasukkan ke dalam saluaran paip (Conduit) / *trunking* mengikut piawaian antarabangsa dan undang-undang siber Negara. c) Setiap pemasangan kabel rangkaian hendaklah dilabelkan di kedua-dua hujung antara punca dan destinasi kabel tersebut bagi memudahkan proses penjejakan (*Tracking*) apabila berlaku sesuatu insiden keselamatan ICT; dan d) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*.	Pengurus ICT/ICTSO

0504 Keselamatan Dokumen

Objektif :

Melindungi maklumat Jabatan dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.

050401	Dokumen	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan e) Menggunakan enkripsi (encryption) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Semua

PERKARA 06 : PENGURUSAN OPERASI DAN KOMUNIKASI

Objektif :

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

060101	**Pengendalian Prosedur**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua prosedur pengurusan operasi yang wujud, dikenal pasti dan digunapakai hendaklah didokumen, disimpan dan dikawal; b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c) Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	Semua
060102	**Kawalan Perubahan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT	Semua

	terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d) Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
060103	**Pengasingan Tugas dan Tanggungjawab**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b) Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau manipulasi; dan	Pengurus ICT dan ICTSO

	c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	

0602 Pengurus Penyampaian Perkhidmatan Pihak Ketiga

Objektif:

Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.

060201	**Perkhidmatan Penyampaian**	
	Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	ICTSO dan Pihak ketiga.

0603 Perancangan dan Penerimaan Sistem

Objektif :

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

060301	**Perancangan Kapasiti**	
	Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. 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.	Pentadbir sistem ICT dan ICTSO
060302	**Penerimaan Sistem**	
	Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT dan ICTSO

0604 Perisian Berbahaya

Objektif:

Melindungi integrity perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, Trojan dan sebagainya.

060401	**Perlindungan dari Perisian Berbahaya**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; b) Penggunaan perisian Antivirus adalah ditetapkan oleh kerajaan dari semasa ke semasa; c) Mengemaskini antivirus dengan pattern antivirus yang terkini. Kaedah yang telah ditetapkan ialah memastikan setiap *client* dikonfigurasikan untuk mendapatkan *pattern antivirus* yang terkini secara automatik melalui server yang ditempatkan di lokasi tertentu; d) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya dan memastikan status antivirus adalah online sepanjang masa;	Semua dan pentadbir sistem ICT

	e) Memasang dan menggunakan hanya perisian yang tulen berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa; f) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; g) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; h) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; i) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; j) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus; dan k) Kemaskini versi untuk segala perisian yang digunakan.	

0605 pengurusan Rangkaian

Objektif :

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

060501	**Kawalan Infrastruktur Rangkaian**	
	Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara- perkara yang perlu dipatuhi adalah seperti berikut: a) Pengurusan rangkaian dalaman di Jabatan adalah di bawah penyelarasan KSIT . Segala penyambungan ke atas rangkaian komputer mestilah mendapat kebenaran rasmi KSIT. b) KSIT yang ditempatkan oleh Jabatan Perkhidmatan Komputer Negeri untuk menyokong ICT di Jabatan merupakan sumber rujukan perancangan, pemasangan dan pengurusan rangkaian dalaman Jabatan. c) Jabatan hendaklah mewujudkan mekanisma untuk memastikan pematuhan terhadap segala arahan keselamatan setiap rangkaian di bawah tanggungjawabnya. d) Penggunaan *administrator tools* dan/atau *hacking tools* tidak dibenarkan dipasang pada komputer pengguna melainkan mendapat kebenaran ICTSO.	Pentadbir Sistem ICT

	e) Sebarang pengujian perkakasan dan perisian aplikasi sistem hendaklah mendapat kebenaran daripada Pentadbir Sistem ICT Jabatan. f) Kawalan capaian yang selamat hendaklah diwujudkan untuk akses komponen-komponen rangkaian komunikasi Jabatan dari semasa ke semasa. g) Semua capaian jarak jauh (remote access) tidak dibenarkan melainkan dengan menggunakan sistem autentikasi dan ciri-ciri keselamatan yang dibenarkan oleh SgCERT. h) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; i) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;	

0606 pengurusan Pertukaran Maklumat

Objektif:

Memastikan keselamatan pertukaran maklumat dan perisian antara Jabatan/agensi dan agensi luar terjamin.

60601	**Pertukaran Maklumat**	
	Perkara-perkara yang dipatuhi adalah seperti berikut: a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara Jabatan dengan agensi luar; c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari Jabatan; dan d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua
60602	**Pengurusan Mel Elektronik (E-Mel)**	
	Penggunaan e-mel di Jabatan 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	Pentadbir e-mel dan semua

	Internet dan Mel Elektronik di Agensi-agensi Kerajaan" dan mana-mana undang-undang bertulis yang berkuatkuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: a) Akaun atau alamat e-mel elektronik (e-mel) yang diperuntukkan oleh Unit Kemajuan IT Negeri (UKIT) merupakan akaun e-mel rasmi. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; b) Semua pihak bertanggungjawab sepenuhnya terhadap semua kandungan e-mel di dalam akaun sendiri; c) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; d) Sebarang penggunaan e-mel yang boleh memudaratkan nama baik Jabatan serta Kerajaan Negeri Sabah adalah dilarang sama sekali; e) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; f) Mengimbas bahan-bahan yang hendak dimuat naik atau dimuat turun supaya bebas virus	

	sebelum digunakan; g) Pengguna hendaklah mengenalpasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; h) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; i) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; j) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; k) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing; l) Kenyataan Penafian (Disclaimer) perlu diletakkan di dalam setiap e-mel rasmi kerajaan seperti : "DISCLAIMER : This email and any files transmitted with it are intended only for the use of the recipient(s) named above and may contain confidential information. You are hereby notified that the taking of any action in reliance upon, or any review, retransmission, dissemination, distribution, printing or copying of this message or any part thereof by anyone other than the recipient(s) is strictly prohibited.	

	If you have received this message in error, you should delete it immediately and advise the sender by return email. Opinions, conclusions and other information in this message that do not relate to the Sabah State Government shall be understood as neither given nor endorsed by the Sabah State Government." m) Semua pihak dilarang daripada melakukan aktiviti yang melanggar tatacara penggunaan e-mel rasmi kerajaan seperti: i. Menggunakan akaun milik orang lain, berkongsi akaun atau memberi kepada orang lain; ii. Menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah; iii. Menggunakan e-mel bagi tujuan komersial atau politik; iv. Menghantar dan memiliki bahan-bahan yang salah disisi undang-undang seperti bahan lucah, perjudian dan jenayah; v. Menghantar dan melibatkan diri dalam e-mel yang berunsur hasutan, e-mel sampah, e-mel bom, e-mel spam, fitnah, ciplak atau aktiviti-aktiviti lain yang ditegah oleh undang-undang Kerajaan Negeri dan Kerajaan	

	Malaysia; vi. Menyebarkan kod perosak seperti virus, worm, Trojan dan trap door yang boleh merosakkan sistem komputer dan maklumat pengguna lain; vii. Menghantar semula e-mel yang gagal sampai ke destinasi sebelum menyiasat punca kejadian; viii. Membenarkan pihak ketiga untuk menjawab e-mel kepada penghantar asal bagi pihaknya;	

PERKARA 07 : KAWALAN CAPAIAN

0701 Capaian Maklumat

Objektif :

Clear Desk dan Clear Screen

070101	**Mengawal capaian ke atas maklumat.**	
	Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Clear Desk dan Clear Screen bermaksud tidak meninggalkan bahan-bahan yang sensitive terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Menggunakan kemudahan password screen saver atau logout apabila meninggalkan komputer; ii. Menyimpan bahan-bahan sensitive di dalam laci atau kabinet fail yang berkunci; dan iii. Memastikan semua dokumen diambil segera dari pencetak pengimbas, mesin faksimili dan mesin fotostat.	Semua

PERKARA 08 : PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0801 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:

Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

080101	**Mekanisme Pelaporan**	
	Insiden keselamatan ICT bermaksud musibah (adverse event) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera: i. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; ii. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; iii. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; iv. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan	Semua

	v. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Prosedur pelaporan insiden keselamatan ICT berdasarkan: 1) Pekeliling AM Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan 2) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	

PERKARA 09 : PEMATUHAN

0901 Pematuhan dan Keperluan Perundangan

Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT Sektor Awam Negeri.

090101	**Pematuhan Dasar**	
	Setiap pengguna di Jabatan hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT Sektor Awam Negeri dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di Jabatan termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT Jabatan selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber jabatan.	Semua
090102	**Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal**	
	ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Semua maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
090103	**Pematuhan Keperluan Audit**	
	Pematuhan kepada keperluan audit perlu bagi meminimumkan	

	ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua
090104	**Keperluan Perundangan**	
	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di Jabatan: i. Arahan Keselamatan; ii. Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan; iii. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMISA) 2002; iv. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); v. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan; vi. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; vii. Surat Arahan Ketua Pengarah MAMPU – langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi	semua

	Kerajaan yang bertarikh 1 Jun 2007; viii. Surat Arahan Ketua Pengarah MAMPU - langkah-langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007; ix. Surat Pekeliling Am Bil. 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa dibawa Jawatankuasa IT dan Internet Kerajaan (JITIK); x. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender; xi. Surat Pekeliling Perbendaharaan Bil. 3/1995 – Peraturan Perolehan Perkhidmatan Perundingan; xii. Akta Tandatangan Digital 1997; xiii. Akta Rahsia Rasmi 1972; xiv. Akta Jenayah Komputer 1997; xv. Akta Hak Cipta (Pindaan) Tahun 1997; xvi. Akta Komunikasi dan Multimedia 1998; xvii. Peraturan-peraturan Pegawai Awam Negeri Sabah 2008; xviii. Arahan Perbendaharaan; xix. Arahan Teknologi Maklumat 2007; dan xx. Polisi Keselamatan ICT Kerajaan Negeri Sabah 2004.	
090105	**Pelanggaran Dasar**	
	Pelanggaran Dasar Keselamatan ICT DIDR boleh dikenakan tindakan tatatertib.	Semua

Glosari

Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetic, optical disk, flash disk, CDROM, thumb drive untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	Chief Information Officer Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of Service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
GCERT	Government Computer Emergency Response Team atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalan.
Hard disk	Cakera Keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.

ICT	Information and Communication Technology (Teknologi Maklumat dan Komunikasi)
ICTSO	ICT Security Officer Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian tersebut agar sentiasa berasingan.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan Komputer
LAN	Local Area Network Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	Log-out komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, Trojan horse, worm, spyware dan sebagainya.
MODEM	Modulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian internet

	dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti spreadsheet dan word processing ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense Multiple Access / Collision Detection (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Pentadbir Sistem ICT	Pegawai Kumpulan Sokongan IT(KSIT) / ICT yang ditempatkan di jabatan.
Pegawai Aset	Pegawai yang mengurus aset jabatan.
Pengurus ICT	Ketua Pegawai Maklumat (CIO) yang bertanggungjawab terhadap ICT di jabatan.
Pihak Ketiga	Pihak yang dipilih / dihubungi bagi menjalankan sesuatu tugasan seperti *vendor* atau pembekal.
Pentadbir e-mel	Pihak yang mentadbir e-mal Kerajaan Negeri Sabah iaitu Pihak Sabahnet.

Lampiran 1

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT JABATAN PEMBANGUNAN PERINDUSTRIAN DAN PENYELIDIKAN

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Bahagian : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....

(Nama Pegawai Keselamatan ICT)

b.p Ketua Jabatan/Agensi

Tarikh : .....