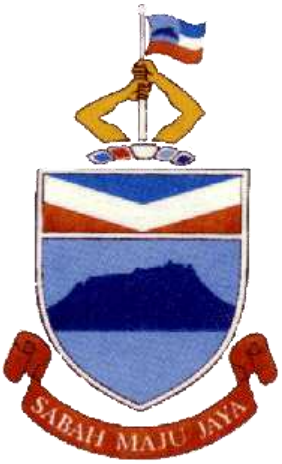
KERAJAAN NEGERI SABAH



DASAR KESELAMATAN ICT SEKTOR AWAM NEGERI SABAH

ISI KANDUNGAN

PERKARA	MUKA SURAT
PRAKATA – SETIAUSAHA KERAJAAN NEGERI	9
SEKAPUR SIRIH – KETUA PEGAWAI MAKLUMAT (CIO) NEGERI	10
SEULAS PINANG – PEGAWAI KESELAMATAN ICT (ICTSO) NEGERI	11
PENGENALAN	12
OBJEKTIF	12
PERNYATAAN DASAR	13
SKOP	15
PRINSIP-PRINSIP KESELAMATAN ICT	17
PERKARA 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR	21
0101 Dasar Keselamatan ICT	21
010101 Pelaksanaan Dasar	21
010102 Penyebaran Dasar	21
010103 Penyelenggaraan Dasar	21
010104 Pengecualian Dasar	22
PERKARA 02 ORGANISASI KESELAMATAN	23
0201 Organisasi Dalaman	23
020101 Setiausaha Kerajaan Negeri	23
020102 Ketua Pegawai Maklumat Negeri (CIO Negeri)	23
020103 Pegawai Keselamatan ICT Negeri (ICTSO Negeri)	24
020104 Ketua Pegawai Maklumat (CIO)	25
020105 Pegawai Keselamatan ICT (ICTSO)	25
020106 Pengurus ICT	27
020107 Pentadbir Sistem ICT	27
020108 Pengguna	28
020109 Jawatankuasa Kerja Keselamatan ICT Kerajaan Negeri	29
020110 Sabah Government Computer Emergency Response Team (SgCERT)	32
0202 Pihak Ketiga	36
020201 Keperluan Keselamatan Kontrak Dengan Pihak Ketiga	36

PERKARA 03 PENGURUSAN ASET	38
0301 Akauntabiliti Aset	38
030101 Inventori Aset ICT	38
0302 Pengelasan dan Pengendalian Maklumat	39
030201 Pengelasan Maklumat	39
030202 Pengendalian Maklumat	39
PERKARA 04 KESELAMATAN SUMBER MANUSIA	41
0401 Keselamatan Sumber Manusia Dalam Tugas Harian	41
040101 Terma Dan Syarat Perkhidmatan	41
040102 Sebelum Perkhidmatan	41
040103 Dalam Perkhidmatan	42
040104 Bertukar Atau Tamat Perkhidmatan	43
PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN	44
0501 Keselamatan Kawasan	44
050101 Kawalan Kawasan	44
050102 Kawalan Masuk Fizikal	45
050103 Kawasan Larangan	46
0502 Keselamatan Peralatan	47
050201 Peralatan ICT	47
050202 Media Storan	50
050203 Media Perisian dan Aplikasi	52
050204 Penyelenggaraan Perkakasan	52
050205 Peminjaman Perkakasan Untuk Kegunaan Di Luar Premis	53
050206 Pengendalian Peralatan Luar Yang Dibawa Masuk/Keluar	54
050207 Pelupusan Perkakasan	54
0503 Keselamatan Persekitaran	56
050301 Kawalan Persekitaran	56
050302 Keselamatan Pusat Data/Bilik Server	58
050303 Bekalan Kuasa	59
050304 Kabel	60
050305 Prosedur Kecemasan	60
0504 Keselamatan Dokumen	61
050401 Dokumen	61
PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI	63

0601 Pengurusan Prosedur Operasi	63
060101 Pengendalian Prosedur	63
060102 Kawalan Perubahan	63
060103 Pengasingan Tugas dan Tanggungjawab	64
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	65
060201 Perkhidmatan Penyampaian	65
0603 Perancangan dan Penerimaan Sistem	66
060301 Perancangan Kapasiti	66
060302 Penerimaan Sistem	66
0604 Perisian Berbahaya	66
060401 Perlindungan Dari Perisian Berbahaya	66
060402 Perlindungan dari *Mobile Code*	68
0605 *Housekeeping*	68
060501 *Backup*	68
0606 Pengurusan Rangkaian	71
060601 Kawalan Infrastruktur Rangkaian	71
0607 Pengurusan Media	73
060701 Penghantaran dan Pemindahan	73
060702 Prosedur Pengendalian Media	73
060703 Keselamatan Sistem Dokumentasi	74
0608 Pengurusan Pertukaran Maklumat	75
060801 Pertukaran Maklumat	75
060802 Pengurusan Mel Elektronik (*E-mel*)	75
0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)	79
060901 E-Dagang	79
060902 Maklumat Umum	80
0610 Pemantauan	81
061001 Pengauditan dan Forensik ICT	81
061002 Jejak Audit	82
061003 Sistem Log	84
061004 Pemantauan Log	84
PERKARA 07 KAWALAN CAPAIAN	85
0701 Dasar Kawalan Capaian	85
070101 Keperluan Kawalan Capaian	85
0702 Pengurusan Capaian Pengguna	86
070201 Akaun Pengguna	86

070202 Hak Capaian	87
070203 Pengurusan Kata Laluan	87
070204 *Clear Desk* dan *Clear Screen*	89
0703 Kawalan Capaian Rangkaian	90
070301 Capaian Rangkaian	90
070302 Capaian Internet	90
0704 Kawalan Capaian Sistem Pengoperasian	92
070401 Capaian Sistem Pengoperasian	92
0705 Kawalan Capaian Aplikasi Dan Maklumat	94
070501 Capaian Aplikasi dan Maklumat	94
0706 Peralatan Mudah Alih	95
070601 Peralatan Mudah Alih	95
070602 Kerja Jarak Jauh	95
PERKARA 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	96
0801 Keselamatan Dalam Membangunkan Sistem Dan Aplikasi	96
080101 Keperluan Keselamatan Sistem Maklumat	96
080102 Pengesahan Data *Input* dan *Output*	97
0802 Kawalan Kriptografi	98
080201 Enkripsi	98
080202 Tandatangan Digital	98
080203 Pengurusan Infrastruktur Kunci Awam (PKI)	98
0803 Keselamatan Fail Sistem	98
080301 Kawalan Fail Sistem	98
0804 Keselamatan Dalam Proses Pembangunan Dan Sokongan	99
080401 Prosedur Kawalan Perubahan	99
080402 Pembangunan Perisian Secara *Outsource*	100
0805 Kawalan Teknikal Keterdedahan (*Vulnerability*)	100
080501 Kawalan Dari Ancaman Teknikal	100
PERKARA 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN	102
0901 Mekanisme Pelaporan Insiden Keselamatan ICT	102
090101 Mekanisme Pelaporan	102
0902 Pengurusan Maklumat Insiden Keselamatan ICT	103
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	103

PERKARA 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	105
1001 Dasar Kesinambungan Perkhidmatan	105
100101 Pelan Kesinambungan Perkhidmatan	105
PERKARA 11 PEMATUHAN	108
1101 Pematuhan dan Keperluan Perundangan	108
110101 Pematuhan Dasar	108
110102 Pematuhan Dengan Dasar, Piawaian Dan Keperluan Teknikal	108
110103 Pematuhan Keperluan Audit	109
110104 Keperluan Perundangan	109
110105 Pelanggaran Dasar	111
GLOSARI	112
Lampiran 1	116
Lampiran 2	117

PRAKATA
SETIAUSAHA KERAJAAN NEGERI

Saya mengucapkan tahniah kepada Jabatan Perkhidmatan Komputer Negeri atas usaha dan inisiatif menggubal Dasar Keselamatan ICT Sektor Awam Negeri (DKICT). Pengwujudan dasar ini membuktikan komitmen kerajaan ke atas perlindungan keselamatan aset-aset ICT dan kualiti sistem penyampaian perkhidmatan berasaskan ICT.

Kerajaan menyedari bahawa aplikasi teknologi maklumat dan komunikasi (ICT) perlu digunakan secara meluas di sektor perkhidmatan awam sebagai mekanisme penting dalam meningkatkan kualiti sistem penyampaian perkhidmatan awam. Walau bagaimanapun, pada masa sama aspek keselamatan perlu diberi perhatian serius kerana sistem ini juga terbuka kepada kemudahterancaman (*vulnerability*). Sistem rangkaian komputer sering menjadi sasaran agen berbahaya (*malicious agent*) yang membawa ancaman keselamatan, mewujudkan gangguan dan kerosakan kepada sistem penyampaian perkhidmatan Kerajaan yang berasaskan ICT.

Dokumen ini perlu dijadikan sumber rujukan dan panduan kepada semua agensi dan penjawat awam selaku pengguna peralatan ICT. Kefahaman ke atas dasar ini adalah perlu bagi mengelakkan sebarang bentuk pelanggaran dan ketidakpatuhan yang boleh membawa kepada ancaman keselamatan ICT Sektor Awam Negeri dan seterusnya menjejaskan sistem penyampaian perkhidmatan kerajaan.

Sekian dan terima kasih.

SUKARTI BIN WAKIMAN

SEKAPUR SIRIH
KETUA PEGAWAI MAKLUMAT (CIO) NEGERI

Pertamanya saya ingin merakamkan sekalung tahniah kepada Jabatan Perkhidmatan Komputer Negeri yang telah berjaya menyediakan dan menerbitkan Dasar Keselamatan ICT Sektor Awam Negeri (DKICT) untuk kegunaan dan rujukan semua peringkat pengguna ICT Kerajaan Negeri Sabah.

Sepertimana yang sedia maklum bahawa salah satu peranan penting Ketua Pegawai Maklumat (CIO) ialah untuk memimpin dan melibatkan agensi dalam usaha-usaha Kerajaan Negeri untuk membangun dan melaksanakan projek ICT sektor awam Negeri yang dapat membawa perubahan dalam pengurusan dan pentadbiran Perkhidmatan awam. Namun, aspek keselamatan terhadap aset-aset ICT perlu diberi penekanan yang cukup oleh setiap agensi Kerajaan Negeri demi menjamin keselamatan aset-aset ICT sepanjang masa supaya sistem penyampaian perkhidmatan awam berjalan secara berterusan tanpa sebarang gangguan.

Memandangkan kejadian pencerobohan, penggodaman, penyalahgunaan, pengubahsuaian dan pendedahan maklumat tanpa izin serta serangan virus ke atas kemudahan ICT Kerajaan Negeri yang kian meningkat, maka saya menyeru agar semua Ketua Pegawai Maklumat (CIO) agensi Kerajaan Negeri dapat memimpin dan membimbing pengguna peralatan ICT di agensi masing-masing dalam melaksanakan dan mematuhi langkah-langkah kawalan yang termaktub di dalam DKICT ini bagi menghadapi sebarang ancaman daripada penjenayah siber.

Sekian dan terima kasih.

DATUK POUNIS @JOSEPH BIN YUNTAVID
Timbalan Setiausaha Kerajaan Negeri (Pembangunan)
merangkap Ketua Pegawai Maklumat (CIO) Negeri

SEULAS PINANG
PEGAWAI KESELAMATAN ICT (ICTSO) NEGERI

Dengan kesempatan ini, saya ingin mengucapkan tahniah dan syabas kepada Bahagian Keselamatan, Jabatan Perkhidmatan Komputer Negeri di atas usaha dan komitmen yang dicurahkan dalam penyediaan dan penerbitan Dasar Keselamatan ICT Sektor Awam Negeri (DKICT) ini. Sesungguhnya DKICT ini merupakan satu dasar keselamatan ICT yang mantap yang disediakan berdasarkan kepada keperluan Sistem Pengurusan keselamatan Maklumat (ISMS) ISO 27001.

Sepertimana yang sedia maklum bahawa Jabatan Perkhidmatan Komputer Negeri merupakan Jabatan yang telah dipertanggungjawabkan untuk melindungi aset-aset ICT Kerajaan Negeri.Namun, tanggungjawab ini bukanlah hanya perlu ditanggung oleh jabatan ini sahaja, tetapi ianya memerlukan tindakan proaktif dan kerjasama padu antara semua agensi kerajaan Negeri dalam mematuhi peraturan-peraturan yang terkandung di dalam DKICT ini.

Sesungguhnya keselamatan ICT bukanlah satu produk tetapi ia merupakan satu proses. Justeru, DKICT ini bukanlah sesuatu dokumen yang statik tetapi ianya adalah dinamik dan tertakluk kepada pengubahsuaian serta penambahbaikan mengikut perubahan landskap keselamatan ICT semasa.Ianya adalah bertujuan untuk memantapkan lagi keberkesanannya dalam 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.

Adalah diharapkan agar semua Pegawai Keselamatan ICT (ICTSO) agensi Kerajaan Negeri memainkan peranan sebagai penggerak kepada pembudayaan dan pematuhan DKICT ini.

Sekian dan terima kasih.

DR HAJI MINGU HAJI JUMAAN
Pengarah Jabatan Perkhidmatan Komputer Negeri
merangkap Pegawai Keselamatan ICT (ICTSO) Negeri

PENGENALAN

Dasar Keselamatan ICT (DKICT) Sektor Awam Negeri Sabah 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 Sektor Awam Negeri 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 keselamatan ICT Sektor Awam Negeri 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 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;

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

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

SKOP

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

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

(a) 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

(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.

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

(a) **Perkakasan**
Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan 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/Agensi;

(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 Jabatan/Agensi. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod Jabatan/Agensi, 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/Agensi bagi mencapai misi dan objektif Jabatan/Agensi. 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 Sektor Awam Negeri 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 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 sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesahkan 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 mengenalpasti insiden berkaitan keselamatan atau mengenalpasti 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 kesahihan *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 Sektor Awam Negeri hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT. Pelaksanaan program pengawasan dan pemantauan keselamatan maklumat secara berterusan hendaklah dilaksanakan oleh setiap perkhidmatan di kawasan tanggungjawab masing-masing. Jabatan Perkhidmatan Komputer Negeri berperanan melaksanakan pengawasan dan pemantauan menyeluruh terhadap keselamatan maklumat pada aset-aset ICT di Jabatan Negeri/ Agensi 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 / Agensi masing-masing.

(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 mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

PERKARA 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR		
0101 Dasar Keselamatan ICT		
Objektif: Menerangkan halatuju dan sokongan pengurusan tehadap keselamatan maklumat selaras dengan keperluan Jabatan / Agensi Sektor Awam Negeri dan perundangan yang berkaitan.		
KENYATAAN		**TANGGUNGJAWAB**
010101	**Pelaksanaan Dasar**	
	Pelaksanaan dasar ini adalah tanggungjawab Setiausaha Kerajaan Negeri dan dibantu oleh :- i. Jawatankuasa Kerja Keselamatan ICT Kerajaan Negeri yang dipengerusikan oleh Ketua Pegawai Maklumat Negeri (CIO Negeri); ii. Sabah Government Computer Emergency Response Team (SgCERT) yang dipengerusikan oleh Ketua Pegawai Keselamatan ICT Negeri (ICTSO Negeri); iii. Jabatan Perkhidmatan Komputer Negeri (JPKN); iv. Semua Ketua Pegawai Maklumat (CIO) Jabatan/Agensi; v. Semua Ketua Pegawai Keselamatan (ICTSO) Jabatan/Agensi; vi. Semua Ketua Jabatan/Agensi; dan vii. Semua Pengurus ICT Jabatan/Agensi.	Setiausaha Kerajaan Negeri
010102	**Penyebaran Dasar**	
	Dasar ini perlu disebarkan kepada semua pengguna Jabatan/Agensi Sektor Awam Negeri (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	ICTSO
010103	**Penyelenggaraan Dasar**	
	Dasar Keselamatan ICT Sektor Awam Negeri ini adalah tertakluk kepada semakan dan pindaan dari semasa ke	ICTSO

	semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT Sektor Awam Negeri: (a) Kenalpasti dan tentukan perubahan yang diperlukan; (b) Kemukakan 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; (c) Maklumkan kepada semua pengguna perubahan yang telah dipersetujui oleh Jawatankuasa Kerja Keselamatan ICT Kerajaan Negeri; dan (d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	
010104	**Pengecualian Dasar**	
	Dasar Keselamatan ICT Sektor Awam Negeri adalah terpakai kepada semua pengguna ICT Jabatan/Agensi Sektor Awam Negeri dan tiada pengecualian diberikan.	Semua

PERKARA 02 ORGANISASI KESELAMATAN		
0201 Organisasi Dalaman		
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT Sektor Awam Negeri.		
	KENYATAAN	**TANGGUNGJAWAB**
020101	**Setiausaha Kerajaan Negeri**	
	Peranan dan tanggungjawab adalah seperti berikut:- (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT Sektor Awam Negeri; (b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT Sektor Awam Negeri; (c) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT Sektor Awam Negeri.	Setiausaha Kerajaan Negeri
020102	**Ketua Pegawai Maklumat Negeri (CIO Negeri)**	
	Ketua Pegawai Maklumat Negeri (CIO Negeri) ialah Timbalan Setiausaha Kerajaan Negeri (Pembangunan). Peranan dan tanggungjawab adalah seperti berikut:- (a) Membantu Setiausaha Kerajaan Negeri dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (b) Memberi kepimpinan dan halatuju kepada	CIO Negeri

	CIO Jabatan/Agensi Sektor Awam Negeri dalam mengurus hal-hal berkaitan keselamatan ICT Jabatan/Agensi Sektor Awam Negeri; (c) Menasihati Setiausaha Kerajaan Negeri tentang penyediaan segala kemudahan berkaitan pembangunan dan pengembangan keselamatan ICT Sektor Awam Negeri yang diperlukan; dan (d) Bertanggungjawab ke atas fungsi-fungsi Jawatankuasa Keselamatan ICT Kerajaan Negeri secara keseluruhan.	
020103	**Pegawai Keselamatan ICT Negeri (ICTSO Negeri)**	
	Pegawai Keselamatan ICT Negeri (ICTSO Negeri) ialah Pengarah Jabatan Perkhidmatan Komputer Negeri. Peranan dan tanggungjawab adalah seperti berikut:- (a) Membantu Setiausaha Kerajaan Negeri dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (b) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT Sektor Awam Negeri secara keseluruhan; (c) Menasihati CIO Negeri perihal pembangunan, perkembangan, pelaksanaan dan pematuhan keselamatan ICT Sektor Awam Negeri; (d) Bertanggungjawab ke atas fungsi-fungsi *Sabah Government Computer Emergency Response Team* (SgCERT) secara keseluruhan; (e) Bertindak sebagai penasihat dalam penyediaan rancangan keselamatan ICT Sektor Awam Negeri; dan	ICTSO Negeri

	(f) Memastikan perhubungan yang rapat di antara Kerajaan Negeri, Persekutuan dan badan-badan yang berkaitan keselamatan ICT dalam usahasama melindungi aset ICT Kerajaan.	
020104	**Ketua Pegawai Maklumat (CIO)**	
	Peranan dan tanggungjawab Ketua Pegawai Maklumat (CIO) di semua Jabatan/ Agensi Negeri adalah seperti berikut:- (a) Menentukan keperluan keselamatan ICT Jabatan/Agensi; (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 Sektor Awam Negeri; (d) Mengambil tindakan tatatertib ke atas anggota yang melanggar Dasar Keselamatan ICT Sektor Awam Negeri; dan (e) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT Jabatan/Agensi.	CIO
020105	**Pegawai Keselamatan ICT (ICTSO)**	
	Peranan dan tanggungjawab Pegawai Keselamatan ICT (ICTSO) di semua Jabatan/Agensi Sektor Awam Negeri adalah seperti berikut:- (a) Mengurus program-program keselamatan ICT Jabatan/Agensi;	ICTSO

	(b)	Menguatkuasa dan memantau pelaksanaan Dasar Keselamatan ICTSektor Awam Negeri;	
	(c)	Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT Sektor Awam Negeri kepada semua pengguna;	
	(d)	Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT Sektor Awam Negeri;	
	(e)	Menjalankan pengurusan risiko;	
	(f)	Menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan Jabatan/Agensi 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 Sektor Awam Negeri; dan	

	(k) Menyedia, menyelaras dan melaksana program-program kesedaran dan latihan mengenai keselamatan ICT.	
020106	**Pengurus ICT**	
	Peranan dan tanggungjawab Pengurus ICT di semua Jabatan/Agensi Sektor Awam Negeri adalah seperti berikut:- (a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Jabatan/Agensi; (b) Menentukan kawalan akses pengguna terhadap aset ICT Jabatan/Agensi; (c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan (d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Jabatan/Agensi.	Pengurus ICT
020107	**Pentadbir Sistem ICT**	
	Peranan dan tanggungjawab Pentadbir Sistem ICT di semua Jabatan/Agensi Sektor Awam Negeri 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) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang	Pentadbir Sistem ICT

	telah ditetapkan di dalam Dasar Keselamatan ICT Sektor Awam Negeri; (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.	
020108	**Pengguna**	
	Peranan dan tanggungjawab pengguna adalah seperti berikut:- (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT Sektor Awam Negeri; (b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (c) Lulus tapisan keselamatan; (d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT Sektor Awam Negeri dan menjaga kerahsiaan	Pengguna

	maklumat Jabatan/Agensi Sektor Awam Negeri; (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 Sektor Awam Negeri. **(Lampiran 1)**	
020109	**Jawatankuasa Kerja Keselamatan ICT Kerajaan Negeri**	
	Jawatankuasa Kerja Keselamatan ICT Kerajaan Negeri adalah jawatankuasa yang bertanggungjawab dalam	

	keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT Sektor Awam Negeri. Keanggotaan Jawatankuasa Kerja Keselamatan ICT Kerajaan Negeri adalah seperti berikut:- **Pengerusi :** Timbalan Setiausaha Kerajaan Negeri (Pembangunan) selaku Ketua Pegawai Maklumat Negeri (*State CIO*) **Ahli :** (1) Pengarah Jabatan Perkhidmatan Komputer Negeri selaku Pegawai Keselamatan ICT Negeri (*State CIO*) dan Ketua Urus Setia; (2) Setiausaha Tetap Kementerian Kewangan; (3) Setiusaha Tetap Kementerian Pembangunan Sumber dan Kemajuan Teknologi Maklumat; (4) Pengarah Jabatan Perkhidmatan Awam Negeri; (5) Pegawai Keselamatan Kerajaan Malaysia, JPM Cawangan Sabah. (6) Setiausaha Hal Ehwal Dalam Negeri dan Penyelidikan; dan (7) Ketua Pegawai Eksekutif KKIPC Sdn. Bhd. **Urus Setia** bagi Jawatankuasa Kerja Keselamatan ICT Kerajaan Negeri ialah Bahagian Keselamatan, Jabatan Perkhidmatan Komputer Negeri. **Terma Rujukan :-** (a) Memperakukan langkah-langkah spesifik kepada *Sabah IT Council* (SITC) dalam menangani isu-isu keselamatan ICT; (b) Menyediakan laporan dan mengemukakan penemuan-penemuan keselamatan ICT untuk	

	penetapan SITC. **Objektif** :- (a) Meminimumkan gangguan akibat insiden-insiden keselamatan ICT; (b) Mendidik pengguna tentang langkah-langkah keselamatan aset ICT; (c) Menyediakan mekanisma pelaporan insiden keselamatan ICT untuk membolehkan tindakan pemulihan awal diambil; dan (d) Memastikan semua pengguna mematuhi langkah-langkah dan garis panduan keselamatan ICT. **Peranan dan Tanggungjawab** :- (a) Menggubal dan mengkaji semula polisi-polisi, strategi-strategi, piawaian dan garis panduan operasi keselamatan ICT Kerajaan Negeri; (b) Menasihati Kerajaan Negeri tentang pembangunan sumber manusia untuk memastikan kejayaan dalam pelaksanaan langkah-langkah keselamatan ICT; (c) Berhubung dengan Kerajaan Persekutuan mengenai polisi dan perancangan keselamatan ICT Negara; (d) Memantau, mengkaji semula dan menyelaras pelaksanaan langkah-langkah keselamatan ICT Negeri di Jabatan/Agensi Sektor Awam Negeri;	

	(e) Menetapkan piawaian dalam pelaksanaan langkah-langkah keselamatan ICT; (f) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; (g) Memperakukan/meluluskan dokumen Dasar Keselamatan ICT Sektor Awam Negeri; (h) Memantau tahap pematuhan Dasar Keselamatan ICT Sektor Awam Negeri; (i) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam perkhidmatan awam yang mematuhi keperluan Dasar Keselamatan ICT Sektor Awam Negeri; (j) Memastikan Dasar Keselamatan ICT Sektor Awam Negeri selaras dengan dasar-dasar ICT kerajaan semasa; (k) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; (l) Membincang tindakan yang melibatkan pelanggaran Dasar Keselamatan ICT Sektor Awam Negeri; dan (m) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	
020110	***Sabah Government Computer Emergency Response Team* (SgCERT)**	
	Keanggotaan SgCERT adalah seperti berikut:- **Pengerusi :**	SgCERT

	Pengarah Jabatan Perkhidmatan Komputer Negeri selaku Pegawai Keselamatan ICT Negeri (ICTSO Negeri) **Ahli :** (1) Pasukan Tindakbalas dan Forensik (SgIRF) diketuai oleh Pegawai Teknologi Maklumat di Jabatan Perkhidmatan Komputer Negeri. (2) Pasukan Audit dan Penilaian (SgSAT) yang diketuai oleh Pegawai Teknologi Maklumat di Jabatan Perkhidmatan Komputer Negeri; (3) Pasukan Latihan, Pendidikan dan Pembudayaan (SgHRD) yang diketuai oleh Pegawai Teknologi Maklumat di Jabatan Perkhidmatan Komputer Negeri; (4) Pasukan Penyelidikan dan Pembangunan (SgRnD) yang diketuai oleh Pegawai Teknologi Maklumat di Jabatan Perkhidmatan Komputer Negeri; (5) Pasukan Pemantauan Keselamatan (SgSMT) yang diketuai oleh Pegawai Teknologi Maklumat di Jabatan Perkhidmatan Komputer Negeri; Fungsi Utama SgCERT adalah seperti berikut:- (a) Menyediakan perkhidmatan pengurusan insiden, keterdedahan (*vulnerability*) dan bukti pencerobohan keselamatan ICT untuk Sektor Awam Negeri; (b) Menyebarluas *"security alerts and warnings"* dari semasa ke semasa; (c) Menjalankan audit keselamatan aset ICT Negeri untuk memastikan pematuhan langkah-langkah dan garis panduan keselamatan ICT; (d) Mempertingkatkan tahap kesedaran ancaman	

	keselamatan ICT di kalangan penjawat sektor awam Negeri; dan (e) Mempertingkatkan usahasama dengan GCERT dalam hal-hal berkaitan keselamatan ICT. Peranan dan tanggungjawab **Pasukan Tindakbalas dan Forensik (SgIRF)** adalah seperti berikut:- (a) Menggubal dan mengkaji semula prosedur-prosedur tindakbalas insiden keselamatan ICT; (b) Merekod dan menjalankan siasatan awal insiden yang diterima; (c) Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; dan (d) Mengumpul dan menganalisa bukti-bukti forensik dan menyediakan laporan serta mencadangkan tindakan yang perlu diambil seperti:- i. Membuat laporan polis; dan/atau ii. Melakukan *'patch'* ke atas sistem. Peranan dan tanggungjawab **Pasukan Audit dan Penilaian (SgSAT)** adalah seperti berikut:- (a) Menggubal dan mengkaji semula prosedur-prosedur pengauditan dan penilaian keselamatan ICT; (b) Mengambil tindakan *'pre-emptive'* untuk mengelakkan ancaman melalui *"penetration test"* yang dilakukan secara berkala;	

	(c) Menyediakan pelan pengukuhan keselamatan ICT; (d) Mendaftar semua kemudahan dan perkhidmatan ICT; dan (e) Menjalankan penilaian dan menyediakan pelan pengukuhan keselamatan ICT bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan. Peranan dan tanggungjawab **Pasukan Latihan, Pendidikan dan Pembudayaan (SgHRD)** adalah seperti berikut:- (a) Menggubal dan mengkaji semula kurikulum latihan keselamatan ICT; (b) Merancang, melaksanakan dan mengkaji semula aktiviti-aktiviti kesedaran keselamatan ICT; dan (c) Menjalankan latihan keselamatan ICT secara berkala. Peranan dan tanggungjawab **Pasukan Penyelidikan dan Pembangunan (SgRnD)** adalah seperti berikut:- (a) Menilai dan membuat cadangan terhadap teknologi keselamatan ICT; (b) Menjalankan penyelidikan ke atas sistem/rangkaian/aplikasi keselamatan dan membuat cadangan penambahbaikan; dan (c) Melaporkan keterdedahan baru kepada vendor. Peranan dan tanggungjawab **Pasukan Pemantauan**	

	Keselamatan (SgSMT) adalah seperti berikut:- (a) Menggubal dan mengkaji semula prosedur-prosedur pemantauan keselamatan ICT; (b) Memantau dan memastikan pematuhan polisi keselamatan; (c) Menyedia dan memantau *"Security Advisory"* ; (d) Merekod dan memantau aktiviti-aktiviti yang mencurigakan; dan (e) Memantau log keselamatan harian.	
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 Sektor Awam Negeri; (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;	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT & Pihak Ketiga

	(d) Akses kepada aset ICT Jabatan/Agensi Sektor Awam Negeri 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 Sektor Awam Negeri; 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 Sektor Awam Negeri. **(Lampiran 1)**	

PERKARA 03 PENGURUSAN ASET		
0301 Akauntabiliti Aset		
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Jabatan/Agensi.		
KENYATAAN		**TANGGUNGJAWAB**
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 serta 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/Agensi; (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 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;	Semua

	(c) Menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	

PERKARA 04 KESELAMATAN SUMBER MANUSIA		
0401 Keselamatan Sumber Manusia Dalam Tugas Harian		
Objektif: Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan Jabatan/Agensi, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua kakitangan Jabatan/Agensi Sektor Awam Negeri hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.		
	KENYATAAN	**TANGGUNGJAWAB**
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/Agensi 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/Agensi serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas	Semua

	perkhidmatan; dan (b) Menjalankan tapisan keselamatan untuk kakitangan Jabatan/Agensi serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras 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 Sektor Awam Negeri dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:- (a) Memastikan kakitangan Jabatan/Agensi serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Jabatan/Agensi; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT Jabatan/Agensi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;	Semua

	(c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan Jabatan/Agensi serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan yang ditetapkan dalam Dasar Keselamatan ICT Sektor Awam Negeri; 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/Agensi masing-masing.	
040104	**Bertukar Atau Tamat Perkhidmatan**	
	Memastikan semua pengguna di Jabatan/Agensi diuruskan dengan teratur apabila tamat perkhidmatan atau bertukar dari Jabatan/Agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:- (a) Memastikan semua aset ICT dikembalikan kepada Jabatan/Agensi 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/Agensi dan/atau terma perkhidmatan.	Semua

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN		
0501 Keselamatan Kawasan		
Objektif: Mencegah akses yang tidak dibenarkan dalam bentuk sebarang pencerobohan, ancaman dan kerosakan kepada premis dan maklumat.		
KENYATAAN		**TANGGUNGJAWAB**
050101	**Kawalan Kawasan**	
	Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh, merosak dan mengganggu secara fizikal terhadap premis dan maklumat Jabatan/Agensi. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut:- (a) Kawasan keselamatan fizikal hendaklah dikenalpasti 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;	CIO dan ICTSO

	(e) Menyediakan kaunter kawalan; (f) Menyediakan tempat atau bilik khas untuk 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; (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	**Kawalan Masuk Fizikal**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut:- (a) Setiap pengguna Jabatan/Agensi hendaklah memakai atau menggunakan pas keselamatan	Semua

	sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan semula kepada Jabatan/Agensi 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/Agensi.	
050103	**Kawasan Larangan**	
	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. (a) Kawalan akses ke pusat data/ bilik *server* hendaklah ditentukan keselamatannya. Kawalan akses boleh diadakan dalam bentuk seperti berikut:- i. Biometrik. ii. Kata laluan. iii. Sistem elektronik kad pintar dan mekanikal. (b) Semua akses yang dibenarkan ke kawasan	Pentadbir Sistem ICT

	persekitaran pusat data/bilik *server* hendaklah diiringi oleh Pentadbir Sistem atau kakitangan teknikal yang dilantik bagi menentukan dan mengawalselia penugasan yang diperlukan. (c) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai. (d) Menyediakan buku log untuk tujuan merekodkan maklumat dan aktiviti yang dilaksanakan oleh Pentadbir Sistem ICT atau Pihak Ketiga. (e) Sebarang pemindahan maklumat daripada pusat data/ bilik *server* hendaklah dipohon dan mendapat kebenaran bertulis daripada pemilik data (*data owner*) dan Ketua Jabatan masing-masing.	
0502 Keselamatan Peralatan		
Objektif: Melindungi peralatan ICT Jabatan/Agensi 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;	Semua

	(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*) dan dikemaskini di samping melakukan imbasan ke atas media storan yang digunakan seperti *hard disk, diskette, thumb drive* 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/Agensi, 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	

	dibaikpulih; (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 jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (t) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan *"OFF"* apabila meninggalkan 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.	Semua

	Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Semua media storan perlu dikawal bagi mencegah daripada 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 daripada 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 pendua (*data backup*) pada media storan kedua bagi tujuan keselamatan 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/Agensi; (b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran bertulis 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 ketersediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-	Pentadbir Sistem ICT dan Pegawai Aset

	(a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh Pengurus ICT/Ketua Jabatan; (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.	
050205	**Peminjaman Perkakasan Untuk Kegunaan Di Luar Premis**	
	Perkakasan yang dipinjam untuk kegunaan di luar premis Jabatan/Agensi adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Mendapatkan kelulusan Pentadbir Sistem ICT Jabatan/Agensi bagi membawa keluar peralatan atau maklumat tertakluk untuk	

	tujuan yang dibenarkan; dan (b) Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan bagi tujuan pemantauan.	
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/Agensinya bagi membawa masuk/keluar peralatan dan; (b) Memastikan peralatan yang dibawa masuk tidak mengancam keselamatan ICT Jabatan/Agensi.	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/Agensi dan ditempatkan di Jabatan/Agensi. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan jabatan/Agensi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;	Semua, Pegawai Aset dan Pentadbir Sistem ICT

	(b)	Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran;	
	(c)	Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat salinan/pendua;	
	(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 ciri-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, *hard disk, motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan tambahan komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di Jabatan/Agensi; iii. Memindah keluar dari Jabatan/Agensi mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Jabatan/Agensi; v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket, CD, *thumb drive* atau *external hard disk* sebelum menghapuskan maklumat tersebut daripada peralatan computer 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/Agensi 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/Agensi, semua cadangan berkaitan pejabat samada urusan perolehan, penyewaan atau	Semua

	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 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:- (a) Susun atur hendaklah dirancang dengan teliti dan mengambil kira ancaman yang akan dihadapi. (b) Mempunyai alat penghawa dingin yang mempunyai keupayaan mengawal kelembapan udara bagi mengelakkan kerosakan komponen elektronik perkakasan komputer berkenaan. Pemeriksaan hendaklah dilaksanakan setiap 6 bulan bagi menentukan keberkesanannya. (c) Menyediakan sistem pengudaraan *(ventilation)* yang mencukupi. (d) Penggunaan lantai bertingkat *(raised floor)* dalam pusat data/bilik *server.* (e) Penggunaan CCTV boleh dilaksanakan bagi meningkatkan kawalan keselamatan.	ICTSO

	Kawasan yang menempatkan pusat data/bilik *server* hendaklah menentukan ciri-ciri keselamatan seperti berikut:- (a) Bekalan kuasa elektrik mesti dari punca yang berasingan dan berkemampuan menampung semua beban termasuk *server*, alat penghawa dingin, alat penggera dan lain-lain. (b) '*Centralized Uninterruptable Power Supply' (UPS)* dan/atau janakuasa sokongan *(back-up)* hendaklah disediakan dan diuji setiap 3 bulan bagi menentukan bekalan kuasa berterusan. (c) 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; (b) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal	Pengurus ICT dan ICTSO

	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 saluran 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 (*Tracing*) apabila berlaku sesuatu insiden keselamatan ICT; dan (d) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*.	Pengurus ICT dan ICTSO
050305	**Prosedur Kecemasan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-	

	(a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan Jabatan/Agensi; dan (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan/Agensi.	Semua dan Pegawai Keselamatan Jabatan
0504 Keselamatan Dokumen		
Objektif: Melindungi maklumat Jabatan/Agensi 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	Semua

	Negara; dan (e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI		
0601 Pengurusan Prosedur Operasi		
Objektif: Memastikan pengurusan operasi dan kemudahan pemprosesan berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.		
KENYATAAN		**TANGGUNGJAWAB**
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	Semua

	pemilik aset ICT 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 direkod 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	Pengurus ICT dan ICTSO

	dimanipulasi; dan (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 Pengurusan 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 integriti 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:-	Pentadbir Sistem ICT dan Semua

	(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;	
	(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.	
060402	**Perlindungan dari *Mobile Code***	
	Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
0605 *Housekeeping*		
Objektif: Melindungi integriti dan ketersediaan maklumat dan kemudahan-kemudahan pemprosesan maklumat.		
060501	***Backup***	
	Bagi memastikan kesinambungan penyampaian perkhidmatan, perkara-perkara seperti berikut hendaklah dipatuhi dan dipantau untuk memenuhi keperluan perlindungan data digital dan sistem aplikasi ICT Kerajaan Negeri yang terkandung dalam Surat Pekeliling Kementerian Kewangan Bil. 12 Tahun 2008 bertajuk *"Dasar Perolehan dan Pelaksanaan*	Pentadbir Sistem ICT dan Semua

	Sistem Aplikasi ICT, serta Penyimpanan Data dan Sistem Aplikasi ICT Ke Pusat Data Kerajaan Negeri " bertarikh 30 Disember 2008. (a) Semua sistem aplikasi ICT yang dibangunkan dan digunapakai oleh semua Kementerian/Jabatan/Pihak Berkuasa Tempatan/Badan Berkanun di bawah Kerajaan Negeri hendaklah disimpan dan ditempatkan di Pusat Data Kerajaan Negeri; (b) Sebarang sistem aplikasi ICT yang dicapai melalui sistem rangkaian Sabah.Net oleh Ibu Pejabat dan Cawangan Agensi di seluruh Negeri hendaklah disimpan dan ditempatkan di Pusat Data Kerajaan Negeri; (c) Menyimpan semua salinan data digital Jabatan/Agensi di Pusat Data Kerajaan Negeri sebagai tempat penyimpanan data secara *offsite*; (d) Menyerahkan dua (2) salinan untuk simpanan sokongan penuh data mingguan (*Weekly Full data backup*) dan sokongan penuh sistem mingguan (*Weekly Full system backup*) kepada Pusat Data Kerajaan Negeri; (e) Melaksanakan prosedur *backup* mengikut tatacara yang dinyatakan dalam Polisi Keselamatan ICT "*Backup and Restoration*" yang disediakan oleh SgCERT dan boleh dirujuk melalui **http://www.sgcert.org/policy.asp ;**	

	(f) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi setelah mendapat versi terbaru; (g) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; (h) Menyimpan *backup* mengikut bilangan generasi *backup* yang ditentukan oleh Jabatan/Agensi masing-masing; (i) Merekod salinan *backup* mengikut tatacara yang dinyatakan dalam Polisi Keselamatan ICT *"Backup and Restoration"* yang disediakan oleh SgCERT dan boleh dirujuk melalui **http://www.sgcert.org/policy.asp** ; (j) Menghantar media sokongan ke Ibu Pejabat Jabatan Perkhidmatan Komputer Negeri yang akan menghantar perkara tersebut ke Pusat Data Kerajaan Negeri untuk disimpan; dan (k) Mengemukakan permohonan untuk mendapatkan semula media sokongan kepada Jabatan Perkhidmatan Komputer Negeri.	

0606 Pengurusan Rangkaian		
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.		
060601	**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/Agensi adalah di bawah penyelarasan Bahagian ICT masing-masing. Segala penyambungan ke atas rangkaian komputer mestilah mendapat kebenaran rasmi Bahagian ICT masing-masing. (b) Jabatan Perkhidmatan Komputer Negeri merupakan sumber rujukan perancangan, pemasangan dan pengurusan rangkaian dalaman Jabatan/Agensi Sektor Awam Negeri. (c) Semua Jabatan/Agensi Sektor Awam Negeri 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 computer pengguna melainkan mendapat kebenaran ICTSO.	Pentadbir Sistem ICT

	(e)	Sebarang pengujian perkakasan dan perisian aplikasi sistem hendaklah mendapat kebenaran daripada Pentadbir Sistem ICT Jabatan/Agensi.	
	(f)	Kawalan capaian yang selamat hendaklah diwujudkan untuk akses kepada komponen-komponen rangkaian komunikasi.	
	(g)	Semua konfigurasi dan infrastruktur rangkaian hendaklah diklasifikasikan, didokumenkan dan sentiasa dikemaskini oleh Pentadbir Sistem ICT Jabatan/Agensi dari semasa ke semasa.	
	(h)	Semua capaian jarak jauh (*remote access*) tidak dibenarkan melainkan dengan menggunakan sistem autentikasi dan ciri-ciri keselamatan yang dibenarkan oleh SgCERT.	
	(i)	Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;	
	(j)	Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;	
	(k)	Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;	
	(l)	*Firewall* dalaman hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Sistem	

	ICT; (m) Semua trafik keluar dan masuk Sabah.Net hendaklah melalui *gateway* di bawah kawalan **Pusat Operasi Rangkaian Sabah;** (n) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; (o) Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat Jabatan/Agensi; (p) Sebarang penyambungan rangkaian dalaman (Intranet) ke rangkaian awam (Internet) yang boleh mewujudkan *backdoor access* adalah tidak dibenarkan; dan (q) Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatannya.	
0607 Pengurusan Media		
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.		
060701	**Penghantaran dan Pemindahan**	
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Semua
060702	**Prosedur Pengendalian Media**	
	Prosedur-prosedur pengendalian media perlu dipatuhi	Semua

	adalah seperti berikut:- (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Menyimpan semua media di tempat yang selamat; dan (f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	
060703	**Keselamatan Sistem Dokumentasi**	
	Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut:- (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan	Semua

	(c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	
0608 Pengurusan Pertukaran Maklumat		
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara Jabatan/Agensi dan agensi luar terjamin.		
060801	**Pertukaran Maklumat**	
	Perkara-perkara yang perlu 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/Agensi dengan agensi luar; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari Jabatan/Agensi; dan (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua
060802	**Pengurusan Mel Elektronik (E-mel)**	
	Penggunaan e-mel di Jabatan/Agensi hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling	Pentadbir e-mel dan Semua

	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. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut:- (a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh Kementerian Pembangunan Sumber & Kemajuan Teknologi Maklumat (KPSKTM) 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/Agensi 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 akaun 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-udang 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; (n) Pentadbir e-mel Jabatan/Agensi hendaklah menggunakan *Government Accounts Tracking System* (GATS) untuk mengurus hal-hal berkaitan akaun e-mel pengguna Jabatan/Agensi; dan (o) Pengguna hendaklah memaklumkan SgCERT dengan segera apabila menerima e-mel yang berunsur *spamming* seperti *phishing*, *pharming*, *laundering* dan *malware*.	
0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)		
Objektif: Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.		
060901	**E-Dagang**	
	Bagi menggalakkan pertumbuhan E-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. Perkara-perkara yang perlu dipatuhi adalah seperti	Semua

	berikut:- (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; (b) Maklumat yang terlibat dalam transaksi dalam talian (*On-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan; dan (d) Sebarang aplikasi sistem dalam talian (*On-line*) hendaklah dirujuk kepada SgCERT terlebih dahulu bagi tujuan *"Penetration Test"* sebelum dilaksanakan.	
060902	**Maklumat Umum**	
	Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut:- (a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian;	Semua

	(b) Memastikan sistem yang boleh diakses oleh orang awam telah melulusi ujian keselamatan *"Penetration Test"* dan *"Vulnerability Assessment"* serta mendapat kebenaran dari SgCERT terlebih dahulu; dan (c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuatnaik ke laman web.	
0610 Pemantauan		
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.		
061001	**Pengauditan dan Forensik ICT**	
	ICTSO mestilah bertanggungjawab merekod, menganalisis dan melapor perkara-perkara berikut:- (a) Sebarang percubaan pencerobohan terhadap sistem ICT Jabatan/Agensi kepada SgCERT; (b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phishing*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*) kepada SgCERT; (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;	ICTSO

	(e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; (g) Aktiviti penyalahgunaan akaun e-mel; dan (h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	
061002	**Jejak Audit**	
	Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut:- (a) Rekod setiap aktiviti transaksi; (b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; (d) Maklumat aktiviti sistem yang tidak normal	Pentadbir Sistem ICT

	aktiviti yang tidak mempunyai ciri-ciri keselamatan; dan (e) Jejak audit hendaklah disimpan untuk tempoh sekurang-kurangnya tujuh (7) tahun. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
061003	**Sistem Log**	
	Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:- (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.	Pentadbir Sistem ICT
061004	**Pemantauan Log**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Log audit yang merekodkan semua aktiviti	Pentadbir Sistem ICT

		perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;	
	(b)	Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala;	
	(c)	Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;	
	(d)	Aktiviti pentadbiran dan operator sistem perlu direkodkan;	
	(e)	Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan ke dalam log, dianalisis dan diambil tindakan sewajarnya; dan	
	(f)	Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Jabatan/Agensi atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	

PERKARA 07 KAWALAN CAPAIAN		
0701 Dasar Kawalan Capaian		
Objektif: Mengawal capaian ke atas maklumat.		
KENYATAAN		**TANGGUNGJAWAB**
070101	**Keperluan Kawalan Capaian**	
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan (d) Kawalan ke atas kemudahan pemprosesan maklumat.	Pentadbir Sistem ICT dan ICTSO

0702 Pengurusan Capaian Pengguna		
Objektif: Mengawal capaian pengguna ke atas aset ICT Jabatan/Agensi.		
070201	**Akaun Pengguna**	
	Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenalpasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:- (a) Akaun yang diperuntukkan oleh Jabatan/Agensi sahaja 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/Agensi. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan (f) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut:-	Semua dan Pentadbir Sistem ICT

	i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	
070202	**Hak Capaian**	
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas. Perkara berikut juga perlu diberikan perhatian:- – Semua pengguna generik hendaklah mempunyai dan menggunakan *username* sendiri apabila menggunakan komputer generik dan pengguna hendaklah *logout* apabila selesai menggunakan komputer. Pengguna adalah tidak dibenarkan menggunakan *username/password* (nama pengguna/kata laluan) pengguna lain.	Pentadbir Sistem ICT
070203	**Pengurusan Kata Laluan**	
	Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh Jabatan/Agensi seperti berikut:- (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;	Semua dan Pentadbir Sistem ICT

	(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 aksara, angka dan aksara khusus (simbol);	
	(d)	Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;	
	(e)	Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;	
	(f)	Kata laluan hendaklah tidak dipaparkan semasa *input,* dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;	
	(g)	Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula;	
	(h)	Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;	
	(i)	Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan;	
	(j)	Kata laluan hendaklah ditukar selepas tiga	

	(3) bulan atau selepas tempoh masa yang bersesuaian; (k) Mengelakkan penggunaan semula kata laluan yang baru digunakan; dan (l) Penggunaan teknologi tambahan seperti kad-kad pintar dan teknologi *biometric authentication* perlu dipertimbangkan untuk sistem yang terperingkat.	
070204	***Clear Desk* dan *Clear Screen***	
	Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Menggunakan kemudahan *screen saver password* atau *logout* apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Semua

0703 Kawalan Capaian Rangkaian		
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.		
070301	**Capaian Rangkaian**	
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:- (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian Jabatan/Agensi rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Sistem ICT dan ICTSO
070302	**Capaian Internet**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Penggunaan internet di Jabatan/Agensi hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code,* virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian Jabatan/Agensi;	Pentadbir Sistem ICT, Pengurus ICT dan Semua

	(b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; (c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; (d) Penggunaan internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya; (e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan/Pegawai yang diberi kuasa; (f) Bahan yang diperolehi dari internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber internet hendaklah dinyatakan; (g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pegawai yang diberi kuasa sebelum dimuat naik ke internet; (h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;	

	(i) Sebarang bahan yang dimuat turun dari internet hendaklah digunakan untuk tujuan yang dibenarkan oleh Jabatan/Agensi; (k) Penggunaan modem untuk tujuan sambungan ke internet tidak dibenarkan sama sekali; dan (l) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:- i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	
0704 Kawalan Capaian Sistem Pengoperasian		
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.		
070401	**Capaian Sistem Pengoperasian**	
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi:- (a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan	Pentadbir Sistem ICT dan ICTSO

	(b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:- (a) Mengesahkan pengguna yang dibenarkan; (b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* dan (c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; (b) Mewujudkan satu pengenalan diri (*ID*) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Menghadkan dan mengawal penggunaan program; dan (d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	

0705 Kawalan Capaian Aplikasi dan Maklumat		
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.		
070501	**Capaian Aplikasi dan Maklumat**	
	Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi:- (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (*sistem log*); (c) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; (d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan (e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau	Pentadbir Sistem ICT dan ICTSO

	bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
0706 Peralatan Mudah Alih		
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.		
070601	**Peralatan Mudah Alih**	
	Perkara yang perlu dipatuhi adalah seperti berikut:- (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua
070602	**Kerja Jarak Jauh**	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

PERKARA 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM		
0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi		
Objektif: Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.		
	KENYATAAN	**TANGGUNGJAWAB**
080101	**Keperluan Keselamatan Sistem Maklumat**	
	Bagi memastikan kesinambungan penyampaian perkhidmatan, perkara-perkara seperti berikut hendaklah dipatuhi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Selaras dengan Surat Pekeliling Kementerian Kewangan Bil. 12 Tahun 2008 bertajuk *"Dasar Perolehan dan Pelaksanaan Sistem Aplikasi ICT, serta Penyimpanan Data dan Sistem Aplikasi ICT Ke Pusat Data Kerajaan Negeri "* bertarikh 30 Disember 2008, sebarang perolehan dan pembangunan sistem aplikasi ICT yang baru secara dalaman perlu dirujuk dan dimaklumkan kepada Jabatan Perkhidmatan Komputer Negeri untuk dimasukkan ke dalam rekod pengurusan sistem aplikasi ICT Kerajaan Negeri Sabah dan juga memastikan audit sistem dilakukan bagi menjamin aspek keselamatan data sistem dipatuhi; (b) Penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan	Pemilik Sistem, Pentadbir Sistem ICT, ICTSO dan SgCERT

	keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (c) Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem *output* untuk memastikan data yang telah diproses adalah tepat; (d) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan (e) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji melalui "*Penetration Test*" dan "*Vulnerability Assessment*" terlebih dahulu oleh SgCERT bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	
080102	**Pengesahan Data *Input* dan *Output***	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan	Pemilik Sistem dan Pentadbir Sistem ICT

	(b) Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	
0802 Kawalan Kriptografi		
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.		
080201	**Enkripsi**	
	Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
080202	**Tandatangan Digital**	
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
080203	**Pengurusan Infrastruktur Kunci Awam (*PKI*)**	
	Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua
0803 Keselamatan Fail Sistem		
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.		
080301	**Kawalan Fail Sistem**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;	Pemilik Sistem dan Pentadbir Sistem ICT

	(b) Kod atau atur cara 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; (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan (e) Mengaktifkan *audit log* bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	
0804 Keselamatan Dalam Proses Pembangunan dan Sokongan		
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.		
080401	**Prosedur Kawalan Perubahan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang	Pemilik Sistem dan Pentadbir Sistem ICT

	dilakukan oleh vendor; (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (d) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan (e) Menghalang sebarang peluang untuk membocorkan maklumat.	
080402	**Pembangunan Perisian Secara *Outsource***	
	Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem dan diuji oleh SgCERT sebelum digunakan. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik Jabatan/Agensi. Garis panduan IT *outsourcing* Jabatan/Agensi Sektor Awam yang dikeluarkan oleh pihak MAMPU perlu dirujuk.	Pentadbir Sistem ICT dan SgCERT
0805 Kawalan Teknikal Keterdedahan (*Vulnerability*)		
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.		
080501	**Kawalan dari Ancaman Teknikal**	
	Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan oleh pihak SgCERT melalui audit keselamatan yang dilakukan secara *pre-emptive* yang sistematik dan berkala untuk:-	Pentadbir Sistem ICT dan SgCERT

	(a)	Memperolehi maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;	
	(b)	Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan	
	(c)	Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	

PERKARA 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN		
0901 Mekanisme Pelaporan Insiden Keselamatan ICT		
Objektif: Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.		
KENYATAAN		**TANGGUNGJAWAB**
090101	**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 dan SgCERT dengan kadar segera:- (a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses 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,	Semua

	penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di Jabatan/Agensi sepertimana **Lampiran 2.** Prosedur pelaporan insiden keselamatan ICT berdasarkan:- (a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
0902 Pengurusan Maklumat Insiden Keselamatan ICT		
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.		
090201	**Prosedur Pengurusan Maklumat Insiden Keselamatan ICT**	
	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 yang tinggi kepada Jabatan/Agensi. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-	ICTSO

	kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:- (a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; (d) Menyediakan tindakan pemulihan segera; dan (e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	

PERKARA 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN		
1001 Dasar Kesinambungan Perkhidmatan		
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.		
KENYATAAN		**TANGGUNGJAWAB**
100101	**Pelan Kesinambungan Perkhidmatan**	
	Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan - BCP*) 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 Jawatankuasa Kerja Keselamatan ICT Kerajaan Negeri. Perkara-perkara berikut perlu diberi perhatian:- (a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; (c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;	Pengurus ICT

	(d) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (f) Membuat *backup*; dan (g) Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali. Pelan Kesinambungan Perkhidmatan (BCP) perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai personel SgCERT, JPKN dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden; (c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh;	

	(e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh; (f) Salinan *BCP* perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. *BCP* hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan; (g) Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan; (h) Ujian *BCP* hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan; dan (i) Jabatan/Agensi hendaklah memastikan salinan *BCP* sentiasa dikemaskini dan dilindungi seperti di lokasi utama.	

PERKARA 11 PEMATUHAN		
1101 Pematuhan dan Keperluan Perundangan		
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari perlanggaran kepada Dasar Keselamatan ICT Sektor Awam Negeri.		
KENYATAAN		**TANGGUNGJAWAB**
110101	**Pematuhan Dasar**	
	Setiap pengguna di Jabatan/Agensi 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/Agensi 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/Agensi selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber Jabatan/Agensi.	Semua
110102	**Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal**	
	ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO

110103	**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
110104	**Keperluan Perundangan**	
	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di Jabatan/Agensi:- (a) Arahan Keselamatan; (b) Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan; (c) *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002; (d) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); (e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;	

	(f) Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; (g) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; (h) Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006; (i) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007; (j) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007; (k) Surat Pekeliling Am Bil.2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK); (l) Surat Pekeliling Perbendaharaan Bil. 2/1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender;	

	(m) Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan; (n) Akta Tandatangan Digital 1997; (o) Akta Rahsia Rasmi 1972; (p) Akta Jenayah Komputer 1997; (q) Akta Hak Cipta (Pindaan) Tahun 1997; (r) Akta Komunikasi dan Multimedia 1998; (s) Peraturan-peraturan Pegawai Awam Negeri Sabah 2008; (t) Arahan Perbendaharaan; (u) Arahan Teknologi Maklumat 2007; dan (v) Polisi Keselamatan ICT Kerajaan Negeri Sabah 2004.	
110105	**Pelanggaran Dasar**	
	Pelanggaran Dasar Keselamatan ICT Sektor Awam Negeri boleh dikenakan tindakan tatatertib.	Semua

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, *magnetic tape*, *optical disk*, *flash disk*, CDROM, *thumb drive* dan sebagainya 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 jangkamasa 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.
Firewall	Sistem yang direkabentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi

	mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
Hub	Hab (*hub*) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau

	semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
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 *stream* 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.
PDKN	Pusat Data Kerajaan Negeri. Pusat data yang memberikan perkhidmatan penyimpanan dan perlindungan keselamatan data Kerajaan Negeri.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.

Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan Komputer
sgCERT	*Sabah Government Computer Emergency Response Team*. Organisasi yang ditubuhkan untuk menguruskan pengendalian insiden Keselamatan ICT Sektor Awam Negeri Sabah.
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 peribadi dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Aturcara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT SEKTOR AWAM NEGERI

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan/Gred : .....

Jabatan/Cawangan/ Bahagian/Unit : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT Sektor Awam Negeri.

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 : .....

Lampiran 2

PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT SEKTOR AWAM NEGERI