

Dasar Keselamatan ICT
Kerajaan Negeri Sarawak

Unit Teknologi Maklumat dan Komunikasi (ICTU)
Jabatan Ketua Menteri

27 Februari 2013

Versi 1.1

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
21 Disember 2012	1.1	JKICT Bil.1 Tahun 2012	27 Februari 2013

JADUAL PINDAAN DASAR KESELAMATAN ICT KERAJAAN NEGERI SARAWAK

TARIKH	VERSI	BUTIRAN PINDAAN
21 Disember 2012	1.1	**i. Tambahan dokumen dalam Lampiran C** (a) Surat Pekeliling ICT No.3/2012 (b) Surat Pekeliling ICT No.4/2012 (c) Surat Pekeliling ICT No.5/2012 **ii. Tambahan Lampiran baru** Lampiran E - Non Disclosure Agreement (NDA) oleh Pembekal Perkhidmatan - SAINS iii. **Perkara 061002 Sistem Log**, muka surat 49, perenggan (c) Sekiranya wujud aktiviti lain yang tidak sah seperti kecurian maklumat atau pencerobohan, Pentadbir Sistem Agensi atau Pembekal Perkhidmatan hendaklah melaporkan kepada ICTSO iv. **Perkara 090101 Mekanisme Pelaporan**, muka surat 61, Surat Pekeliling ICT 3/2009 - Penubuhan QCERT dan Pengurusan Pengendalian Insiden ICT Sektor Awam di Peringkat Negeri

ISI KANDUNGAN

PENGENALAN 7

OBJEKTIF 8

PERNYATAAN DASAR 9

SKOP 10

PRINSIP-PRINSIP 12

BIDANG 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR 14

0101 Dasar Keselamatan ICT 14

010101 Pelaksanaan Dasar 14

010102 Penyebaran Dasar 14

010103 Kajian Semula Dasar 14

010104 Aplikasi Dasar 14

BIDANG 02 ORGANISASI KESELAMATAN 15

0201 Struktur Organisasi Dalaman 15

020101 Pengarah Unit Teknologi Maklumat dan Komunikasi (ICTU) 15

020102 Ketua Pegawai Keselamatan ICT Negeri (Ketua ICTSO) 16

020103 Ketua Agensi 16

020104 Ketua Pegawai Maklumat Agensi (CIO Agensi) 17

020105 Pegawai Keselamatan ICT (ICTSO Agensi) 17

020106 Penolong Ketua Pegawai Maklumat (ACIO Agensi) 18

020107 Pembekal Perkhidmatan 18

020108 Penjawat Awam 19

020109 Jawatankuasa Keselamatan ICT Kerajaan Negeri (JKICT Kerajaan Negeri) 20

020110 Majlis Teknologi Dan Sumber Maklumat Negeri Sarawak (SITRC) 20

020111 Kumpulan Kerja Domain Keselamatan ICT Negeri (KKDKICT) 21

020112 Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (QCERT) 22

020113 Pentadbir Sistem 23

0202 Pihak Yang Berkepentingan 24

0201013 Keperluan Keselamatan Dalam Kontrak Dengan Pihak Yang Berkepentingan 24

BIDANG 03 PENGURUSAN ASET ICT 25

0301 Akauntabiliti Aset 25

030101 Inventori Aset ICT 25

0302 Pengkelasan Dan Pengendalian Maklumat 25

030201 Pengkelasan Maklumat 25
030202 Pengendalian Maklumat 26
030203 Penggunaan Aset ICT Yang Dibenarkan 26
BIDANG 04 KESELAMATAN SUMBER MANUSIA 27
0401 Keselamatan Sumber Manusia 27
040101 Sebelum Perkhidmatan 27
040102 Dalam Perkhidmatan 27
040103 Bertukar Atau Tamat Perkhidmatan 28
BIDANG 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN 29
0501 Keselamatan Kawasan 29
050101 Kawalan Kawasan 29
050102 Kawalan Masuk Fizikal 30
050103 Kawasan Terhad 30
0502 Keselamatan Perkakasan 31
050201 Perkakasan ICT 31
050202 Media Storan 32
050203 Media Tandatangan Digital 32
050204 Media Perisian Dan Applikasi 33
050205 Penyelenggaraan Perkakasan ICT 33
050206 Perkakasan Dibawa Keluar Dari Premis 34
050207 Pelupusan Dan Kitar Semula Perkakasan ICT 34
0503 Keselamatan Persekitaran 35
050301 Kawalan Persekitaran 35
050302 Bekalan Kuasa 36
050303 Kabel 36
050304 Prosedur Kecemasan 36
0504 Keselamatan Dokumen 37
050401 Dokumen 37
BIDANG 06 PENGURUSAN OPERASI DAN KOMUNIKASI 38
0601 Pengurusan Prosedur Operasi 38
060101 Pengendalian Prosedur Operasi 38
060102 Kawalan Perubahan 38
060103 Pengasingan Tugas Dan Tanggungjawab 39

0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga 39
060201 Perkhidmatan Penyampaian 39
0603 Perancangan Dan Penerimaan Sistem 40
060301 Perancangan Kapasiti 40
060302 Penerimaan Sistem 40
0604 Perisian Berbahaya 41
060401 Perlindungan Dari Perisian Berbahaya 41
060402 Perlindungan Dari Mobile Code 41
0605 Housekeeping 42
060501 Backup 42
0606 Pengurusan Rangkaian 43
060601 Kawalan Infrastruktur Rangkaian 43
0607 Pengurusan Media 44
060701 Pengurusan Media Mudah Alih 44
060702 Pelupusan Media 44
060703 Prosedur Pengendalian Maklumat 44
060704 Keselamatan Sistem Dokumentasi 44
0608 Pengurusan Pertukaran Maklumat 45
060801 Pertukaran Maklumat 45
060802 Pengurusan Mel Elektronik (E-mel) 45
0609 Perkhidmatan E-Dagang (Electronic Commerce Services) 47
060901 E-Dagang 47
060902 Maklumat Umum 47
0610 Pemantauan 48
061001 Pengauditan Dan Forensik ICT 48
061002 Jejak Audit 48
061003 Sistem Log 49
061004 Pemantauan Log 49
BIDANG 07 KAWALAN CAPAIAN 49
0701 Dasar Kawalan Capaian 50
070101 Keperluan Kawalan Capaian 50
0702 Pengurusan Capaian Pengguna 50
070201 Pendaftaran Akaun Pengguna 50

070202 Hak Capaian 51
070203 Pengurusan Kata Laluan 52
070204 Clear Desk Dan Clear Screen 53
0703 Kawalan Capaian Rangkaian 53
070301 Capaian Rangkaian 53
070302 Capaian Internet 54
0704 Kawalan Capaian Sistem Pengoperasian 55
070401 Capaian Sistem Pengoperasian 55
0705 Kawalan Capaian Aplikasi Dan Maklumat 56
070501 Capaian Aplikasi Dan Maklumat 56
0706 Perkakasan Mudah Alih Dan Kerja Jerak Jauh 56
070601 Perkakasan Mudah Alih 56
070602 Kerja Jarak Jauh 56
BIDANG 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM 57
0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi 57
080101 Keperluan Keselamatan Sistem Maklumat 57
080102 Pengesahan Data Input Dan Output 57
0802 Kawalan Kriptografi 58
080201 Enkripsi 58
080202 Tandatangan Digital 58
080203 Pengurusan Infrastruktur Kunci Awam (PKI) 58
0803 Keselamatan Fail Sistem 58
080301 Kawalan Fail Sistem 58
0804 Keselamatan Dalam Proses Pembangunan Dan Sokongan 59
080401 Prosedur Kawalan Perubahan 59
0805 Kawalan Teknikal Keterdedahan (Vulnerability) 59
080501 Kawalan Dari Ancaman Teknikal 59
BIDANG 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN 60
0901 Mekanisme Pelaporan Insiden Keselamatan ICT 60
090101 Mekanisme Pelaporan 60
0902 Pengurusan Maklumat Insiden Keselamatan ICT 61
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT 61
BIDANG 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN 62

1001 Dasar Kesinambungan Perkhidmatan …….. 62
100101 Pelan Kesinambungan Perkhidmatan …… 62
BIDANG 11 PEMATUHAN …… 64
1101 Pematuhan Dan Keperluan Perundangan …… 64
110101 Pematuhan Dasar …… 64
110102 Pematuhan Dengan Dasar, Piawaian dan Keperluan Teknikal …….. 64
110103 Pematuhan Keperluan Audit …… 64
110104 Keperluan Perundangan …….. 65
110105 Pelanggaran Dasar ……... 65
GLOSARI …….. 66
LAMPIRAN A …… 70
LAMPIRAN B …… 71
LAMPIRAN C …… 74
LAMPIRAN D …… 76
LAMPIRAN E 77

PENGENALAN

Dasar Keselamatan ICT (DKICT) Kerajaan Negeri Sarawak mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini juga menerangkan kepada semua penjawat awam Pentadbiran Negeri mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT Kerajaan Negeri.

OBJEKTIF

Dasar Keselamatan ICT Kerajaan Negeri diwujudkan untuk menjamin kesinambungan urusan dengan meminimumkan kesan insiden keselamatan ICT. Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi Kerajaan Negeri Sarawak . Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT Kerajaan Negeri ialah seperti berikut:

(a) Memastikan kelancaran operasi Kerajaan dan meminimumkan kerosakan atau kemusnahan;

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

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

PERNYATAAN DASAR

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

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

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

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

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

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

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

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

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

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

(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

Aset ICT Kerajaan Negeri Sarawak terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT Kerajaan Negeri Sarawak 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 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. Contoh komputer, pelayan, perkakasan 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 agensi-agensi Kerajaan;

(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 Kerajaan Negeri. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod di Agensi Kerajaan Negeri, 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 bagi mencapai misi dan objektif 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

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT Kerajaan Negeri Sarawak 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 perenggan 53, muka surat 15;

(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, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

(c) Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap darisemasa ke semasa;

iii. Menentukan maklumat sedia untuk digunakan;

iv. Menjaga kerahsiaan kata laluan;

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

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

vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

(d) Pengasingan

Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi asset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

(e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

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

(f) Pematuhan

Dasar Keselamatan ICT Kerajaan Negeri Sarawak hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

(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 aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan; dan

(h) 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.

BIDANG 01 – DASAR KESELAMATAN	
0101 Dasar Keselamatan ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Kerajaan Negeri dan perundangan yang berkaitan.	
010101 Pelaksanaan Dasar	
Dasar ini diluluskan oleh Majlis Teknologi dan Sumber Maklumat Negeri (SITRC), dan dilaksanakan oleh Jawatankuasa Keselamatan ICT (JKICT) Kerajaan Negeri.	Pengarah ICTU selaku Pengerusi JKICT
010102 Penyebaran Dasar	
Dasar ini hendaklah disebarkan kepada semua Penjawat Awam dan pihak yang berkepentingan.	Ketua Agensi
010103 Kajian Semula Dasar	
Dasar Keselamatan ICT hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa untuk memastikan kesinambungan perkhidmatan. Prosedur kajian semula Dasar Keselamatan ICT Kerajaan Negeri adalah seperti berikut: (a) Kenal pasti dan tentukan perubahan yang diperlukan; (b) Kemukakan cadangan pindaan secara bertulis kepada Kumpulan Kerja Domain untuk pembentangan dan pertimbangan JKICT dan seterusnya untuk kelulusan SITRC; (c) Maklum kepada semua Penjawat Awam dan pihak berkepentingan mengenai perubahan yang telah diluluskan.	ICTSO Agensi, Kumpulan Kerja Domain Keselamatan ICT Negeri dan Ketua Agensi
010104 Aplikasi Dasar	
Dasar Keselamatan ICT Kerajaan Negeri Sarawak adalah terpakai kepada semua penjawat awam serta pihak berkepentingan.	Penjawat Awam

BIDANG 02 – ORGANISASI KESELAMATAN ICT	
0201 Struktur Organisasi Dalaman	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT Kerajaan Negeri Sarawak.	
020101 Pengarah Unit Teknologi Maklumat dan Komunikasi (ICTU)	
Pengarah ICTU adalah Pengerusi kepada Jawatankuasa Keselamatan ICT (JKICT) Kerajaan Negeri Sarawak dan Ketua Pegawai Maklumat Negeri (Chief CIO) berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: (a) Memastikan semua penjawat awam memahami peruntukan- peruntukan di bawah Dasar Keselamatan ICT Kerajaan Negeri Sarawak; (b) Memastikan semua penjawat awam mematuhi Dasar Keselamatan ICT Kerajaan Negeri Sarawak; (c) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT Kerajaan Negeri Sarawak; dan (e) Mempengerusikan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT).	Pengarah ICTU

020102 Ketua Pegawai Keselamatan ICT Negeri (Ketua ICTSO)	
Ketua ICTSO bagi Kerajaan Negeri ialah Ketua Penolong Pengarah, Bahagian Kerajaan Elektronik, Unit Teknologi Maklumat Dan Komunikasi, Jabatan Ketua Menteri (ICTU). Peranan dan tanggungjawab Ketua ICTSO adalah seperti berikut: (a) Mengurus keseluruhan program-program keselamatan ICT Kerajaan Negeri; (b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT Kerajaan Negeri; (c) Menyelaraskan program penerangan dan pendedahan berkenaan Dasar Keselamatan ICT Kerajaan Negeri kepada semua penjawat awam dan pihak berkepentingan pengguna; dan (d) Menyelaraskan pembangunan dan penyelenggaraan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT Kerajaan Negeri.	Ketua ICTSO
020103 Ketua Agensi	
Ketua Agensi adalah berperanan dan bertanggungjawab dalam perkara-perkara berikut di agensi masing-masing: (a) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT Kerajaan Negeri; (b) Memastikan semua Penjawat Awam dan pihak berkepentingan memahami peruntukan-peruntukan Dasar Keselamatan ICT Kerajaan Negeri; (c) Memastikan semua keperluan sumber agensi adalah mencukupi; (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan berlandaskan Dasar Keselamatan ICT Kerajaan Negeri; dan (e) Mencalonkan Ketua Pegawai Maklumat (CIO), Penolong Ketua Pegawai Maklumat (ACIO), Pegawai Keselamatan ICT (ICTSO), dan Pentadbir Laman Web dan Pentadbir Sistem.	Ketua Agensi

020104 Ketua Pegawai Maklumat Agensi (CIO Agensi)	
CIO Agensi bertanggungjawab kepada perkara berikut: (a) Membantu Ketua Agensi dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT di agensi masing-masing; (b) Memastikan pelaksanaan dasar keselamatan ICT, piawaian ataupun garis panduan untuk diterima pakai dalam penyimpanan maklumat terkini sehinggalah mengikut langkah perubahan teknologi, hala tuju organisasi dan ancaman yang mungkin dihadapi; (c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT serta pengurusan risiko dan pengauditan; dan (d) Menentukan kawalan akses pengguna terhadap aset ICT Kerajaan.	CIO Agensi
020105 Pegawai Keselamatan ICT (ICTSO Agensi)	
ICTSO Agensi bertanggungjawab terhadap perkara berikut: (a) Melaksana program-program keselamatan ICT yang telah dikenalpasti; (b) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT Kerajaan Negeri kepada semua pengguna agensi; (c) Mengenal pasti dan menganalisis risiko aset ICT. Menjalankan pengurusan risiko; (d) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan Negeri (QCERT), dan memaklumkannya kepada CIO Agensi; (e) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan mengesyorkan memperakukan langkah-langkah baik pulih dengan segera kepada tindakan pencegahan dan pengukuhan kepada Ketua ICTSO; dan (f) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Kerajaan Negeri.	ICTSO Agensi

020106 Penolong Ketua Pegawai Maklumat (ACIO Agensi)	
ACIO Agensi bertanggungjawab kepada perkara berikut: (a) Membantu CIO dalam melaksanakan tanggungjawab berkaitan aset ICT. (b) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang tamat perkhidmatan, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; dan (c) Bertanggungjawab memantau setiap perkakasan dan perisian ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	ACIO Agensi
020107 Pembekal Perkhidmatan	
Pembekal Perkhidmatan yang dilantik mempunyai peranan dan tanggungjawab seperti berikut: (a) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan dalam Dasar Keselamatan ICT Kerajaan Negeri; (b) Memantau aktiviti capaian harian bagi aplikasi sistem dan rangkaian; (c) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan memberhentikannya dengan serta merta; (d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT Kerajaan Negeri dan menjaga kerahsiaan maklumat Kerajaan Negeri; (e) Menyediakan laporan mengenai aktiviti capaian secara berkala; (f) Menganalisis dan menyimpan rekod jejak audit; dan (g) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada Ketua ICTSO dan QCERT dengan segera.	Pembekal Perkhidmatan

020108 Penjawat Awam	
Penjawat Awam mempunyai peranan dan tanggungjawab seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan Negeri; (b) Memahami implikasi keselamatan ICT kesan dari tindakannya; (c) Lulus tapisan keselamatan; (d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT Kerajaan Negeri dan menjaga kerahsiaan maklumat Kerajaan Negeri; (e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO agensi dengan segera; (f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan (g) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT Kerajaan Negeri seperti di Lampiran 1.	Penjawat Awam

020109 Jawatankuasa Keselamatan ICT Kerajaan Negeri (JKICT Kerajaan Negeri)	
JKICT Kerajaan Negeri bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT Kerajaan Negeri yang akan dibentangkan untuk kelulusan SITRC sebelum pelaksanaan. Keanggotaan JKICT Kerajaan Negeri adalah seperti di Lampiran **Pengerusi:** Pengarah, Unit ICT Kerajaan Negeri **Ahli:** (1) Semua Ketua Penolong Pengarah Unit ICT (2) Pengarah Unit Keselamatan Negeri (3) Ketua Agensi Pembekal Perkhidmatan yang dilantik oleh Kerajaan Negeri (4) Semua Ketua Kumpulan Kerja Domain Keselamatan ICT Kerajaan Negeri **Perlantikan:** Pegawai-pegawai yang diperlukan boleh dilantik secara rasmi. **Urus Setia** bagi JKICT Kerajaan Negeri ialah Seksyen Kerajaan Elektronik (Keselamatan ICT), Unit ICT. **Bidang kuasa:** (a) Membentang dokumen DKICT Kerajaan Negeri untuk kelulusan SITRC; (b) Memantau tahap pematuhan keselamatan ICT; (c) Memperaku garis panduan, dan prosedur aplikasi Kerajaan Negeri berlandaskan DKICT Kerajaan Negeri; (d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; (e) Memastikan DKICT Kerajaan Negeri selaras dengan dasar ICT Kerajaan Pusat; (f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; (g) Membincang tindakan yang melibatkan pelanggaran DKICT Kerajaan Negeri; dan (h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	JKICT Kerajaan Negeri
0201010 Majlis Teknologi dan Sumber Maklumat Negeri Sarawak (SITRC)	
Majlis Teknologi dan Sumber Maklumat Negeri Sarawak (SITRC) adalah badan yang bertanggungjawab untuk merangka, mengkaji dan menentukan dasar, objektif, strategi dan piawaian dalam pembangunan sumber dan sistem maklumat untuk Kerajaan Negeri.	SITRC

0201011 Kumpulan Kerja Domain Keselamatan ICT Negeri (KKDKICT)

KKDKICT

Peranan dan tanggungjawab Kumpulan Kerja Domain Keselamatan ICT (KKDKICT) Negeri adalah seperti berikut:

(a) Membangun dan menyelenggara prosedur dalam menyokong pelaksanaan Dasar Keselamatan ICT Kerajaan Negeri; dan

(b) Mengkaji semula prosedur sedia ada bagi memastikan ianya selaras dengan Dasar Keselamatan ICT Kerajaan Negeri semasa secara berkala.

Keanggotaan Kumpulan Kerja Domain adalah seperti berikut:

Bil.	Kumpulan Kerja Keselamatan ICT Negeri	Ahli
1.	Kumpulan kerja Domain 1 • Pembangunan dan Penyelenggaraan Dasar • Organisasi Keselamatan • Pengurusan Aset • Keselamatan Sumber Manusia	CIO, ICT Unit (Leader) CIO, SFS Office ICTSO, JKR ICTSO, HRM Unit ICTSO, IAU
2.	Kumpulan kerja Domain 2 • Keselamatan Fizikal dan Persekitaran • Pengurusan Operasi dan Komunikasi • Kawalan Capaian	ICTSO, ICTU CIO, L&S Dept ICTSO, Security Unit ICTSO, KASKA ACIO, ICT Unit Pentadbir Sistem, SAINS
3.	Kumpulan kerja Domain 3 • Perolehan, Pembangunan dan Penyelenggaraan Sistem • Pengurusan Pengendalian Insiden Keselamatan	Ketua ICTSO, ICT Unit ICTSO, DBKU ISM, L&S Dept ICTSO, SAINS
4.	Kumpulan kerja Domain 4 • Pengurusan Kesinambungan Perkhidmatan • Pematuhan	CIO, IAU CIO, SAG Office CIO, Pustaka Negeri ICTSO, L&S Dept Penolong Pengarah, ICT Unit

Agensi-agensi boleh dikooptasikan jika diperlukan.

0201012 PasukanTindak Balas Insiden Keselamatan ICT Kerajaan (QCERT)	
Keanggotaan QCERT adalah seperti berikut: (a) **Pengarah QCERT** : Pengarah Unit ICT (b) **Pengurus QCERT** : Ketua Penolong Pengarah, Seksyen Kerajaan Elektronik, Unit ICT (c) **Ahli** : 1) Ketua Penolong Pengarah, Seksyen Perancangan dan Pelaksanaan ICT, Unit ICT 2) ICTSO, Unit ICT 3) Pegawai Sistem Perisian, Unit ICT 4) Pegawai Sistem Rangkaian, Unit ICT 5) Pegawai Fail Log, Unit ICT 6) Ketua Penolong Pengarah, Unit Audit Dalam 7) ICTSO, Unit Keselamatan Negeri Peranan dan tanggungjawab QCERT adalah seperti berikut: (a) Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; (b) Merekod dan menjalankan siasatan awal insiden yang diterima; (c) Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih dengan kadar segera; (d) Menasihati Kerajaan Negeri mengambil tindakan pemulihan dan pengukuhan; (e) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada Kerajaan Negeri; dan (f) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	QCERT

0201013 Pentadbir Sistem*	
Peranan dan tanggungjawab Pentadbir Sistem adalah seperti berikut: (a) Memastikan prosedur pengurusan operasi sistem dilaksanakan seperti yang ditetapkan oleh Agensi Kerajaan Negeri; (b) Mengambil tindakan yang sesuai dengan segera apabila dimaklumkan mengenai pengguna sistem yang tamat perkhidmatan, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; (c) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian kepada sistem aplikasi ICT berdasarkan arahan pihak pengurusan atasan; (d) Memastikan kerahsiaan kata laluan yang telah didaftarkan dalam sistem dan memantau aktiviti capaian harian pengguna sistem; (e) Mengenal pasti aktiviti-aktiviti seperti pencerobohan dan pengubahsuaian data dan/atau sistem tanpa kebenaran dan mengambil tindakan membatalkan atau memberhentikannya dengan serta-merta; dan (f) Menyimpan dan menganalisis rekod jejak audit (*audit trail*); ** Agensi Kerajaan Negeri yang berkaitan sahaja.*	Pentadbir Sistem

0202 Pihak Yang Berkepentingan	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak yang berkepentingan.	
020201 Keperluan Keselamatan Dalam Kontrak Dengan Pihak Yang Berkepentingan	
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak yang berkepentingan dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: (a) Memahami dan mematuhi Dasar Keselamatan ICT Kerajaan Negeri; (b) Mengenalpasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksana kawalan yang sesuai sebelum memberi kebenaran capaian; (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak yang berkepentingan; (d) Akses kepada aset ICT Kerajaan Negeri perlu berlandaskan perjanjian kontrak; dan (e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam dokumen perjanjian dengan pihak yang berkepentingan.	Ketua Agensi, CIO, ICTSO, ACIO dan Pihak yang berkepentingan

BIDANG 03 – PENGURUSAN ASET ICT	
0301 Akauntabiliti Aset	
Objektif: Memberi perlindungan yang bersesuaian ke atas semua aset ICT hak milik agensi Kerajaan Negeri.	
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 dikenal pasti dan maklumat aset direkod ke dalam *Asset Management System* dan sentiasa dikemas kini; (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 agensi masing-masing; (d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumenkan dan dilaksanakan; dan (e) Setiap Penjawat Awam adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pegawai Aset, ACIO dan Penjawat Awam
0302 Pengkelasan dan Pengendalian Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
030201 Pengkelasan Maklumat	
Maklumat hendaklah dikategorikan dengan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Berdasarkan Arahan Keselamatan, maklumat hendaklah diperingkatkan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad.	Penjawat Awam

030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah keselamatan berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) Menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur 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.	Penjawat Awam
030203 Penggunaan Aset ICT Yang Dibenarkan	
Aset ICT yang diperuntukkan kepada kakitangan adalah untuk kegunaan rasmi dan perkara yang berkaitan dengan tugas sahaja. Antaranya : (a) Peraturan penggunaan Internet dan mel elektronik (0608 – Pengurusan Pertukaran Maklumat) (b) Penggunaan peranti mudah alih, terutama sekali untuk kegunaan luar pejabat dan syarikat (0706 – Perkakasan Mudah Alih dan Kerja Jarak Jauh) (c) Peraturan penggunaan komputer agensi (sila rujuk DSM-GP04-SP01-SD01).	Penjawat Awam

BIDANG 04 – KESELAMATAN SUMBER MANUSIA	
0401 Keselamatan Sumber Manusia	
Objektif: Memastikan sumber manusia yang terlibat termasuk Penjawat Awam dan pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.	
040101 Sebelum Perkhidmatan	
Perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pejawat awam serta pihak yang berkepentingan terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk pejawat awam serta pihak yang berkepentingan berasaskan keperluan perundangan, peraturan dan etika selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.	Penjawat Awam
040102 Dalam Perkhidmatan	
Perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan penjawat awam serta pihak yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Agensi Kerajaan Negeri; (b) Memastikan latihan kesedaran berkaitan pengurusan keselamatan aset ICT diberi kepada pengguna ICT secara berterusan dalam melaksanakan tugas dan tanggungjawab mereka; (c) Memastikan tindakan disiplin dan/atau undang-undang yang sewajarnya ke atas Penjawat Awam serta pihak yang berkepentingan di atas kegagalan mematuhi perundangan dan peraturan Agensi Kerajaan Negeri; dan (d) Memantapkan pengetahuan berkaitan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, Penjawat Awam hendaklah merujuk kepada Ketua Agensi.	Penjawat Awam

040103 Bertukar Atau Tamat Perkhidmatan	
Perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua perkakasan ICT di bawah kawalan dikembalikan kepada Ketua Agensi mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) Menamatkan dengan segera semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh Kerajaan Negeri dan/atau terma perkhidmatan.	Penjawat Awam

BIDANG 05 – KESELAMATAN FIZIKAL DAN PERSEKITARAN	
0501 Keselamatan Kawasan	
Objektif: Melindungi premis, aset dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
050101 Kawalan Kawasan	
Kawalan kawasan bertujuan mencegah akses tanpa kebenaran, kerosakan dan gangguan secara fizikal terhadap premis, aset dan maklumat agensi. Perkara yang harus dipatuhi termasuk yang berikut: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (b) Menggunakan perimeter keselamatan (halangan seperti dinding, pagar kawalan, pengawal keselamatan, kamera litar tertutup(CCTV)) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (c) Menghadkan laluan keluar masuk; (d) Mengadakan kaunter kawalan berserta perkhidmatan kawalan keselamatan; (e) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan dan pelawat yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (f) Merekabentuk dan susun atur pejabat bagi melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan pejabat; (g) Menyediakan kemudahan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan lain-lain bencana; (h) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (i) Memastikan akses ke kawasan penghantaran, pemunggahan dan lain-lain lokasi terhad hanya kepada pihak yang dibenarkan.	Unit Keselamatan Negeri dan Ketua Agensi

050102 Kawalan Masuk Fizikal	
Perkara yang perlu dipatuhi termasuk yang berikut: (a) Penjawat awam hendaklah memakai pas pengenalan sepanjang waktu bertugas; (b) Pas tersebut hendaklah dikembalikan kepada Agensi Kerajaan Negeri apabila pemilik pas tamat perkhidmatan atau bersara; (c) Pelawat hendaklah mendapatkan Pas Pelawat di pintu masuk bangunan pejabat/kaunter perkhidmatan Agensi Kerajaan Negeri dan mengembalikannya selepas tamat lawatan. Tarikh, masa dan maklumat pelawat hendaklah direkodkan; dan (d) Kehilangan pas mestilah dilaporkan kepada pegawai keselamatan dengan segera.	Penjawat Awan Negeri, Pelawat dan Pegawai Keselamatan
050103 Kawasan Terhad	
Kawasan terhad adalah kawasan yang aksesnya hanya dibenarkan kepada pegawai-pegawai tertentu sahaja. Ini dilaksanakan untuk melindungi aset yang terdapat di dalam kawasan tersebut. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan terhad kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Ketua Agensi dan Pegawai Keselamatan Agensi

0502 Keselamatan Perkakasan	
Objektif: Mengelak sebarang kehilangan, kerosakan, kecurian serta penyalahgunaan perkakasan dan gangguan perkhidmatan	
050201 Perkakasan ICT	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Penjawat Awam hendaklah memastikan perkakasan ICT di bawah kawalannya berfungsi dengan sempurna dan melaporkan sebarang kerosakan atau kehilangan; (b) Penjawat Awam tidak dibenarkan membuat sebarang pengubahsuaian, pertukaran perkakasan ICT dan konfigurasi yang telah ditetapkan kecuali mendapat kebenaran CIO; (c) Penjawat Awam mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*), berfungsi dan dikemaskini; di samping melakukan imbasan ke atas media storan yang digunakan; (d) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (e) Semua perkakasan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; (f) Penggunaan Uninteruptable Power Supply (UPS) bagi perkakasan-perkakasan kritikal adalah diwajibkan; perlu disokong oleh Uninteruptable Power Supply (UPS); (g) Perkakasan ICT hendaklah disimpan atau diletakkan di tempat yang selamat, teratur, bersih dan mempunyai ciri-ciri keselamatan. Perkakasan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak/bilik khas dan berkunci; (h) Perkakasan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai sistem pengudaraan (*air ventilation*) yang baik; (i) Kelulusan dari Pegawai Inventori Agensi adalah diperlukan untuk mengeluarkan sebarang perkakasan ICT dari premis Kerajaan Negeri dan hendaklah direkodkan bagi tujuan pemantauan; (j) Pengendalian perkakasan ICT hendaklah mematuhi peraturan semasa yang berkuatkuasa; (k) Pengguna tidak dibenarkan mengubah lokasi komputer dari tempat asal ia ditempatkan tanpa kebenaran ACIO; dan (l) Sebarang pelekat selain bagi tujuan rasmi adalah tidak dibenarkan. Ini bagi memastikan perkakasan tersebut sentiasa berada dalam keadaan baik.	Penjawat Awam, CIO,

050202 Media Storan	
Media storan merupakan perkakasan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *thumb drive, external hard disk* dan media storan lain. Media-media storan perlu berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan yang bersesuaian dengan kandungan maklumat; (b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; (c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan (refer to Arahan Keselamatan) termasuk tidak mudah diganggu-gugat, kalis api, air dan medan *magnet*; (e) Akses dan pergerakan media storan hendaklah direkodkan; (f) Membuat salinan atau penduaan (backup) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; (g) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan (h) Data dalam media storan yang hendak dilupuskan mestilah dihapuskan dengan cara yang teratur dan selamat.	Penjawat Awam
050203 Media Tandatangan Digital	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan (c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Penjawat Awam

050204 Media Perisian Dan Aplikasi	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan Kerajaan Negeri; (b) Sistem aplikasi dalaman tidak dibenarkan ditunjuk atau diagih kepada pihak lain kecuali dengan kebenaran CIO; (c) Lesen perisian (*registration code, serials, CD-keys, product keys*) perlu disimpan berasingan daripada cakera padat CD-ROM, disket atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan (d) Kod sumber aplikasi sesuatu sistem hendaklah disimpan oleh CIO Agensi dengan teratur dan selamat. Sebarang pindaan perubahan mestilah mengikut prosedur yang ditetapkan.	Penjawat Awam, CIO Agensi
050205 Penyelenggaraan Perkakasan ICT	
Perkakasan ICT hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penyelenggaraan perkakasan ICT yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh vendor; (b) Memastikan perkakasan ICT hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) ACIO bertanggungjawab terhadap penyelanggaraan setiap perkakasan ICT sama ada dalam tempoh jaminan atau setelah habis tempoh jaminan; (d) Menyemak dan menguji semua perkakasan ICT sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Sebarang penyelenggaraan mestilah mendapat kebenaran daripada CIO.	ACIO, CIO

050206 Perkakasan Dibawa Keluar Dari Premis	
Perkakasan ICT yang dibawa keluar dari premis Kerajaan Negeri adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Kebenaran membawa keluar sebarang perkakasan ICT perlu mendapat kelulusan bertulis daripada pegawai yang diberi kuasa; (b) Aktiviti membawa keluar perkakasan hendaklah direkodkan; (c) Perkakasan perlu dilindungi dan dikawal sepanjang masa; dan (d) Penyimpanan atau penempatan perkakasan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Penjawat Awam, Pegawai Aset Agensi, CIO dan ACIO
050207 Pelupusan Dan Kitar Semula Perkakasan ICT	
Pelupusan melibatkan perkakasan ICT yang telah rosak, usang dan tidak boleh dibaikpulih sama ada harta modal atau inventori yang dibekalkan oleh Kerajaan Negeri dan ditempatkan di agensi. Perkakasan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Kerajaan Negeri.	Penjawat Awam dan ACIO

0503 Keselamatan Persekitaran	
Objektif: Melindungi aset ICT Agensi Kerajaan Negeri dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian manusia serta kemalangan.	
050301 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk menyewa, mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada pihak berkuasa yang berkenaan. Bagi menjamin keselamatan persekitaran, perkara berikut hendaklah dipatuhi: (a) Merancang dan menyediakan pelan keseluruhan susun atur premis (pusat data, bilik percetakan, perkakasan komputer, 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 berpatutan seperti alat amaran kebakaran, pemadam api dan sebagainya. (c) Perkakasan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dilihat, dicapai dan dikendalikan; (d) Bahan mudah terbakar dan/atau bercecair hendaklah disimpan di tempat yang bersesuaian dan berjauhan dari aset ICT; (e) Pengguna adalah dilarang merokok atau menggunakan perkakasan memasak seperti cerek elektrik berhampiran perkakasan komputer; (f) Semua perkakasan perlindungan hendaklah disemak dan diuji secara berjadual atau mengikut peruntukan undang-undang. Aktiviti dan keputusan ujian perlu direkodkan bagi memudahkan rujukan dan tindakan susulan sekiranya perlu; dan (g) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	Ketua Agensi

050302 Bekalan Kuasa	
Bekalan kuasa merupakan sumber kuasa elektrik yang dibekalkan kepada perkakasan ICT. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua perkakasan ICT hendaklah dibekalkan dengan bekalan elektrik yang berpatutan; (b) Perkakasan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal yang dikenal pasti seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan (c) Semua perkakasan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	ICTSO
050303 Kabel	
Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan maklumat hendaklah dilindungi untuk mengelak berlakunya kebocoran maklumat. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: (a) Menggunakan kabel mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan (d) Semua kabel perlu dilabelkan dengan jelas untuk memudahkan pengenalpastian semasa berlakunya gangguan atau kerosakan.	ICTSO dan Pembekal Perkhidmatan
050304 Prosedur Kecemasan	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Prosedur kecemasan mesti diletakkan di tempat yang bersesuaian; (b) Prosedur kecemasan mesti jelas dan mudah difahami. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan; dan (c) Sebarang insiden kecemasan persekitaran yang berlaku hendaklah dilaporkan kepada Pegawai Keselamatan Agensi Jabatan (PKJ) yang dilantik.	Unit Keselamatan Negeri, Penjawat Awam dan Pegawai Keselamatan Agensi

0504 Keselamatan Dokumen	
Objektif: Melindungi maklumat Agensi Kerajaan Negeri dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam serta kesilapan atau kecuaian manusia.	
050401 Dokumen	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua pengendalian dokumen hendaklah mengikut peringkat keselamatan masing-masing; (b) Dokumen terperingkat hendaklah dikendali mengikut Arahan Keselamatan; dan (c) Dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik hendaklah menggunakan kaedah enkripsi (*encryption*).	Penjawat Awam

BIDANG 06 – PENGURUSAN OPERASI DAN KOMUNIKASI	
0601 Pengurusan Prosedur Operasi	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
060101 Pengendalian Prosedur Operasi	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur pengurusan operasi yang diguna pakai hendaklah didokumentasi, disimpan, dikawal dan mudah dicapai oleh sesiapa yang berkenaan; (b) Setiap prosedur mesti 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 mengikut keperluan semasa.	CIO dan ICTSO agensi
060102 Kawalan Perubahan	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (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.	CIO dan ICTSO agensi

060103 Pengasingan Tugas Dan Tanggungjawab	
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, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan (c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan untuk produksi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan kumpulan pengurusan pusat data.	CIO, ACIO dan ICTSO Agensi
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 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 ketigaperlu sentiasa dipantau, disemak semula dan diaudit mengikut keperluan; dan (c) Pengurusan perubahan dasar terhadap perkhidmatan yang dilaksanakan dan diselenggarakan oleh pihak ketiga perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua

0603 Perancangan Dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301 Perancangan Kapasiti	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. 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.	CIO, ICTSO dan Pentadbir Sistem Agensi
060302 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah diuji dan memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	CIO, ACIO, ICTSO dan Pentadbir Sistem Agensi

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 yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System (IDS)* dan *Intrusion Prevention System (IPS)* serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa; (c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; (d) Mengemaskini anti virus dengan *pattern* antivirus yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (g) 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; (h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan (i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	Penjawat Awam dan Pentadbir Sistem
060402 Perlindungan dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Penjawat Awam

0605 *Housekeeping*	
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
060501 *Backup*	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat; (c) Menguji sistem *backup* dan prosedur restore sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; (d) Menyimpan sekurang-kurangnya tiga (3) generasi backup; dan (e) Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat.	Penjawat Awam, Pentadbir Sistem, ICTSO agensi

0606 Pengurusan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan	
060601 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mesti dikawal dan diselenggara demi melindungi sistem dan aplikasi di dalam rangkaian dari ancaman. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tanggungjawab dan kerja-kerja operasi rangkaian hendaklah diasingkan dari kerja-kerja operasi komputer bagi mengelakkan capaian dan pengubahsuaian yang tidak dibenarkan; (b) Perkakasan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan kotoran; (c) Capaian kepada perkakasan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Semua perkakasan mestilah melalui proses *Factory Acceptance Check (FAC)* semasa pemasangan dan konfigurasi; (e) *Firewall* hendaklah dipasang dan dikonfigurasi serta diselia oleh Pentadbir Sistem atau ICTSO; (f) Semua trafik keluar dan masuk hendaklah melalui firewall di bawah kawalan SarawakNet atau agensi Kerajaan Negeri yang telah mendapat kelulusan daripada SITRC; (g) Penjawat Awam yang diberi kuasa oleh SITRC dibenarkan memasang perisian sniffer atau network analyser pada komputer pengguna; (h) Memasang perisian *Intrusion Prevention System (IPS)* atau *Intrusion Detection System (IDS)* bagi mengesan sebarang pencerobohan dan aktiviti lain yang boleh mengancam sistem dan maklumat Kerajaan Negeri; (i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; (j) Sebarang penyambungan (seperti *USB modem*, komputer peribadi) dan penggunaan rangkaian Kerajaan Negeri yang bukan di bawah kawalan dan kelulusan SITRC adalah tidak dibenarkan; dan (k) Kemudahan bagi *wireless LAN* perlu dipastikan kawalan keselamatan.	ICTSO, Pentadbir Sistem dan Pembekal Kerajaan

0607 Pengurusan Media	
Objektif: Media dikawal dan dilindungi daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
060701 Pengurusan Media Mudah Alih	
Pengurusan media mudah alih perlu dipatuhi seperti berikut: (a) Mendaftar dan melabelkan semua media mengikut klasifikasi 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; dan (e) Menyimpan semua media di tempat yang selamat.	Pegawai Aset Agensi dan ACIO,
060702 Pelupusan M edia	
Pelupusan media yang mengandungi maklumat terperingkat perlu mematuhi prosedur yang betul dan selamat	Pegawai Aset Agensi dan ACIO,
060703 Prosedur Pengendalian Maklumat	
Prosedur pengendalian maklumat perlu dipatuhi seperti berikut: (a) Menyelenggara rekod penerima data/media yang dibenarkan; (b) Melabelkan salinan media dengan jelas bagi salinan media kepada penerima media yang dibenarkan; dan (c) Mengkaji semula senarai edaran penerima data secara berkala.	Pegawai Aset Agensi, ACIO dan Penjawat Awam,
060704 Keselamatan Sistem Dokumentasi	
Perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Capaian ke atas sistem dokumentasi perlu dikawal, direkodkan dan adalah terhad kepada pengguna yang diluluskan oleh CIO; dan (c) Menyedia, mengemaskini dan memantapkan keselamatan sistem dokumentasi mengikut keperluan semasa.	Penjawat Awam, CIO

0608 Pengurusan Pertukaran Maklumat	
Objektif: Menjamin keselamatan pertukaran maklumat rasmi dan perisian antara Kerajaan Negeri dengan agensi luar.	
060801 Pertukaran Maklumat	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar, prosedur dan kawalan pertukaran maklumat perlu diwujudkan untuk melindungi maklumat yang disalurkan melalui pelbagai kemudahan komunikasi; (b) Mewujudkan perjanjian bertulis bagi pertukaran maklumat dan perisian di antara Kerajaan Negeri dengan agensi luar; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari Kerajaan Negeri; dan (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi.	Penjawat Awam,
060802 Pengurusan Mel Elektronik (E-mel)	
Memantau penggunaan e-mel di Kerajaan Negeri secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet dengan merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*" dan mana- mana undang-undang bertulis yang berkuat kuasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: (a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh Kerajaan Negeri sahaja boleh digunakan. Penggunaan akaun milik orang lain atau berkongsi akaun adalah dilarang; (b) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; (c) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; (d) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;	Penjawat Awam,

060802 Pengurusan Mel Elektronik (E-mel)	
(e) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang diragui atau tidak dikenali; (f) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; (g) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan dan difailkan; (h) E-mel yang tidak diperlukan, tidak penting atau tidak mempunyai nilai arkib dan telah diambil tindakan hendaklah dihapuskan; (i) Pengguna hendaklah memastikan tarikh dan masa sistem komputer adalah betul. Sistem dan pelayan e-mel perlu merujuk kepada *Server Network Time Protocol (NTP)* untuk keseragaman tarikh dan masa e-mel; (j) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan segera; (k) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan (l) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbo*x* masing-masing.	Penjawat Awam,

0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)	
Objektif: Mengawal keselamatan aplikasi dan maklumat agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
060901 E-Dagang	
Pengguna boleh menggunakan kemudahan Internet bagi menggalakkan pertumbuhan e-dagang serta menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; (b) Maklumat yang terlibat dalam transaksi dalam talian (*online*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi mesej yang tidak dibenarkan; dan (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Penjawat Awam,
060902 Maklumat Umum	
Perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: (a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; (b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan (c) Memastikan segala maklumat yang hendak dipaparkan telah disahkan dan serta diluluskan sebelum dimuat naik ke laman web.	Penjawat Awam,

0610 Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
061001 Pengauditan dan Forensik ICT	
ICTSO bertanggungjawab merekod dan menganalisis perkara berikut: (a) Sebarang cubaan pencerobohan kepada sistem ICT Kerajaan Negeri; (b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), spoofing, ancaman (*threats*) dan kehilangan fizikal (*physical loss*); (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sistem tanpa pengetahuan, arahan atau persetujuan pihak bertanggungjawab; (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan 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 Ketua ICTSO.	Ketua ICTSO dan ICTSO Agensi
061002 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi tujuan pemeriksaan transaksi. Jejak audit hendaklah mengandungi maklumat berikut: (a) Rekod setiap aktiviti transaksi; (b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan (sebelum dan selepas) maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan	Ketua ICTSO, ICTSO Unit ICT, Pembekal Perkhidmatan, Pentadbir Sistem Agensi, Ahli-ahli QCERT

(d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem Agensi atau ahli-ahli QCERT hendaklah menyemak catatan jejak audit dari masa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
061003 Sistem Log	
ICTSO, Pentadbir Sistem Agensi atau Pembekal Perkhidmatan hendaklah melaksanakan 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 aktivit lain yang tidak sah seperti kecurian maklumat atau pencerobohan, Pentadbir Sistem Agensi atau Pembekal Perkhidmatan hendaklah melaporkan kepada QCERT	ICTSO atau Pentadbir Sistem Agensi, Pembekal Perkhidmatan
061004 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; (b) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; (c) Aktiviti pentadbiran dan operator sistem perlu direkodkan; (d) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan (e) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Kerajaan Negeri atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	ICTSO atau Pentadbir Sistem Agensi, Pembekal Perkhidmatan

BIDANG 07 – KAWALAN CAPAIAN	
0701 Dasar Kawalan Capaian	
Objektif: Mengawal capaian ke atas maklumat.	
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 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 perkakasan mudah alih; dan (d) Kawalan ke atas kemudahan pemprosesan maklumat.	Seksyen Kerajaan Elektronik, Unit ICT dan Pengurusan Atasan Agensi atau Ketua Agensi
0702 Pengurusan Capaian Pengguna	
Objektif: Mengawal capaian pengguna ke atas aset ICT Kerajaan Negeri.	
070201 Pendaftaran Akaun Pengguna	
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan oleh Kerajaan Negeri 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;	Penjawat Awam, Unit ICT (untuk aplikasi gunasama), JKM dan ICTSO Agensi atau Pentadbir Sistem Agensi

(d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan Kerajaan Negeri. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan (f) Akaun Pengguna boleh ditamatkan atas sebab-sebab berikut: i. Bersara ii. Digantung kerja atau iii. Ditamatkan perkhidmatan	
070202 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pengurusan Atasan Agensi atau Ketua Agensi

070203 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan katalaluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh Kerajaan Negeri seperti berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi. Kata laluan hendaklah ditukar sekurang-kurangnya selepas 90 hari atau selepas tempoh masa yang bersesuaian; (c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) dengan kombinasi aksara, angka dan/atau aksara khusus; (d) Kata laluan TIDAK BOLEH didedahkan dengan apa cara sekalipun; (e) Kata laluan *windows* dan *screen saver* hendaklah sentiasa diaktifkan~~;~~ (f) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula; (g) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (h) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; dan (i) Mengelakkan penggunaan semula kata laluan yang baru digunakan. (j) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;	Penjawat Awam, Pentadbir Sistem Agensi dan ICTSO Agensi

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 di atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *password screen saver* 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 faksimile dan mesin fotostat.	Penjawat Awam
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 Kerajaan Negeri, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Ketua ICTSO atau ICTSO Agensi,

070302 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet di Kerajaan Negeri hendaklah dipantau secara berterusan. Kewaspadaan ini akan dapat melindungi daripada kemasukan malicious code, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian Kerajaan Negeri; (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. Ketua Agensi atau Ketua Pegawai Maklumat (CIO) 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 Agensi atau Ketua Pegawai Maklumat (CIO); (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 Pengarah Bahagian Ketua Agensi 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 rasmi sahaja; (j) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan (k) Penjawat Awam adalah **DILARANG** melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan bahan bacaan, teks ucapan atau bahan-bahan yang mengandungi unsu-unsur lucah; dan ii. Menggunakan perisian tidak berlesen dan sebarang aplikasi yang boleh menjejaskan tahap capaian internet.	Penjawat Awam dan Ketua Agensi, CIO, ACIO

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 (b) Merekodkan capaian yang berjaya dan gagal. Kaedah yang digunakan hendaklah mampu menyokong 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 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 tidak boleh dikongsi; (c) Menghadkan dan mengawal penggunaan program mengikut hak capaian; dan (d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	CIO dan ICTSO Agensi atau Pentadbir Sistem Agensi

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 digalakkan dan penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	CIO dan ICTSO Agensi atau Pentadbir Sistem Agensi
0706 Perkakasan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan perkakasan mudah alih dan kemudahan kerja jarak jauh.	
070601 Perkakasan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Perkakasan mudah alih hendaklah diletakkan dan dikunci di tempat yang selamat sepanjang masa.	Penjawat Awam
070602 Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan perkakasan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Penjawat Awam

BIDANG 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.	
080101 Keperluan Keselamatan Sistem Maklumat	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah menjalankan ujian keselamatan dan mempunyai semakan pengesahan (*validation*) untuk memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat.	CIO, Pentadbir Sistem, ICTSO dan Pembekal Perkhidmatan
080102 Pengesahan Data Input dan Output	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan (b) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	CIO , ICTSO Agensi dan Pengguna Utama

0802 Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080201 Enkripsi	
Pengguna hendaklah menggunakan kaedah enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Penjawat Awam
080202 Tandatangan Digital	
Penggunaan tandatangan digital adalah digalakkan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Penjawat Awam
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.	Penjawat Awam
0803 Keselamatan Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
080301 Kawalan Fail Sistem	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Kod sumber, aturcara sistem, data ujian mesti dikawal dan dikemaskini untuk mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan (b) Mengaktifkan audit log untuk merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	ACIO dan ICTSO Agensi

0804 Keselamatan Dalam Proses Pembangunan dan Sokongan	
Objektif: Menjaga dan menjamin keselamatan dan kesahihan sistem maklumat dan aplikasi.	
080401 Prosedur Kawalan Perubahan	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem aplikasi dan pakej perisian hendaklah dikawal, diuji direkodkan dan disahkan mengikut keperluan sebelum ia 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 dilakukan oleh vendor; dan (c) Hanya pegawai yang diizinkan sahaja boleh akses kod sumber sistem aplikasi dan ianya mesti dikawal untuk mengelakkan sebarang kebocoran maklumat;	CIO, ICTSO dan Pentadbir Sistem
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. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	CIO dan ICTSO Agensi,

BIDANG 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.	
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 atau CIO dan QCERT(CERT Sarawak) dengan kadar segera: (a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; (d) Berlaku kejadian sistem yang luar kebiasaan seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT Kerajaan Negeri Sarawak adalah seperti di **Lampiran B** Prosedur pelaporan insiden keselamatan ICT berdasarkan: (a) Surat Pekeliling ICT 3/2009 – Penubuhan QCERT dan Pengurusan Pengendalian Insiden ICT Sektor Awam di Peringkat Negeri.	Penjawat awam, ICTSO, CIO dan QCERT

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. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada Kerajaan Negeri. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-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. (f) Menguji data yang dibackup secara berkala bagi memastikan ianya boleh didapat semula (*restored*).	ICTSO Agensi

BIDANG 10 – PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	
1001 Dasar Kesinambungan Perkhidmatan	
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
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 JKICT Kerajaan Negeri. Pelan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai personel Kerajaan Negeri 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) Tanggungjawab semua personel yang terlibat; (d) Senarai insiden yang boleh menjejaskan penyampaian perkhidmatan bersama dengan kemungkinan dan impak insiden tersebut terhadap keselamatan ICT; (e) Prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (f) Program latihan kepada pengguna mengenai prosedur-prosedur kecemasan; (g) Polisi dan prosedur backup dan pengujian restoration; (h) Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (i) Sumber pemprosesan dan lokasi alternatif untuk menggantikan sumber yang telah lumpuh; dan (j) Keperluan mengadakan perjanjian bertulis dengan pembekal perkhidmatan untuk penyambungan semula perkhidmatan dalam tempoh yang ditetapkan .	Ketua Agensi, CIO

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. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. 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.	Ketua Agensi, CIO

BIDANG 11 – PEMATUHAN	
1101 Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT Kerajaan Negeri.	
110101 Pematuhan Dasar	
Setiap penjawat awam hendaklah memahami dan mematuhi Dasar Keselamatan ICT Kerajaan Negeri Sarawak dan undang- undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua perkakasan, perisian, perkhidmatan, data dan maklumat ICT di Agensi Kerajaan Negeri Sarawak adalah hak milik Kerajaan Negeri Sarawak. Ketua Agensi/pegawai yang diberi kuasa berhak memantau aktiviti pengguna untuk mengesan penggunaan yang lain daripada tujuan rasmi. Sebarang penggunaan aset ICT milik Kerajaan Negeri Sarawak selain daripada maksud dan tujuan rasmi merupakan satu penyalahgunaan sumber.	Penjawat Awam
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
Semua projek ICT hendaklah diluluskan oleh SITRC. Semua prosedur keselamatan dalam bidang tugas setiap penjawat awam hendaklah mematuhi dasar, piawaian dan keperluan teknikal Agensi. Pemeriksaan berkala perlu dilakukan ke atas sistem maklumat Jabatan bagi memastikan ianya mematuhi piawaian perlaksanaan Dasar Keselamatan ICT.	Ketua Agensi, Urusetia SITRC, CIO dan 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 yang beroperasi perlu dirancang dan dipersetujui sebagai satu strategi pencegahan terhadap kebarangkalian berlakunya gangguan dalam penyediaan perkhidmatan. Capaian ke atas perkakasan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlakunya penyalahgunaan.	Ketua Agensi, CIO, ICTSO dan semua personel ICT lain

110104 Keperluan Perundangan	
Semua penjawat awam hendaklah mematuhi keperluan perundangan atau peraturan-peraturan berkaitan seperti di Lampiran C. Sebarang keperluan perundangan atau peraturan-peraturan daripada Kerajaan Persekutuan seperti di Lampiran D juga boleh dirujuk.	Penjawat Awam
110105 Pelanggaran Dasar	
Penjawat awam yang melanggar mana-mana peruntukan dalam. Dasar Keselamatan ICT Kerajaan Negeri boleh dikenakan tindakan tatatertib tertakluk kepada perundangan kerajaan yang berkuat kuasa semasa.	Pihak berkuasa tatatertib yang berkaitan

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Perkakasan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau volum data yang boleh dipindahkan melalui kawalan komunikasi (contohnya antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. *Firewall* 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*).
QCERT	*Sarawak 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.

GLOSARI	
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 titk 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, atau kesilapan yang berbahaya kepada sistem. Sifat IDS adalah berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perisian dan 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.

GLOSARI	
Log-out	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat daripada komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *wordprocessing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah Agensi Kerajaan Negeri.
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
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.

GLOSARI	
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif persendirian dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu perkakasan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada sumber lain ketika ketiadaan bekalan kuasa kepada perkakasan yang disambungkan.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna pada masa ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang membenarkan interaksi antara dua atau lebih lokasi melalui paparan video dan audio dua hala secara serentak.
Virus	Perisian yang bertujuan merosakkan perkakasan, perisian atau data elektronik.
Wireless LAN	Rangkaian komputer yang terhubung tanpa melalui kabel.
Agensi Kerajaan Negeri	Termasuk Kementerian dan Jabatan Negeri, Badan-badan Berkanun Negeri dan Pihak Berkuasa Tempatan.
WAN	Wide Area Network Rangkaian Kawasan Luas yang menghubungkan komputer
Penjawat Awam	Kakitangan Agensi Kerajaan Negeri

Lampiran A

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KERAJAAN NEGERI

Nama (Huruf Besar) : ……

No. Kad Pengenalan : ……

Jawatan : ……

Bahagian : ……

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

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

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

Tanda tangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT (ICTSO)

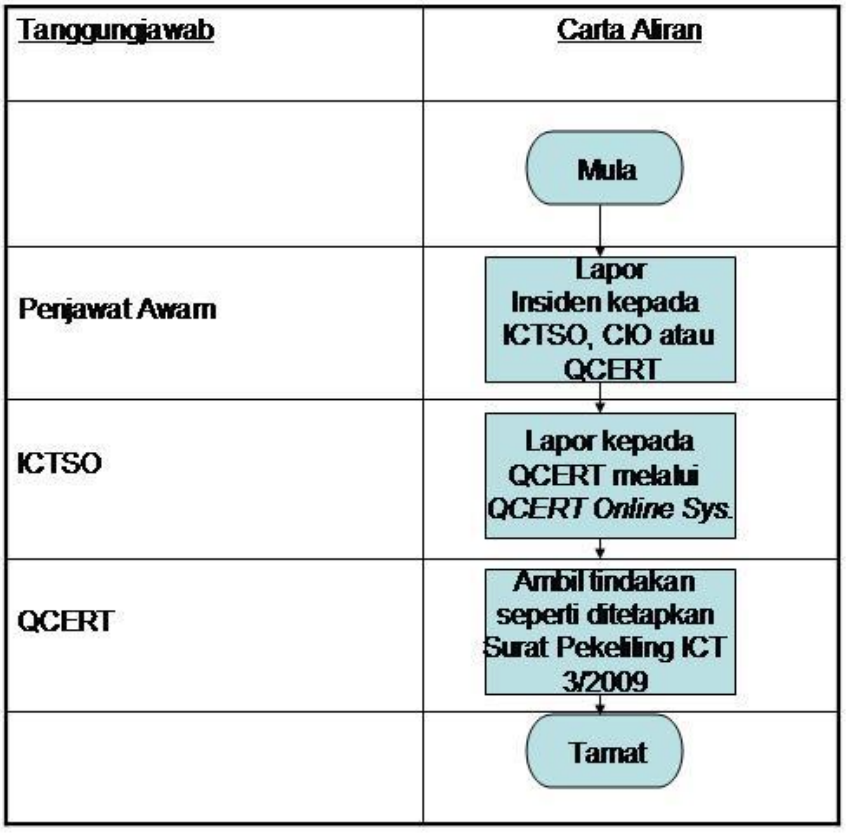
.....

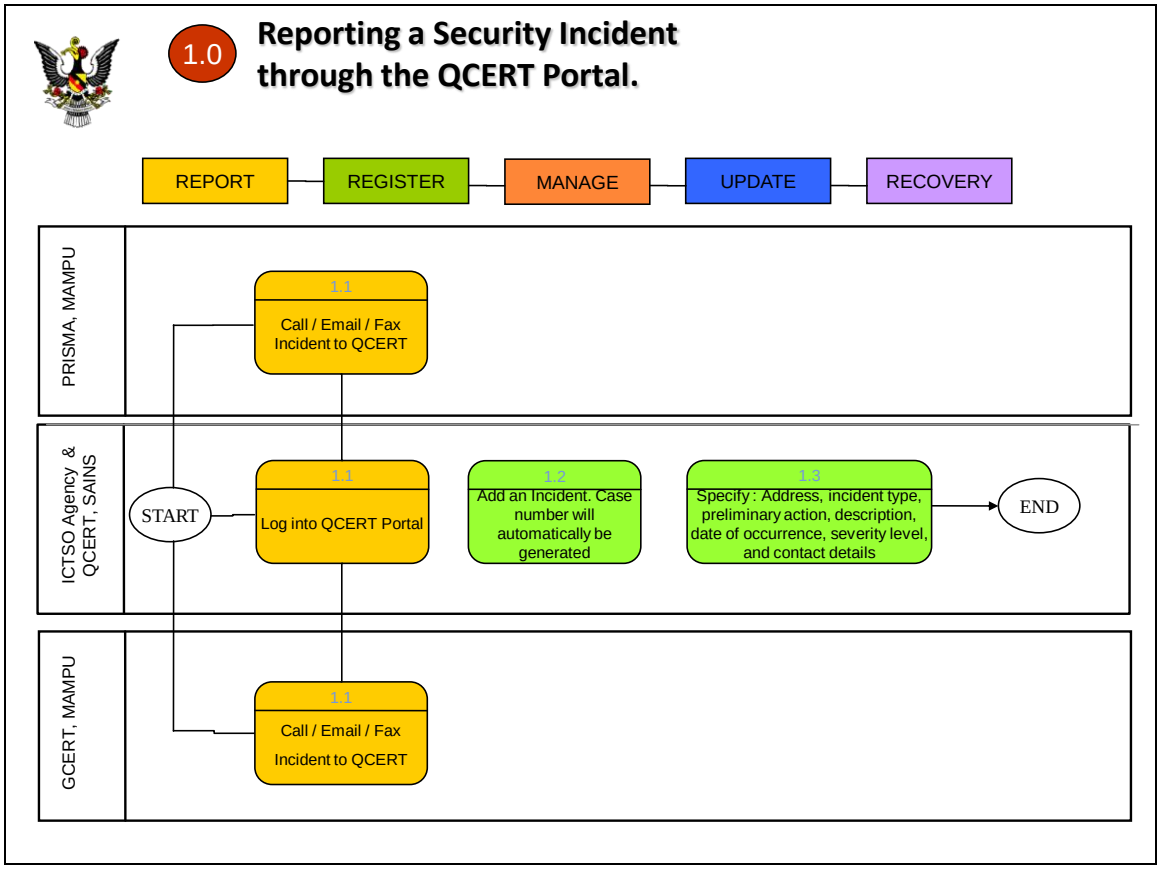
(Nama Pegawai Keselamatan ICT)
b.p. Ketua Agensi Kerajaan Negeri

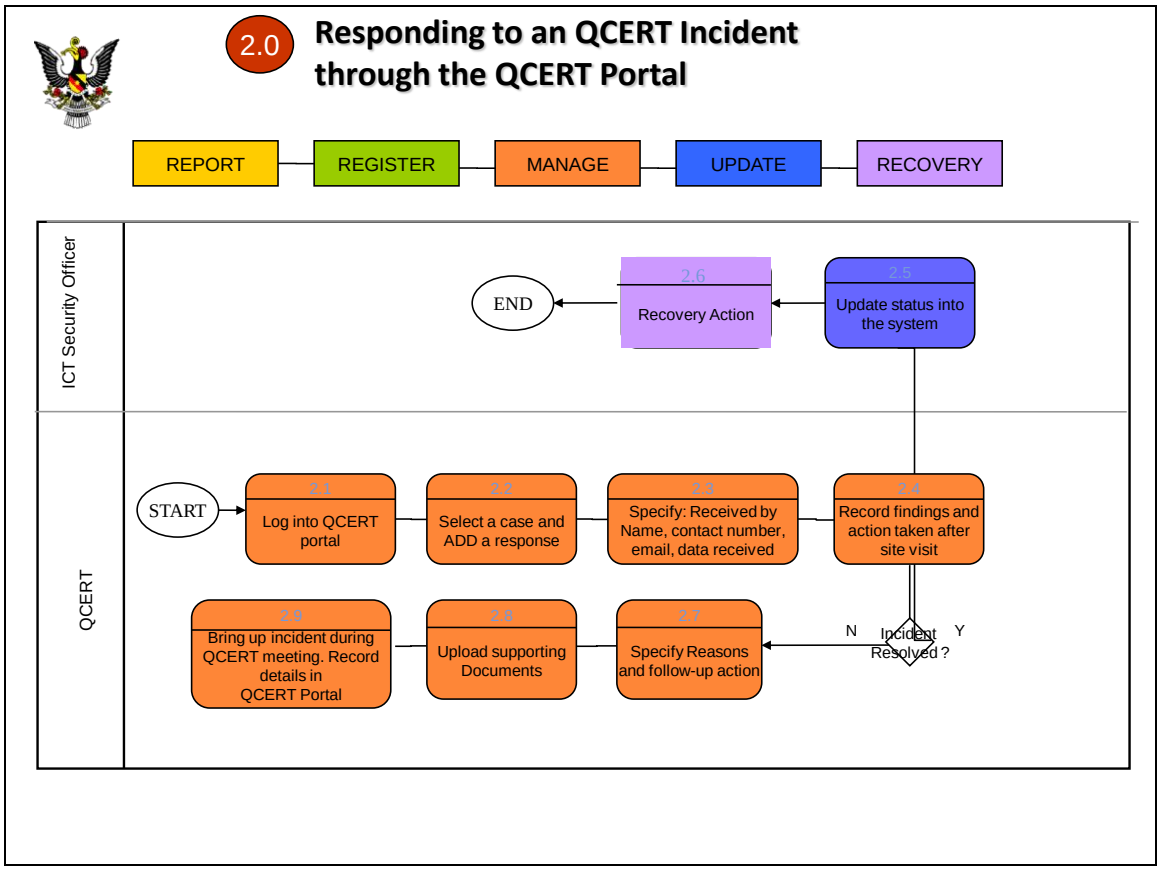
Tarikh: .....

Lampiran B

PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT Kerajaan Negeri




1.0
Reporting a Security Incident through the QCERT Portal.
REPORT
REGISTER
MANAGE
UPDATE
RECOVERY
PRISMA, MAMPU
1.1
Call / Email / Fax Incident to QCERT
ICTSO Agency & QCERT, SAINS
START
1.1
Log into QCERT Portal
1.2
Add an Incident. Case number will automatically be generated
1.3
Specify : Address, incident type, preliminary action, description, date of occurrence, severity level, and contact details
END
GCERT, MAMPU
1.1
Call / Email / Fax Incident to QCERT


2.0
Responding to an QCERT Incident through the QCERT Portal
REPORT
REGISTER
MANAGE
UPDATE
RECOVERY
ICT Security Officer
QCERT
END
2.6
Recovery Action
2.5
Update status into the system
START
2.1
Log into QCERT portal
2.2
Select a case and ADD a response
2.3
Specify: Received by Name, contact number, email, data received
2.4
Record findings and action taken after site visit
N
Incident Resolved ?
Y
2.7
Specify Reasons and follow-up action
2.8
Upload supporting Documents
2.9
Bring up incident during QCERT meeting. Record details in QCERT Portal

Lampiran C

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua penjawat awam Negeri:

(a) Surat Pekeliling ICT No.3/2012
Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 (ISMS) Dalam Sektor Awam Negeri

(b) Surat Pekeliling ICT No.4/2012
Penilaian Risiko Keselamatan Maklumat Sektor Awam Negeri

(c) Surat Pekeliling ICT No.5/2012
Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam

(d) Surat Pekeliling ICT No.1/2010
Capaian Internet Bagi Pegawai Sokongan (Gred 27-38), Jurutrengkas, Seetiausaha Sulit kepada Menteri dan Menteri Muda di Sektor Awam Kerajaan Negeri Sarawak

(e) Surat Pekeliling ICT No. 4/2008
Penggunaan Telefon Mudah Alih Blackberry

(f) Surat Pekeliling ICT No. 1/2008
Garis Panduan Mengenai Pembangunan Dan Penyelenggaraan Laman Web/Portal Kerajaan Negeri Sarawak

(g) Surat Pekeliling No. 2/2007
Penyediaan Piagam Pelanggan Di Laman Web/Portal Agensi Kerajaan

(h) Surat Pekeliling ICT No. 3/2007
Langkah-langkah Mengenai Penggunaan Mel Elektronik (E-MEL) Di Agensi-agensi Kerajaan

(i) Surat Pekeliling No. 1/2007
Pelaksanaan Dan Pemasangan Infrastruktur ICT Bagi Bangunan Kerajaan Negeri

(j) Surat Pekeliling No. 2/2006
Pelaksanaan Voice Over Internet Protocol (VOIP) dan Panggilan Telefon Berdiskaun (Discounted Call) untuk Kerajaan Negeri Sarawak

(k) Surat Pekeliling (Perj. Bil. 4/2000)
Mel Elektronik (EMel)

(l) Surat Pekeliling Bil. 40/2000
Laman Web Agensi Dan Capaian Internet

(m) Surat Pekeliling Np. 47/2006
Kata Laluan Tidak Dienkripsikan Di Dalam Pangkalan Data Komputer

(n) Surat Pekeliling No. 1/2006
Polisi Keselamatan ICT Negeri Sarawak – Pengurusan Keselamatan Komputer Peribadi (Desktop Security Management – DSM)

(o) Perintah-Perintah Am Negeri 1996

(p) Akta Hak Cipta 1997;

(q) Perintah-Perintah Am;

(r) Arahan Perbendaharaan;

Lampiran D

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang boleh dirujuk oleh semua penjawat awam Negeri:

(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 Kerajaan Negeri – Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

(j) Surat Arahan Ketua Pengarah Kerajaan Negeri – 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) Akta Tandatangan Digital 1997;

(m) Akta Rahsia Rasmi 1972;

(n) Akta Jenayah Komputer 1997;

(o) Akta Hak Cipta (Pindaan) Tahun 1997;

(p) Akta Komunikasi dan Multimedia 1998;

(q) Perintah-Perintah Am;

(r) Arahan Perbendaharaan;

(s) Arahan Teknologi Maklumat 2007;

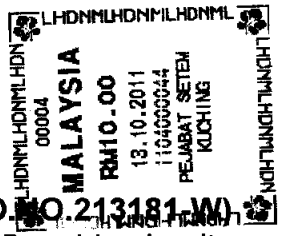
10

NONDISCLOSURE AGREEMENT

THIS AGREEMENT is made on the 25th day of April , 2011.

BETWEEN

THE STATE GOVERNMENT OF SARAWAK who for this purpose is represented by the Information and Communication Technology Unit (ICTU) of the Chief Minister's Department having an address at Level 4, Wisma Bapa Malaysia, 93502 Petra Jaya, Kuching, Sarawak (hereinafter referred to as "the State Government") of the first part;



AND

SARAWAK INFORMATION SYSTEMS SENDIRIAN BERHAD (CO.NO.213181-W) a company incorporated in Malaysia under the Companies Act, 1965 and having its principal place of business and registered address at Level 3, Wisma Bapa Malaysia, Petra Jaya, 93350Kuching, Sarawak (hereinafter referred to as "SAINS") of the second part.

1. PURPOSE

This Agreement is intended to protect all information and/or data transmitted by the State Government whether classified and/or unclassified which each party has disclosed and/or may further disclose in the future to the other party in the course of performing contractual obligations under the ICT Service Agreement executed between the State Government and SAINS.

2. DEFINITION OF CONFIDENTIAL INFORMATION

"Confidential Information" means any oral, written, graphic or machine-readable information including, but not limited to, that which relates to document, data, technology, plans, products, developments, inventions, processes, designs, drawings, formula, markets, software (including source and object code), hardware configuration, agreements with third parties, services, stakeholders, account or finances of the disclosing party, which Confidential Information is designated in writing to be confidential or proprietary or is reasonably understood to be confidential or proprietary, or if given orally, is confirmed in writing as having been disclosed as confidential or proprietary within a reasonable time (not to exceed thirty (30) days) after the oral disclosure.

3. NONDISLOSURE OF CONFIDENTIAL INFORMATION

(a) The State Government and SAINS each agree not to use any information whether classified or unclassified disclosed to it by the other party for its own use or for any purpose other than to carry out discussions concerning, and for the performance of the Agreement.

(b) Exceptions. Notwithstanding the above, neither party shall have liability to the other with regard to any Confidential Information of the other which the receiving party can prove:

(i) was in the public domain at the time it was disclosed or has entered the public domain through no fault of the receiving party;

(ii) was known to the receiving party, without restriction, at the time of disclosure, as demonstrated by files in existence at the time of disclosure;

(iii) is disclosed with the prior written approval of the disclosing party;

(iv) was independently developed by the receiving party without any use of the Confidential Information of the disclosing party and by employees of the receiving party who have not had access to the Confidential Information, as demonstrated by files created at the time of such independent development;

(v) becomes known to the receiving party, without restriction, from a source other than the disclosing party without breach of this Agreement by the receiving party and otherwise not in violation of the disclosing party's rights;

(vi) is disclosed pursuant to the order or requirement of a court, administrative agency, or other governmental body; provided, however, that the receiving party shall provide prompt notice of such court order or requirement to the disclosing party to enable the disclosing party to seek a protective order or otherwise prevent or restrict such disclosure.

4. RETURN OF MATERIALS.

Any materials or documents that have been furnished by one party to the other in connection with the Relationship shall be promptly returned by the receiving party, accompanied by all copies of such documentation, within ten (10) days after (a) the Relationship has been rejected or concluded or (b) the written request of the disclosing party.

5. NO RIGHTS GRANTED

Nothing in this Agreement shall be construed as granting any rights under any patent, copyright, trade secret, mask work or other intellectual property right of

either party, nor shall this Agreement grant either party any rights in or to the other party's Confidential Information other than the limited right to review such Confidential Information solely for the purpose of determining whether to enter into the Relationship.

6. TERM

The foregoing commitments of each party shall survive any termination of the Agreement between the parties, and shall continue for until all the information in respect of this Agreement is available in the public domain.

7. SUCCESSORS AND ASSIGNS

The terms and conditions of this Agreement shall inure to the benefit of and be binding upon the respective successors and assigns of the parties, provided that Confidential Information of the disclosing party may not be assigned without the prior written consent of the disclosing party unless the assignee shall be the successor entity to the assignor upon the dissolution of the assignor in its present form. Nothing in this Agreement, express or implied, is intended to confer upon any party other than the parties hereto or their respective successors and assigns any rights, remedies, obligations, or liabilities under or by reason of this Agreement, except as expressly provided in this Agreement.

8. SEVERABILITY

If one or more provisions of this Agreement are held to be unenforceable under applicable law, the parties agree to renegotiate such provision in good faith. In the event that the parties cannot reach a mutually agreeable and enforceable replacement for such provision, then (a) such provision shall be excluded from this Agreement, (b) the balance of the Agreement shall be interpreted as if such provision were so excluded and (c) the balance of the Agreement shall be enforceable in accordance with its terms.

9. INDEPENDENT CONTRACTORS

The State Government and SAINS are independent contractors, and nothing contained in this Agreement shall be construed to constitute the State Government and SAINS as partners, joint ventures, co-owners or otherwise as participants in a joint or common undertaking.

10. GOVERNING LAW

This Agreement and all acts and transactions pursuant hereto and the rights and obligations of the parties hereto shall be governed, construed and interpreted in

accordance with the laws of Malaysia, and to the exclusive jurisdiction and venue of the courts therein.

11. REMEDIES

The State Government and SAINS each agree that its obligations set forth in this Agreement are necessary and reasonable in order to protect the disclosing party and its business. The State Government and SAINS each expressly agree that due to the unique nature of the disclosing party's Confidential Information, monetary damages would be inadequate to compensate the disclosing party for any breach by the receiving party of its covenants and agreements set forth in this Agreement. Accordingly, the State Government and SAINS each agree and acknowledge that any such violation or threatened violation shall cause irreparable injury to the disclosing party and that, in addition to any other remedies that may be available, in law, in equity or otherwise, the disclosing party shall be entitled to obtain injunctive relief against the threatened breach of this Agreement or the continuation of any such breach by the receiving party, without the necessity of proving actual damages.

12. AMENDMENT AND WAIVER.

Any term of this Agreement may be amended by written agreement of the State Government and SAINS. Any amendment or waiver effected in accordance with this Section shall be binding upon the parties and their respective successors and assigns. Failure to enforce any provision of this Agreement by a party shall not constitute a waiver of any term hereof by such party.

13. COUNTERPARTS

This Agreement may be executed in two or more counterparts, each of which shall be deemed an original and all of which together shall constitute one instrument.

14. ENTIRE AGREEMENT

This Agreement is the product of both of the parties hereto, and constitutes the entire agreement between such parties pertaining to the subject matter hereof, and merges all prior negotiations and drafts of the parties with regard to the transactions contemplated herein. Any and all other written or oral agreements existing between the parties hereto regarding such transactions are expressly cancelled.

15. NO PUBLICITY

Neither the State Government nor SAINS shall, without the prior consent of the other party, disclose to any other person the fact that Confidential Information of the other party has been and/or may be disclosed under this Agreement, that discussions or negotiations are taking place between the State Government and SAINS, or any of the terms, conditions, status or other facts with respect thereto, except as required by law and then only with prior notice as soon as possible to the other party.

IN WITNESS WHEREOF the parties hereto have caused this Agreement to be executed in their respective names by their duly authorized representatives the day and year first above written.

SIGNED FOR AND ON BEHALF OF THE STATE GOVERNMENT

.....

Name: WILLIAM PATRICK NYIGOR
I.C No: 580702-13-5027
Designation: DIRECTOR

IN THE PRESENCE OF:-

.....

Name: GRACE HUONG SIEW HUNG
I.C No: 620624-13-5016
Designation: Ketua Penolong Pengarah

SIGNED FOR AND ON BEHALF OF SARAWAK INFORMATION SYSTEMS SDN. BHD.

.....

Name: TEO TIEN HIONG
I.C No: 480404-13-5047
Designation: Chief Executive Officer

IN THE PRESENCE OF:-

.....

Name: TEO LOON TONG
I.C No: 620201-13-5073
Designation: Chief Operating Officer