DASAR KESELAMATAN ICT
NEGERI SEMBILAN DARUL KHUSUS

OGOS 2015
VERSI 2.1

OLEH:
UNIT PENGURUSAN TEKNOLOGI MAKLUMAT
PEJABAT SETIAUSAHA KERAJAAN
NEGERI SEMBILAN DARUL KHUSUS
BLOK B, TINGKAT 3, WISMA NEGERI
70503 SEREMBAN

ISI KANDUNGAN

PENGENALAN

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

OBJEKTIF

Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan diwujudkan untuk menjamin kesinambungan urusan Pentadbiran Kerajaan Negeri Sembilan dengan meminimumkan kesan insiden keselamatan ICT.

Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi Pentadbiran Kerajaan Negeri Sembilan. Ini hanya boleh dicapai dengan memastikan semua Aset ICT dilindungi.

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

a. Memastikan kelancaran operasi Pentadbiran Kerajaan Negeri Sembilan dan meminimumkan kerosakan atau kemusnahan;

b. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

c. Mencegah salah guna atau kecurian Aset ICT Kerajaan; dan

d. Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan merupakan 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 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 betul;

c. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

d. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat daripada sumber yang sah.

Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk

menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan.

Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

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

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

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

d. Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan

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

Selain daripada 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 Pentadbiran Kerajaan Negeri Sembilan terdiri daripada perkakasan, perisian, aplikasi sistem, perkhidmatan, data, maklumat, manusia, media storan, dokumentasi, premis komputer dan peralatan rangkaian. Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan 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 Pentadbiran Kerajaan Negeri Sembilan ini merangkumi perlindungan semua bentuk maklumat kerajaan yang diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan serta prosedur dalam pengendalian semua perkara-perkara berikut:

a. Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan Pentadbiran Kerajaan Negeri Sembilan. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

b. Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan 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 Pentadbiran Kerajaan Negeri Sembilan ;

c. Aplikasi Sistem

Satu program komputer yang dibangunkan untuk melakukan tugasan pengguna secara specifik untuk pengguna akhir komputer (*end users*).

d. 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.

e. Data atau Maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif Pentadbiran Kerajaan Negeri Sembilan. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod Pentadbiran Kerajaan Negeri Sembilan, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

f. Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian Pentadbiran Kerajaan Negeri Sembilan bagi mencapai misi dan objektif jabatan. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan;

g. Media Storan

Semua media storan dan peralatan yang berkaitan seperti storan, storan mudah alih dan pemacu storan;

h. Dokumentasi

Dokumen yang berkaitan dengan Aset ICT, pemasangan dan pengoperasian dan perisian, samada dalam bentuk elektronik atau bukan elektronik;

i. Peralatan Rangkaian

Peralatan rangkaian atau peranti rangkaian komputer berfungsi sebagai pengantara data dalam rangkaian komputer. Peralatan rangkaian termasuklah *switch, core switch* dan *firewall*; dan

j. Premis Komputer Dan Komunikasi

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

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

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan 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 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 dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;
v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan, dan;
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

d. Pengasingan

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

e. Pengauditan

Pengauditan merupakan 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 Pentadbiran Kerajaan Negeri Sembilan 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.

PENILAIAN RISIKO KESELAMATAN ICT

Pentadbiran Kerajaan Negeri Sembilan hendaklah mengambil kira kewujudan risiko ke atas Aset ICT akibat daripada ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu Pentadbiran Kerajaan Negeri Sembilan perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko Aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas Aset ICT.

Pentadbiran Kerajaan Negeri Sembilan hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada

perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat Pentadbiran Kerajaan Negeri Sembilan termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

Pentadbiran Kerajaan Negeri Sembilan bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

Pentadbiran Kerajaan Negeri Sembilan perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

b. Menerima dan/ atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan jabatan;

c. Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/ atau mencegah berlakunya risiko; dan

d. Memindahkan risiko kepada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

BIDANG 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101 Dasar Keselamatan ICT

Objektif:

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat dan Aset ICT selaras dengan keperluan Kerajaan Negeri Sembilan dan perundangan yang berkaitan.

010101 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Setiausaha Kerajaan Negeri Sembilan selaku Pemilik Aset ICT dan Pengerusi Mesyuarat Jawatankuasa Pemandu ICT Kerajaan Negeri Sembilan (JPICTNS). Ahli JPICTNS ini terdiri daripada senarai di 020108. Pelaksanaan dasar ini hendaklah disokong oleh prosedur-prosedur yang lebih terperinci untuk memastikan keberkesanan penyataan dasar.	Setiausaha Kerajaan Negeri Sembilan dan CIO

010102 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua pengguna ICT Pentadbiran Kerajaan Negeri Sembilan	ICTSO

termasuk kakitangan, pembekal, pakar runding dan lain-lain.	
010103 Penyelenggaraan Dasar	
Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan: a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Ke muka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT Kerajaan Negeri Sembilan (JPICTNS); c. Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh Mesyuarat Jawatankuasa Pemandu ICT Kerajaan Negeri Sembilan (JPICTNS); dan	JPICTNS dan ICTSO

d. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali dalam tempoh satu (1) tahun atau mengikut keperluan semasa.	
010104 Pengecualian Dasar	
Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan adalah terpakai kepada semua pengguna ICT Pentadbiran Kerajaan Negeri Sembilan dan tiada pengecualian diberikan.	Pengguna

BIDANG 02 ORGANISASI KESELAMATAN

0201 Struktur Organisasi Dalaman

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan.

020101 Setiausaha Kerajaan Negeri

Setiausaha Kerajaan Negeri adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut:	Setiausaha Kerajaan Negeri Sembilan
a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan;	
b. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan;	
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 Pentadbiran Kerajaan Negeri Sembilan; dan e. Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT Kerajaan Negeri Sembilan (JPICTNS).	
020102 Ketua Pegawai Maklumat (CIO)	
Ketua Pegawai Maklumat atau *Chief Information Officer* (CIO) bagi Pentadbiran Kerajaan Negeri Sembilan ialah Timbalan Setiausaha Kerajaan Negeri (Pengurusan), Pihak Berkuasa Tempatan ialah Yang DiPertua dan Badan Berkanun Negeri ialah Ketua Jabatan masing-masing. Peranan dan tanggungjawab CIO adalah seperti berikut : a. Memperkasakan tadbir urus keselamatan ICT Jabatan; b. Merancang pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan serta pengurusan risiko dan	CIO

pengauditan; dan c. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan.	
020103 Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) bagi Pentadbiran Kerajaan Negeri Sembilan ialah ialah Ketua Jabatan ICT di jabatan masing-masing. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut : a. Mengurus keseluruhan program-program keselamatan ICT; b. Menguatkuasakan pelaksanaan Dasar Keselamatan ICT; c. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT kepada semua pengguna; d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT; e. Menjalankan pengurusan risiko; f. Menjalankan audit, mengkaji semula, merumus	ICTSO

	tindak balas pengurusan Pentadbiran Kerajaan Negeri Sembilan berdasarkan hasil penemuan dan menyediakan laporan mengenainya;	
g.	Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;	
h.	Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (CERTNS), Pentadbiran Kerajaan Negeri Sembilan dan memaklumkannya kepada CIO;	
i.	Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;	
j.	Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT;	
k.	Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; dan	
l.	Bertanggungjawab sebagai Koordinator Pengurusan Pelan Pemulihan Bencana/ *Disaster*	

Recovery Plan (DRP) Pentadbiran Kerajaan Negeri Sembilan.	
020104 Pengurus ICT	
Pengurus ICT merupakan pegawai yang bertanggungjawab menguruskan keselamatan ICT di bawah kawalannya. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Pentadbiran Kerajaan Negeri Sembilan; b. Menentukan kawalan akses pengguna terhadap Aset ICT Pentadbiran Kerajaan Negeri Sembilan; c. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; d. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan; dan e. Bertanggungjawab terhadap pemilikan aset ICT bagi pihak Kerajaan Negeri.	Pengurus ICT
020105 Pentadbir Sistem ICT	

Pentadbir Sistem ICT bagi Pentadbiran Kerajaan Negeri Sembilan ialah Pentadbir Sistem ICT di Jabatan. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a. Mengambil tindakan dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan; c. Memantau aktiviti capaian harian sistem aplikasi pengguna; d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e. Menganalisis dan menyimpan rekod jejak audit; dan f. Menyediakan laporan mengenai aktiviti capaian secara berkala.	Pentadbir Sistem ICT

020106 Pegawai Aset	
Pegawai Aset adalah pegawai yang telah dilantik oleh Jawatankuasa Pengurusan Aset (JKPAK)/ Ketua Jabatan. Peranan dan tanggungjawab Pegawai Aset adalah seperti berikut: a. Menguruskan pendaftaran dan pelupusan Aset ICT; b. Bertanggungjawab terhadap kesiapsediaan, selenggaraan dan keselamatan aset untuk kegunaan harian; dan c. Bertanggungjawab memantau perkakasan ICT yang diagihkan kepada pengguna.	Pegawai Aset
020107 Pengguna	
Pengguna mempunyai peranan dan tanggungjawab seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;	Pengguna

c. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; d. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan dan menjaga kerahsiaan maklumat Pentadbiran Kerajaan Negeri Sembilan; e. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; f. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan g. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan sebagaimana Lampiran 1.	
020108 Jawatan Kuasa Pemandu ICT Negeri Sembilan (JPICTNS)	
Jawatankuasa Pemandu ICT Kerajaan Negeri Sembilan (JPICTNS) merupakan jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan.	JPICTNS

Keanggotaan JPICTNS adalah seperti berikut:

Pengerusi:
Setiausaha Kerajaan Negeri

Ahli :

1. Pegawai Kewangan Negeri
2. Timbalan Setiausaha Kerajaan Negeri (Pembangunan)
3. Timbalan Setiausaha Kerajaan Negeri (Pengurusan)/ Ketua Pegawai Maklumat (*Chief Information Officer*-CIO) Kerajaan Negeri Sembilan
4. Ketua-ketua Jabatan Teknikal Negeri
5. Pengurus ICT Negeri
6. Pegawai Keselamatan ICT Negeri
7. Perunding ICT (MAMPU)
8. Pengarah ICT, Pusat Data Negara dan Inovasi (NADI), ICU Jabatan Perdana Menteri
9. Wakil Pegawai ICT (MAMPU)

Urus Setia bagi Jawatankuasa Pemandu ICT Kerajaan Negeri Sembilan (JPICTNS) ialah Unit Pengurusan Teknologi Maklumat (UPTM). Bidang kuasa JPICTNS adalah seperti berikut

a. Menetapkan arah tuju dan strategi untuk pelaksanaan ICT Kerajaan Negeri;

b. Merancang, mengenal pasti dan mencadangkan sumber kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/ strategi ICT kementerian; c. Merancang dan menyelaras pelaksanaan program/ projek ICT Jabatan Kerajaan Negeri supaya selaras dengan Pelan Strategik ICT Kerajaan Negeri; d. Menyelaras dan menyeragamkan pelaksanaan ICT antara jabatan Kerajaan Negeri dengan Pelan Strategik ICT (ISP) Pejabat Setiausaha Kerajaan Negeri Sembilan; e. Mempromosi dan menggalakkan perkongsian pintar projek-projek ICT antara semua Jabatan Kerajaan Negeri; f. Merancang dan menentukan langkah-langkah keselamatan ICT; g. Memantau perkembangan program ICT jabatan Kerajaan Negeri serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT;	

h. Meluluskan perolehan ICT bagi jabatan Negeri Sembilan berdasarkan keperluan sebenar dengan perbelanjaan yang berhemah; i. Menyelaras pelaksanaan projek ICT Jabatan Kerajaan Negeri Sembilan; dan j. Menyelaras pelaksanaan program merapatkan jurang digital peringkat negeri.	
020109 Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan Negeri Sembilan (CERTNS)	
Pasukan CERTNS ditubuhkan bagi membantu mengedalikan insiden keselamatan ICT, mengawasi dan memberi nasihat berkaitan keselamatan ICT kepada agensi-agensi di bawah kawalannya. Keanggotaan CERTNS adalah seperti berikut: GCERT Pengarah : Pengarah Unit Pengurusan Teknologi Maklumat Pengurus : Penolong Pengarah (Kanan) (Operasi dan	CERTNS

	Rangkaian), Unit Pengurusan Teknologi Maklumat Ahli Tetap: 1. Penolong Pengarah (Keselamatan), Unit Pengurusan Teknologi Maklumat 2. Penolong Pengarah (Rangkaian), Unit Pengurusan Teknologi Maklumat 3. Penolong Pegawai Teknologi Maklumat (Keselamatan), Unit Pengurusan Teknologi Maklumat 4. Penolong Pegawai Teknologi Maklumat (Rangkaian), Unit Pengurusan Teknologi Maklumat 5. Pegawai Teknologi Maklumat, Pejabat Tanah dan Galian 6. Pegawai Teknologi Maklumat, Pejabat Bendahari Negeri Ahli Dilantik: 1. Wakil Pihak Berkuasa Tempatan 2. Wakil Pejabat Tanah dan Daerah 3. Wakil Agensi Peranan dan tanggungjawab CERTNS adalah seperti berikut: a. Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden;	

b. Merekodkan dan menjalankan siasatan awal insiden yang diterima; c. Menangani tindak balas insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d. Menasihati agensi di bawah Pentadbiran Kerajaan Negeri Sembilan supaya mengambil tindakan pemulihan dan pengukuhan; dan e. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada Pentadbiran Kerajaan Negeri Sembilan.	
0202 Pihak Ketiga	
Objektif: Menjamin keselamatan semua Aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).	
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Ini bertujuan memastikan penggunaan Aset ICT, penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga

Sembilan; b. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d. Akses kepada Aset ICT Pentadbiran Kerajaan Negeri Sembilan perlu berlandaskan kepada prosedur-prosedur keselamatan yang berkaitan; e. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan dalam perjanjian yang dimeterai. i. Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan; ii. *Non-Disclosure Agreement* (NDA); dan iii. Perakuan Akta Rahsia Rasmi 1972; f. Membaca, memahami dan menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan seperti Lampiran 1.	

BIDANG 03 PENGURUSAN ASET

0301 Akauntabiliti Aset

Objektif:
Memberi dan menyokong perlindungan yang sepatutnya ke atas semua Aset ICT pelbagai jabatan di bawah Pentadbiran Kerajaan Negeri Sembilan.

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, direkodkan dalam Borang Daftar Harta Modal/ Borang Daftar Harta Inventori dan sentiasa dikemas kini selaras dengan Pekeliling Perbendaharaan Bil.5 Tahun 2007 : Tatacara Pengurusan Aset Alih Kerajaan;	Pegawai Aset dan Pengguna

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 semua jabatan di bawah Pentadbiran Kerajaan Negeri Sembilan; d. Peraturan bagi pengendalian Aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan oleh Pegawai Aset; e. Setiap pengguna adalah bertanggungjawab ke atas semua Aset ICT di bawah kawalannya termasuk Aset ICT yang dipinjamkan; f. Pengguna yang dibekalkan dengan Aset ICT bertanggungjawab melaporkan kerosakan kepada Pegawai Aset; dan g. Ketua Jabatan atau pegawai bertanggungjawab hendaklah membuat laporan polis dengan segera, tidak lewat dari 24 jam selepas berlaku kehilangan.	
0302 Pengelasan dan Pengendalian Maklumat	
Objektif: Memastikan setiap maklumat atau Aset ICT diberikan tahap perlindungan	

yang bersesuaian.	
030201 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan hendaklah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a. Rahsia Besar b. Rahsia; c. Sulit; atau d. Terhad.	Pengguna
030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat	Pentadbir Sistem ICT dan Pengguna

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

BIDANG 04 KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia Dalam Tugasan Harian

Objektif:

Memastikan semua sumber manusia yang terlibat di bawah Pentadbiran Kerajaan Negeri Sembilan dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan, meningkatkan pengetahuan dalam keselamatan Aset ICT serta mematuhi terma dan syarat perkhidmatan.

040101 Sebelum Perkhidmatan

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. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan di bawah Pentadbiran Kerajaan Negeri Sembilan serta pihak ketiga yang terlibat dalam menjamin keselamatan Aset ICT sebelum, semasa dan selepas perkhidmatan;	Pentadbir Sistem ICT dan Pengguna

b. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan di bawah Pentadbiran Kerajaan Negeri Sembilan serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; c. Memenuhi keperluan prosedur keselamatan (NDA) bagi pihak ketiga yang berkepentingan selaras dengan keperluan perkhidmatan; dan d. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	
040102 Dalam Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan pegawai dan kakitangan di bawah Pentadbiran Kerajaan Negeri Sembilan serta pihak ketiga yang berkepentingan mengurus keselamatan Aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Pentadbiran Kerajaan Negeri Sembilan atau jabatan yang berkenaan;	Pentadbir Sistem ICT dan Pengguna

b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan Aset ICT diberi kepada pengguna ICT di bawah Pentadbiran Kerajaan Negeri Sembilan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;

c. Memastikan adanya proses tindakan disiplin dan/ atau undang-undang ke atas pegawai dan kakitangan di bawah Pentadbiran Kerajaan Negeri Sembilan serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh Pentadbiran Kerajaan Negeri Sembilan atau jabatan yang berkenaan; dan

d. Memantapkan pengetahuan berkaitan dengan penggunaan Aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Pengurusan Sumber Manusia, Pejabat Setiausaha Kerajaan Negeri Sembilan atau jabatan yang

berkenaan.	
040103 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan semua Aset ICT dikembalikan kepada pegawai yang dipertanggungjawabkan di bawah jabatan yang berkenaan mengikut peraturan dan/ atau terma perkhidmatan yang ditetapkan; b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh Pentadbiran Kerajaan Negeri Sembilan atau jabatan yang berkenaan; dan/ atau terma perkhidmatan.	Pentadbir Sistem ICT, Pegawai Aset dan Pengguna

BIDANG 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 Keselamatan Kawasan

Objektif:

Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

050101 Kawalan Kawasan

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat jabatan. Perkara-perkara yang perlu 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; contoh: Bilik server. b. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;	CIO dan ICTSO

c. Memasang alat penggera atau kamera litar tertutup (CCTV); d. Menghadkan jalan keluar masuk; e. Mengadakan kaunter kawalan; f. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; g. Mewujudkan perkhidmatan kawalan keselamatan; h. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; i. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; j. Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau dan bencana; k. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan l. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya	

050102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Setiap pegawai dan kakitangan di bawah Pentadbiran Kerajaan Negeri Sembilan hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Semua pas keselamatan hendaklah diserahkan balik kepada ketua jabatan apabila pegawai dan kakitangan berhenti atau bersara; c. Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan d. Kehilangan pas hendaklah dilaporkan dengan segera.	Pentadbir Sistem ICT dan Pengguna
050103 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi Aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di Jabatan Pentadbiran Kerajaan Negeri adalah Bilik Ketua Jabatan, Bilik Timbalan Ketua Jabatan, Bilik Server, *Disaster Recovery*	Pengurus ICT, Pentadbir Sistem ICT, Pihak Ketiga dan Pengguna

Centre (DRC) dan Pusat Data (*Data Centre*). Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja. Pihak ketiga dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal. Mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	
0502 Keselamatan Peralatan	
Objektif: Melindungi peralatan ICT jabatan daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
050201 Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna;	CIO, Pentadbir Sistem ICT, Pegawai Aset dan Pengguna

b. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f. Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;	

i. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); j. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; k. Semua peralatan yang digunakan secara berterusan hendaklah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; l. Peralatan ICT yang hendak dibawa keluar dari premis jabatan perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan; m. Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera; n. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; o. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;	

p. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk di baik pulih; q. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; r. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; s. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT; t. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; dan u. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.	
050202 Media Storan	
Media storan perlu berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan	Pengguna

kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan 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 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 termasuk tahan daripada dipecahkan, api, air dan medan magnet; e. Akses dan pergerakan media storan hendaklah direkodkan; f. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; g. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan	

data. Satu salinan pendua harus disimpan di bangunan berbeza dan di luar jabatan; h. Semua media storan data yang hendak dilupuskan hendaklah dihapuskan dengan teratur dan selamat; i. Penghapusan maklumat atau kandungan media hendaklah mendapat kelulusan pemilik maklumat terlebih dahulu; dan j. Pegawai dan kakitangan Pentadbiran Kerajaan Negeri Sembilan hendaklah bertanggungjawab sepenuhnya dalam membuat salinan fail kerja harian ke dalam media storan peribadi.	
050203 Media Tandatangan Digital	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pegawai dan kakitangan Pentadbiran Kerajaan Negeri Sembilan 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	Pengguna

c. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada penyedia perkhidmatan untuk tindakan seterusnya.	
050204 Media Perisian dan Aplikasi (*Software*)	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan di jabatan; b. Sistem aplikasi dalaman tidak dibenarkan di demonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c. Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada *CD-rom*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan d. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan hendaklah mengikut prosedur yang ditetapkan.	Pengurus ICT, Pentadbir Sistem ICT dan Pegawai Aset
050205 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan	Pengurus ICT dan Pegawai

dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b. Memastikan perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; f. Semua penyelenggaraan hendaklah mendapat kebenaran daripada Pengurus ICT; dan g. Merekod kerja-kerja penyelenggaraan di dalam kad harta modal mengikut tatacara pengurusan aset.	Aset

050206 Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari premis jabatan adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan perlu dilindungi dan dikawal sepanjang masa; b. Penyimpanan atau penempatan peralatan hendaklah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan c. Setiap peralatan yang dibawa keluar premis hendaklah direkodkan.	Pegawai Aset dan Pengguna
050207 Pelupusan Perkakasan	
Pelupusan peralatan ICT perlu dilakukan secara terkawal mengikut prosedur pelupusan semasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran;	Pengguna, Pegawai Aset

b. Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat penduaan (*backup*);

c. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

d. Peralatan yang hendak di lupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan;

e. Data-data yang terkandung dalam storan peralatan ICT yang akan dilupuskan sebelum dipindah-milik perlu dihapuskan dengan cara yang selamat;

f. Pegawai Aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam kad harta modal mengikut tatacara pengurusan aset;

g. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan

h. Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:

1. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan

perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; 2. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di premis jabatan; 3. Memindah keluar dari premis jabatan mana-mana peralatan ICT yang hendak dilupuskan; 4. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab jabatan; dan 5. Pengguna bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
0503 Keselamatan Persekitaran	
Objektif: Melindungi Aset ICT jabatan daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050301 Kawalan Persekitaran	

Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan Aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari Aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer;	Pengguna

g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan h. Akses kepada saluran *riser* hendaklah sentiasa dikunci.	
050302 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	ICTSO

050303 Kabel Komputer/ Rangkaian	
Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Menggunakan kabel komputer/ rangkaian yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel komputer/ rangkaian daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel komputer/ rangkaian sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; d. Kabel rangkaian perlu dilabelkan dengan jelas dan hendaklah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat; dan e. Penambahan/ penyelenggaraan kabel rangkaian perlu melalui Pentadbir Sistem ICT.	ICTSO dan Pentadbir Sistem ICT
050304 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pegawai Keselamatan Jabatan

a. Setiap Pegawai dan kakitangan Pentadbiran Kerajaan Negeri Sembilan hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan yang dikeluarkan oleh Pegawai Keselamatan Jabatan; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik.	

0504 Keselamatan Dokumen

Objektif:
Melindungi maklumat jabatan daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.

050401 Dokumen

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;	Pengguna

b. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; c. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; d. Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan e. Semua dokumen terperingkat yang disediakan dan dihantar secara elektronik perlu menggunakan kaedah enkripsi (*encryption*).	

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur pengurusan operasi yang di diguna pakai hendaklah didokumen, disimpan dan dikawal; dan b. Setiap prosedur hendaklah mengandungi arahan-arahan yang jelas, teratur, lengkap dan hendaklah dikemas kini mengikut keperluan.	Pentadbir Sistem ICT

060102 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	

a. Peningkatan atau pengubahsuaian yang melibatkan perkakasan, perisian, sistem rangkaian, sistem aplikasi, dan prosedur hendaklah mendapat kebenaran daripada pegawai atasan; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen Aset ICT hendaklah dikendalikan oleh pegawai atau pihak yang diberi kebenaran; c. Semua aktiviti pengubahsuaian Aset ICT hendaklah mematuhi spesifikasi yang telah ditetapkan; dan d. Semua aktiviti peningkatan dan pengubahsuaian hendaklah direkod untuk tujuan kawalan dan semakan semula.	Pengurus ICT, Pentadbir Sistem ICT dan Pegawai Aset
060103 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

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 atau di manipulasi; dan c. Perkakasan yang digunakan bagi tujuan pembangunan sistem aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai produksi.	
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Objektif: Memastikan penyampaian perkhidmatan pihak ketiga selaras dengan kontrak perjanjian dan prosedur.	
060201 Penyampaian Perkhidmatan	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a. Memastikan skop perkhidmatan dan tahap penyampaian yang terkandung dalam kontrak	Pengurus ICT, Pentadbir Sistem ICT, dan Pihak Ketiga

perjanjian dipatuhi dan dilaksanakan oleh pihak ketiga; dan b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit oleh pegawai yang bertanggungjawab.	
0603 Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko gangguan dan kegagalan sistem.	
060301 Perancangan Kapasiti	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang bertanggung jawab pada masa akan datang. Perancangan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko gangguan dan kegagalan perkhidmatan serta kerugian akibat pengubahsuaian yang tidak dirancang.	Pengurus ICT dan Pentadbir Sistem ICT

060302 Penerimaan Sistem	
a. Semua sistem baharu dan diubah suai hendaklah memenuhi spesifikasi yang ditetapkan sebelum diterima pakai; b. Semua sistem baharu dan yang diubah suai hendaklah melalui peringkat pengujian *User Acceptance Test (UAT), Provisional Acceptance Test (PAT) & Final Acceptance Test (FAT)* sebelum dilaksanakan secara rasmi; dan c. Dokumentasi sistem perlu disediakan, dikemas kini mengikut kawalan versi dan dibuat salinan serta disimpan di tempat yang selamat.	Pentadbir Sistem ICT
0604 Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya.	
060401 Perlindungan daripada Perisian Berbahaya	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pengurus ICT, Pentadbir

a. Memasang sistem keselamatan seperti *antivirus*, *Intrusion Detection System (IDS)* dan *Intrusion Prevention System* (IPS) yang bersesuaian mengikut prosedur penggunaan yang betul dan selamat; b. Menggunakan perisian yang dan dilindungi di bawah undang-undang bertulis yang berkuat kuasa; c. Mengimbas media storan dengan anti virus terkini sebelum menggunakannya; d. Mengemas kini *patches* sistem operasi mengikut keperluan. e. Menyemak fail sistem dan pangkalan data; f. Memasukkan klausa tuntutan baik pulih dalam kontrak perjanjian. g. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan h. Memaklumkan pengguna mengenai ancaman keselamatan ICT seperti serangan virus.	Sistem ICT dan Pengguna

060402 Perlindungan daripada *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pengurus ICT dan Semua
0605 Housekeeping	
Objektif: Meningkatkan prestasi perkakasan dan pangkalan data bagi memastikan keboleh sediaan data dan maklumat.	
060501 *Backup*	
Proses salinan sistem aplikasi, data dan fail konfigurasi bagi memastikan sistem dapat beroperasi semula sekiranya diperlukan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Melaksanakan *backup* ke atas semua sistem aplikasi dan fail konfigurasi; b. Melaksanakan *backup* ke atas semua data secara berkala;	Pentadbir Sistem ICT dan Semua

c. Menguji fail *backup* melalui prosedur *restore* bagi memastikan ianya berfungsi dengan baik; dan d. Merekod dan menyimpan salinan *backup* di lokasi yang selamat.	
0606 Pengurusan Rangkaian	
Objektif: Melindungi infrastruktur rangkaian dan maklumat.	
060601 Kawalan Infrastruktur Rangkaian	
Infrastruktur rangkaian hendaklah dikawal dan diuruskan bagi mengelakkan ancaman ke atas sistem aplikasi dan data. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan rangkaian hendaklah diletakkan di lokasi yang selamat; b. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh pegawai yang bertangungjawab; c. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan jabatan;	Pengurus ICT dan Pentadbir Sistem ICT

d. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; e. Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat jabatan. f. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; g. Sebarang penyambungan rangkaian yang bukan di bawah kawalan jabatan adalah tidak dibenarkan; h. Penggunaan *modem, access point dan wireless broadband* hendaklah mendapat kebenaran ICTSO; i. Pemasangan peralatan rangkaian dan keselamatan lain yang bersesuaian digalakkan.	
0607 Pengurusan Media	
Objektif: Melindungi Aset ICT daripada ancaman yang menyebabkan gangguan	

terhadap perkhidmatan.	
060701 Pengendalian Media	
a. Penghantaran atau pemindahan media ke lokasi lain di luar pejabat hendaklah direkodkan dan mengikut jadual yang telah ditetapkan; b. Mengawal dan merekodkan aktiviti pengendalian media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; c. Menyimpan semua media di tempat yang selamat; dan d. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan hendaklah dilupuskan mengikut prosedur yang betul dan selamat.	Pegawai Aset dan Pengguna
060702 Keselamatan Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan dokumentasi adalah seperti berikut: a. Menyedia dan memantapkan keselamatan dokumentasi;	Pengurus ICT dan Pentadbir Sistem ICT

b. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; dan c. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	

0608 Pengurusan Pertukaran Maklumat

Objektif:

Memastikan pertukaran maklumat di antara jabatan dan agensi luar adalah selamat dan terjamin.

060801 Pertukaran Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan	Pengurus ICT dan Pentadbir Sistem ICT

semasa pemindahan keluar dari premis jabatan; dan c. Maklumat yang terdapat dalam mel elektronik perlu dilindungi.	
060802 Pengurusan Mel Elektronik (E-mel)	
Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: a. Pengguna e-mel di jabatan hendaklah mematuhi etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*" b. Jabatan perlu menyediakan polisi, prosedur atau arahan-arahan bertulis yang bersesuaian mengenai penggunaan e-mel.	Pentadbir Sistem ICT dan Pengguna
0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)	
Objektif: Mengawal sensitiviti aplikasi dan maklumat agar sebarang risiko dapat dielakkan.	

060901 E-Dagang	
E-Dagang ialah perniagaan atau perdagangan yang menggunakan ICT sebagai medium untuk tujuan komunikasi dan juga transaksi. Perkara-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 atau pengulangan 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.	Pengurus ICT dan Pengguna

0610 Pemantauan

Objektif:
Memastikan Aset ICT bebas daripada ancaman.

061001 Pengauditan dan Forensik ICT

Pegawai yang bertanggungjawab hendaklah merekod dan menganalisis/ melaporkan perkara-perkara berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT jabatan; b. Pengubahsuaian sesebuah sistem ICT tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; c. Insiden keselamatan ICT jabatan; d. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e. Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*); f. Aktiviti penyalahgunaan akaun e-mel;	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

g. Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran; dan h. Larangan memuat turun dan instalasi permainan komputer *(games)*, *hacking tools*, atau *streaming* video/ audio dan perisian yang tidak dibenarkan.	
061002 Jejak Audit	
Setiap sistem ICT hendaklah mempunyai jejak audit (*audit trail*). Jejak audit hendaklah mengandungi maklumat-maklumat berikut: a. Rekod bagi setiap aktiviti transaksi; b. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; c. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan; d. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara; e. Jejak audit perlu dilindungi daripada kerosakan, kehilangan, penghapusan,	Pentadbir Sistem ICT

pemalsuan dan pengubahsuaian yang tidak dibenarkan; dan f. Jabatan perlu menyediakan polisi, prosedur atau arahan-arahan bertulis yang bersesuaian.	
061003 Sistem Log	
Pegawai yang bertanggung jawab hendaklah melaksanakan perkara-perkara berikut: a. Mewujudkan fail log bagi merekodkan semua aktiviti harian pengguna; b. Menyemak sistem log secara berkala bagi mengesan ancaman yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera~~;~~ c. Pegawai yang bertanggung jawab hendaklah melaporkan kepada ICTSO dan CIO terhadap sebarang insiden keselamatan. d. Melakukan *housekeeping* sistem log secara berkala.	Pentadbir Sistem ICT
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. Maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; c. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan, dianalisis dan diambil tindakan sewajarnya; dan d. Penentuan masa bagi sistem aplikasi perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	Pengurus ICT dan Pentadbir Sistem ICT

BIDANG 07 KAWALAN CAPAIAN

0701 Dasar Kawalan Capaian

Objektif:
Mengawal capaian ke atas Aset ICT

070101 Keperluan Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. , Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Kawalan capaian ke atas Aset ICT mengikut keperluan keselamatan dan peranan pengguna; b. Kawalan capaian ke atas perkhidmatan semua jenis rangkaian (tanpa wayar dan berwayar) dalaman dan luaran;	Pengurus ICT dan Pentadbir Sistem ICT

c. Kawalan capaian maklumat menggunakan kemudahan atau peralatan mudah alih; dan d. Kawalan ke atas kemudahan pemprosesan maklumat seperti server, komputer peribadi dan komputer riba.	
0702 Pengurusan Capaian Pengguna	
Objektif: Mengawal capaian pengguna ke atas Aset ICT.	
070201 Akaun Pengguna	
Setiap pengguna adalah bertanggungjawab ke atas Aset ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara berikut hendaklah dipatuhi: a. Akaun yang diberikan oleh Pentadbir Sistem ICT sahaja boleh digunakan; b. Akaun pengguna yang diwujudkan hendaklah unik dan mendapat kelulusan daripada Pentadbir Sistem ICT; c. Pemilikan akaun pengguna bukanlah hak milik mutlak;	Pentadbir Sistem ICT dan Pengguna

d. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan e. Pentadbir Sistem ICT boleh membeku atau menamatkan akaun pengguna atas sebab-sebab berikut: i. Pengguna yang tidak aktif melebihi enam (6) bulan; ii. Bertukar bidang tugas kerja; iii. Bertukar ke jabatan lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	
070202 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
070203 Pengurusan Kata Laluan	
Pengurusan kata laluan hendaklah mematuhi	Pentadbir Sistem ICT dan

prosedur yang ditetapkan seperti berikut: a. Kata laluan hendaklah dilindungi dan tidak boleh dikongsi; b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran; c. Panjang kata laluan hendaklah sekurang-kurangnya dua belas (12) aksara dengan gabungan huruf, angka dan aksara khusus; d. Kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan; e. Kata laluan log masuk komputer dan screen saver hendaklah diaktifkan; f. Kata laluan hendaklah tidak dipaparkan semasa input; g. Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas kata laluan diset semula; h. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i. Kata laluan hendaklah ditukar sekurang-kurangnya sekali dalam tempoh enam (6) bulan;	Pengguna

j. Mengelakkan penggunaan semula kata laluan yang terdahulu; dan k. Kata laluan pengguna hendaklah melalui proses enkripsi apabila disimpan di dalam pangkalan data.	
070204 *Clear Desk* dan *Clear Screen*	
Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja atau di paparan skrin apabila pengguna tidak berada di tempatnya. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan kemudahan *password screen saver*, *logout* apabila meninggalkan komputer atau perisian yang bersesuaian; b. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; c. Memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat; dan d. Memastikan media storan mudah alih tidak	Pentadbir Sistem ICT dan Pengguna

ditinggalkan di komputer atau di ruang kerja.	
0703 Kawalan Capaian Rangkaian	
Objektif: Menghalang capaian tidak sah ke atas perkhidmatan rangkaian.	
070301 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Memasang peralatan yang bersesuaian antara rangkaian Pentadbiran Kerajaan Negeri Sembilan, rangkaian jabatan lain dan rangkaian awam; b. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pengurus ICT dan Pentadbir Sistem ICT
070302 Capaian Internet	

Capaian Internet hendaklah memenuhi keperluan etika penggunaan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan" dan undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan Internet hendaklah dikawal secara berterusan oleh Pentadbir Sistem ICT bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja; b. Kaedah *Content Filtering* hendaklah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti seperti *video conferencing*, *video streaming*, *chat*, *downloading* dan laman sosial adalah perlu bagi memastikan penggunaan jalur lebar (*bandwidth*) secara optimum; d. Penggunaan Internet hanya untuk kegunaan rasmi sahaja;	ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pengguna

e. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet; f. Sebarang bahan yang dimuat turun daripada Internet hendaklah digunakan untuk tujuan yang dibenarkan; dan g. Penggunaan modem peribadi untuk tujuan sambungan ke Internet dalam persekitaran jabatan tidak dibenarkan.	
0704 Kawalan Capaian Sistem Pengoperasian	
Objektif: Menghalang capaian tidak sah ke atas sistem pengoperasian.	
070401 Capaian Sistem Pengoperasian	
Kemudahan keselamatan dalam sistem pengoperasian perlu digunakan untuk menghalang capaian ke sistem komputer iaitu: a. Mengenal pasti identiti, setiap pengguna yang dibenarkan; dan b. Merekodkan capaian yang berjaya dan gagal. Kaedah yang digunakan hendaklah mampu	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

menyokong perkara berikut: a. Mengesahkan pengguna yang dibenarkan; b. Melaksana audit log ke atas semua capaian sistem pengoperasian; dan c. Menamatkan capaian sekiranya dibiarkan dalam keadaan *idle* dalam tempoh yang ditetapkan.	
070402 Capaian Pihak Ketiga	
Pihak ketiga hendaklah: a. Mendapatkan kebenaran bertulis sekiranya hendak membuat capaian jarak jauh; b. Mendapat kebenaran daripada pegawai yang bertanggungjawab bagi penggunaan perisian akses jarak jauh; c. Bertanggungjawab sepenuhnya terhadap sebarang insiden yang disebabkan oleh aktiviti yang dilakukan; dan d. Mematuhi peraturan keselamatan jabatan.	Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga
070403 Kad Pintar	

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian Sistem Kerajaan Elektronik yang dikhususkan; b. Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang penyalahgunaan; c. Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan; d. Sebarang masalah penggunaan dan kehilangan perlu dilaporkan kepada penyedia perkhidmatan; dan e. Pengguna perlu menyerahkan kepada Ketua Jabatan atas sebab-sebab berikut: i. Bertukar bidang tugas kerja; ii. Bertukar ke jabatan lain; iii. Bersara; atau iv. Ditamatkan perkhidmatan.	ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pengguna

0705 Kawalan Capaian Data, Maklumat dan Sistem Aplikasi	
Objektif: Menghalang capaian tidak sah ke atas data, maklumat dan sistem aplikasi.	
070501 Capaian Data, Maklumat dan Sistem Aplikasi	
Perkara berikut hendaklah dipatuhi: a. Pengguna hanya boleh menggunakan sistem aplikasi yang dibenarkan mengikut tahap capaian yang telah ditentukan; b. Setiap aktiviti capaian sistem aplikasi hendaklah direkodkan (jejak audit); c. Mengehadkan capaian sistem aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun pengguna akan disekat; dan d. Melaksanakan tambahan ciri-ciri keselamatan pada sistem aplikasi seperti penggunaan kad pintar, tandatangan digital, SSL dan CAPTCHA.	Pengurus ICT, Pentadbir Sistem ICT dan Pengguna

0706 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.	
070601 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan mudah alih hendaklah disimpan di tempat yang selamat; b. Pergerakan peralatan mudah alih keluar daripada pejabat hendaklah mendapat kebenaran Ketua Jabatan; c. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan; dan d. Kawalan capaian dari luar terhadap sistem aplikasi dalaman hendaklah diberikan kepada pengguna yang dibenarkan sahaja dan kawalan	Pengurus ICT, Pegawai Aset dan Pengguna

ini hendaklah dilakukan melalui *firewall* jabatan.	

BIDANG 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM APLIKASI

0801 Keselamatan Dalam Membangunkan Sistem Aplikasi

Objektif:
Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT.

080101 Keperluan Keselamatan Sistem Aplikasi

Perkara yang perlu dipatuhi adalah seperti berikut: a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan; b. Pengujian hendaklah dijalankan ke atas sistem aplikasi untuk menyemak pengesahan dan integriti data; dan c. Sistem hendaklah diuji terlebih dahulu bagi memenuhi keperluan keselamatan yang telah ditetapkan.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

080102 Pengesahan Data Input dan Output	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Data input aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul; b. Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat; dan c. Proses verifikasi data hendaklah dibuat terhadap kesahihan migrasi dan pindahan data.	Pentadbir Sistem ICT
0802 Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080201 Enkripsi	
Pembangun sistem hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi.	Semua

080202 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Pengurus ICT dan Pentadbir Sistem ICT dan Pengguna
080203 Pengurusan Infrastruktur Kunci Awam (PKI)	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, di musnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pengurus ICT dan Pentadbir Sistem ICT dan Pengguna
0803 Keselamatan Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
080301 Kawalan Fail Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh pegawai yang bertanggungjawab;	Pengurus ICT dan Pentadbir Sistem ICT

b. Kod sumber sistem aplikasi hanya boleh digunakan selepas ujian penerimaan; dan c. Mengawal capaian ke atas kod sumber sistem aplikasi bagi mengelakkan risiko;	
0804 Keselamatan Proses Pembangunan dan Penyelenggaraan	
Objektif: Menjaga dan menjamin keselamatan sistem aplikasi	
080401 Prosedur Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perubahan atau pengubahsuaian ke atas sistem aplikasi hendaklah diuji, direkod dan disahkan sebelum diguna pakai; b. Sistem aplikasi perlu dikaji dan diuji apabila terdapat perubahan kepada sistem; c. Melaksanakan perubahan ke atas pakej perisian mengikut keperluan; dan d. Capaian kepada kod sumber aplikasi hanya dibenarkan kepada pegawai yang	Pengurus ICT dan Pentadbir Sistem ICT

bertanggungjawab.	
080402 Pembangunan Sistem Aplikasi Secara *Outsource*	
Pembangunan sistem aplikasi secara *outsource* perlu diselia oleh pentadbir dan pemilik sistem. Kod sumber bagi sistem aplikasi merupakan hak milik jabatan. Semua capaian yang dibenarkan kepada pihak ketiga hendaklah dimansuhkan selepas tamat tempoh jaminan.	Pentadbir Sistem ICT
0805 Kawalan *Vulnerability* Teknikal	
Objektif: Memastikan kawalan *vulnerability* teknikal adalah sistematik dan berkesan.	
080501 Kawalan Ancaman Teknikal	
Kawalan ancaman teknikal perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi dengan mematuhi perkara berikut: a. Memperoleh maklumat *vulnerability* teknikal yang tepat ke atas sistem aplikasi; b. Menilai *vulnerability* bagi mengenal pasti tahap	Pengurus ICT dan Pentadbir Sistem ICT

risiko; dan c. Mengambil langkah kawalan untuk mengatasi risiko.	

BIDANG 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:
Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden.

090101 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah *(adverse event*) atau ancaman kemungkinan berlaku ke atas Aset ICT secara sengaja atau tidak. Insiden keselamatan ICT hendaklah dilaporkan kepada ICTSO dan CERTNS dengan kadar segera seperti berikut: a. Maklumat didapati hilang atau disyaki hilang kepada pihak yang tidak diberi kuasa; b. Maklumat didapati didedahkan atau disyaki didedahkan kepada pihak-pihak yang tidak diberi kuasa capaian; c. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;	ICTSO, CERTNS dan Pengguna

d. Mekanisme kawalan akses hilang, dicuri, didedahkan atau disyaki sedemikian; e. Berlaku kejadian sistem yang luar daripada kebiasaan; dan f. Berlaku pencerobohan, penyelewengan dan insiden yang tidak dijangka atau disyaki sedemikian. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden seperti di Lampiran 2. Prosedur pelaporan insiden keselamatan ICT berdasarkan: a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan b. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
0902 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif: Memastikan insiden keselamatan ICT diuruskan dengan sistematik dan berkesan.	

090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT perlu dikendalikan, disimpan dan dianalisis bagi tujuan perancangan, tindakan pembetulan dan pengukuhan Kawalan pengurusan pengendalian insiden adalah seperti berikut: a. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti di tempat yang selamat; b. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c. Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; d. Menyediakan tindakan pemulihan segera; dan e. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO, CERTNS, Pengurus ICT dan Pentadbir Sistem ICT

BIDANG 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (PKP)

1001 Dasar Kesinambungan Perkhidmatan

Objektif:

Memastikan penyampaian perkhidmatan yang berterusan kepada pelanggan.

100101 Pelan Kesinambungan Perkhidmatan (PKP)

Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan*) hendaklah dibangunkan untuk mengekalkan kesinambungan perkhidmatan. Langkah berikut perlu dilakukan sebelum membangunkan PKP: **1. Penilaian Risiko Jabatan** Penilaian risiko perlu dilakukan bagi mengenal pasti kelemahan utama dan tahap risiko jabatan. Kelemahan bidang-bidang utama dapat dikenal pasti dan tindakan kawalan dapat ditentukan. Hasil penemuan perlu didokumenkan dalam Laporan Penilaian Risiko. **2. Analisis Impak Perkhidmatan Jabatan** Analisis Impak Perkhidmatan perlu dijalankan bagi mengenal pasti fungsi-fungsi kritikal perkhidmatan, tempoh	CIO, ICTSO dan Pengurus ICT

pemulihan dan sumber-sumber operasi dan kewangan minimum yang diperlukan. Jabatan perlu mengenal pasti fungsi kritikal bagi perkhidmatan yang disediakan oleh jabatan dan tahap toleransi jabatan sekiranya terdapat gangguan kepada fungsi berkenaan.

Pelan PKP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:

a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;

b. Senarai Pengurus ICT Pentadbiran Kerajaan Negeri Sembilan dan pihak ketiga berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan Pengurus ICT tidak dapat hadir untuk menangani insiden;

c. Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;

d. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan

e. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.

Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini hendaklah diluluskan oleh Mesyuarat Pengurusan Jabatan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; c. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; d. Mendokumentasikan proses dan prosedur yang telah dipersetujui; e. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; f. Salinan pelan PKP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama dan sentiasa dikemas kini mengikut pelan utama.	

g. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. h. Ujian PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. Pembangunan PKP hendaklah merujuk kepada dokumen Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang dilampirkan bersama surat arahan Ketua Pengarah MAMPU (Rujukan MAMPU.BPICT.700-4/2/11 (3) bertarikh 22 Januari 2010.	

BIDANG 11 PEMATUHAN

1101 Pematuhan dan Keperluan Perundangan

Objektif:
Meningkatkan tahap keselamatan ICT dan mengelakkan pelanggaran Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan.

110101 Pematuhan Dasar

Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan hendaklah dibaca, difahami dan dipatuhi. Ketua Jabatan berhak untuk mengesan penggunaan selain daripada tujuan yang telah ditetapkan. Sebarang penggunaan Aset ICT selain daripada maksud dan tujuan yang telah ditetapkan, merupakan satu penyalahgunaan sumber.	Pengguna

110102 Pematuhan Dasar, Piawaian dan Prosedur

Pegawai bertanggungjawab hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan prosedur.	CIO, ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

110103 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan.	Pengguna
110104 Dokumen Perundangan	
Dokumen perundangan yang perlu dipatuhi adalah seperti di Lampiran 3.	Pengguna
110105 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan serta semua perbuatan kecuaian dan kelalaian yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 akan dikenakan tindakan tatatertib.	Pengguna

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Terdiri daripada perkakasan, perisian, aplikasi sistem, perkhidmatan, data, maklumat, manusia, media storan, dokumentasi, premis komputer dan peralatan rangkaian.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Jalur Lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CAPTCHA	*Completely Automated Public Turing test to tell Computers and Humans Apart* Bertujuan untuk membezakan antara mesin (bot) dan manusia.
CERTNS	*Computer Emergency Response Team Negeri Sembilan* Pasukan yang ditubuhkan untuk mengendalikan insiden keselamatan ICT di bawah penadbiran kerajaan Negeri Sembilan.
CIO	*Chief Information Officer*

	Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
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. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Harddisk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (*hub*) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port*kepada semua *port*yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.

Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/ atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.

Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
Media Tandatangan Digital	Satu mekanisma yang digunakan untuk menandatangani sesuatu dokumen rasmi secara elektronik.
MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pegawai Aset	Pegawai yang dilantik untuk menjaga dan menguruskan aset.
Pegawai Keselamatan Jabatan	Pegawai yang bertanggungjawab mengenai pentadbiran Jabatan untuk melaksanakan arahan-arahan keselamatan Kerajaan dengan berhubung rapat dan mendapat nasihat dari Pegawai Keselamatan Kerajaan

Pengguna	Pegawai dan kakitangan yang bertanggungjawab menggunakan sistem
Pengurus ICT	Pegawai yang bertanggungjawab menguruskan keselamatan ICT di bawah kawalannya.
Pentadbiran Kerajaan Negeri Sembilan	Semua jabatan dan agensi termasuk Badan Berkanun Negeri dan Pihak Berkuasa Tempatan
Pentadbir Sistem ICT	Pegawai yang bertanggungjawab sebagai Pengurus Projek/ Pentadbir Rangkaian/ Pentadbir Sistem Aplikasi/ Pentadbir Web/ Pentadbir Pangkalan Data/ Pengurus Pusat Data.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer sekiranya tidak digunakan dalam jangka masa tertentu.

SSL	*Secure Socket Layer* merupakan protokol kriptografi yang digunakan dalam keselamatan komunikasi melalui internet.
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.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT NEGERI SEMBILAN

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

Tandatangan : .....

Tarikh : .....

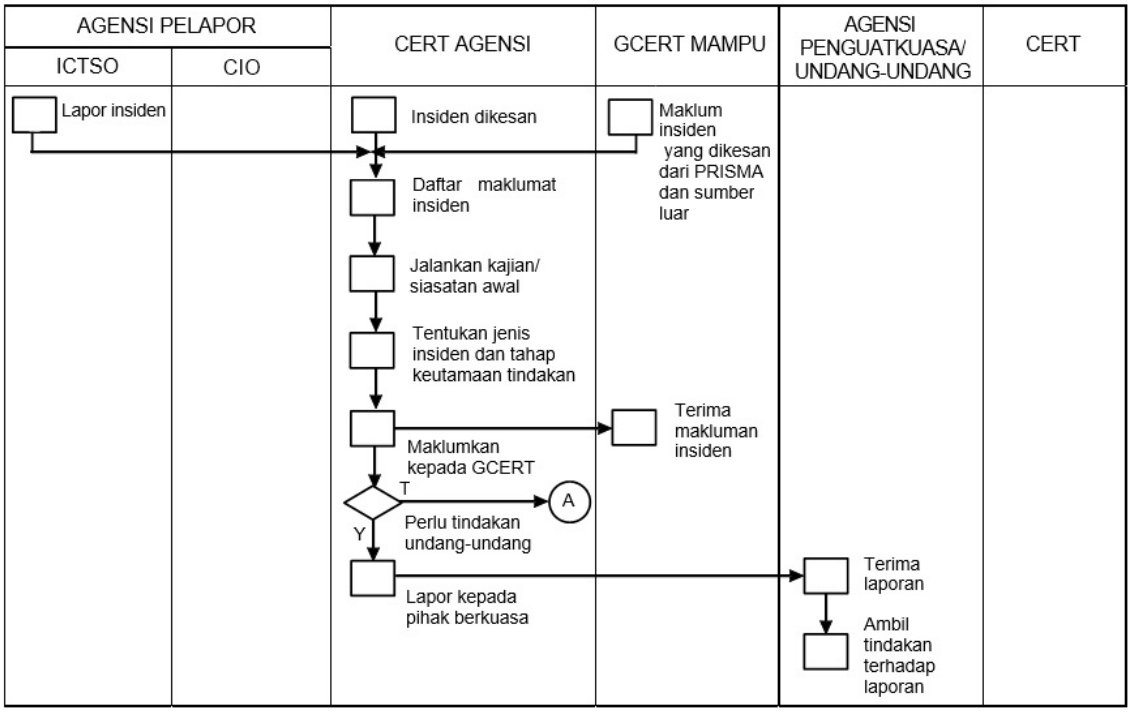
Pengesahan

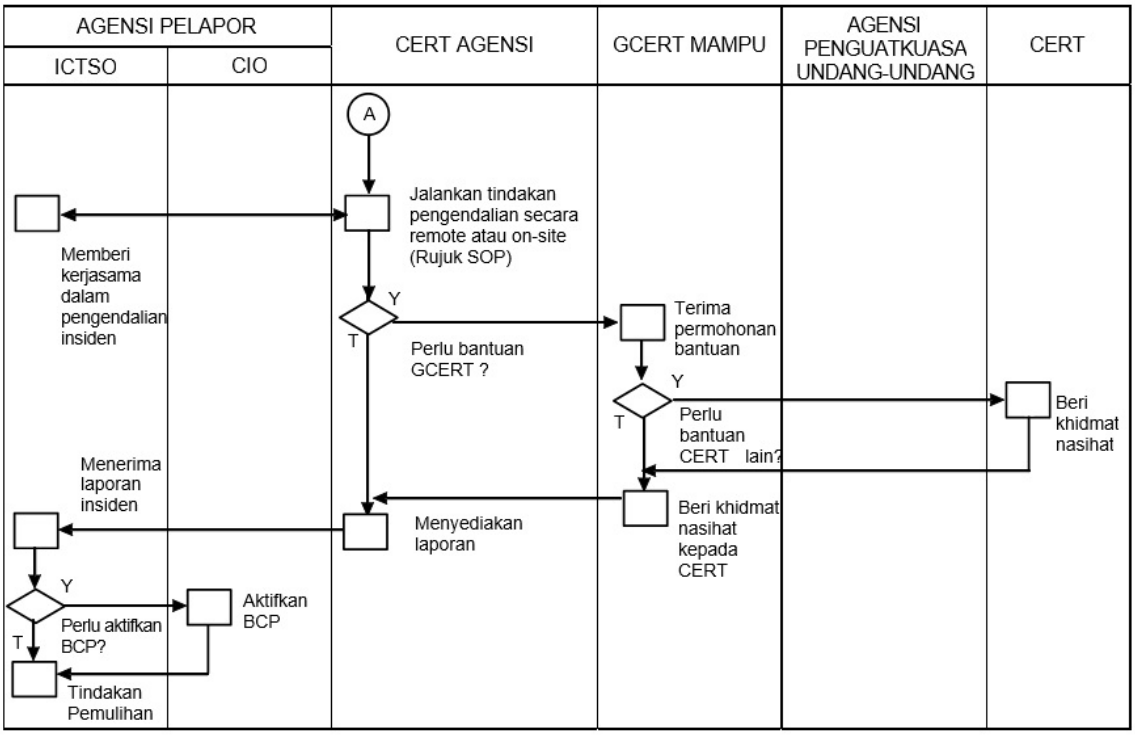
.....

Ketua Pegawai Maklumat (CIO)

LAMPIRAN 2

Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT Agensi





LAMPIRAN 3

DOKUMEN PERUNDANGAN

a. Arahan Keselamatan;
b. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
c. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
d. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
f. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
g. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
h. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
i. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
j. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
k. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
l. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender; (Dibatalkan oleh SPP 5/2007)
m. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
n. Akta Tandatangan Digital 1997;

o. Akta Rahsia Rasmi 1972;

p. Akta Jenayah Komputer 1997;

q. Akta Hak Cipta (Pindaan) Tahun 1997;

r. Akta Komunikasi dan Multimedia 1998;

s. Perintah-Perintah Am;

t. Arahan Perbendaharaan;

u. Arahan Teknologi Maklumat 2007;

v. Garis Panduan Keselamatan MAMPU 2004;

w. Standard Operating Procedure (SOP) ICT MAMPU;

x. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;

y. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.