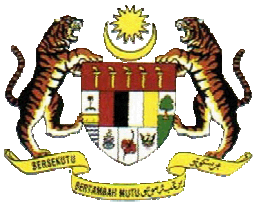

DASAR KESELAMATAN ICT

Jabatan Perpaduan Negara dan Integrasi Nasional
Jabatan Perdana Menteri

5 November 2009

Versi 1.0

KANDUNGAN

PRAKATA KETUA PENGARAH
Jabatan Perpaduan Negara & Integrasi Nasional

بسم الله الرحمن الرحيم

Assalamu'alaikum dan Salam Perpaduan,

Terlebih dahulu saya ingin merakamkan sekalung tahniah kepada semua pihak yang terlibat di Jabatan Perpaduan Negara dan Integrasi Nasional (JPNIN) yang telah berjaya membangunkan dan menerbitkan Dokumen Dasar Keselamatan ICT ver 1.0 untuk kegunaan dan rujukan semua peringkat pengguna ICT di JPNIN.

Sebagaimana kita semua maklum, Kerajaan telah mengeluarkan Pekeliling Am Bil. 3 Tahun 2000 mengenai Rangka Dasar Teknologi Maklumat dan Komunikasi Kerajaan yang menjelaskan perkara-perkara berkaitan keselamatan ICT yang perlu diberi pertimbangan dan tindakan oleh agensi-agensi Kerajaan. Sehubungan dengan itu, JPNIN telah mengambil langkah untuk menghasilkan Dasar Keselamatan ICT (DKICT) di peringkat jabatan sendiri bagi dipatuhi oleh semua warga kerja JPNIN.

Usaha yang dilaksanakan bagi membangunkan DKICT JPNIN adalah sangat baik dalam menangani sebarang bentuk insiden keselamatan ICT yang mungkin wujud secara lebih teratur dan berkesan agar gangguan terhadap sistem penyampaian jabatan melalui ICT dapat dikurangkan dan sentiasa terkawal dari aspek keselamatan pada setiap masa. Namun begitu, DKICT ini perlu sentiasa disemak semula agar selari dengan keperluan teknologi dan corak ancaman keselamatan ICT semasa.

Saya berharap dengan adanya panduan ini, lebih ramai yang akan peka kepada isu dan kepentingan keselamatan ICT dan pada masa yang sama usaha bagi mempertingkatkan kesedaran ini perlu dibuat dari masa ke masa melalui program-program pembudayaan ICT kepada warga kerja JPNIN.

Kesimpulannya, diharap semua warga kerja JPNIN dapat mengambil manfaat dan memberi perhatian serta kerjasama sepenuhnya dalam mematuhi DKICT ini bagi memastikan matlamat dan objektifnya tercapai.

Wassalam...

(**DATO' AZMAN AMIN BIN HASSAN**)
Ketua Pengarah
Jabatan Perpaduan Negara dan Integrasi Nasional

PENGENALAN

Dasar Keselamatan ICT (DKICT) JPNIN 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 JPNIN. Dasar ini dibuat berasaskan kepada Dasar Keselamatan ICT MAMPU yang sedia ada.

OBJEKTIF

Dasar Keselamatan ICT JPNIN diwujudkan untuk menjamin kesinambungan urusan JPNIN dengan meminimumkan kesan insiden keselamatan ICT.

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

Manakala, objektif utama Keselamatan ICT JPNIN ialah seperti berikut:

a) Memastikan kelancaran operasi JPNIN dan meminimumkan kerosakan atau kemusnahan;

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

c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

PERNYATAAN DASAR

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

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

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

b) Menjamin setiap maklumat adalah tepat dan sempurna;

c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

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

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

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

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

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

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

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

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada :

a) Penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT;

b) Ancaman yang wujud akibat daripada kelemahan tersebut;

c) Risiko yang mungkin timbul; dan

d) Langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

SKOP

Aset ICT JPNIN terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT JPNIN 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 JPNIN ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan.

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

a) Perkakasan

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

b) Perisian

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

c) Perkhidmatan

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

   i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;

   ii. Sistem halangan akses seperti sistem kad akses; dan

   iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

d) Data atau Maklumat

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

e) Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian JPNIN bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

f) Premis Komputer Dan Komunikasi

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

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

PRINSIP-PRINSIP

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

i. 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;

ii. Hak akses minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari masa ke masa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

iii. 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 JPNIN menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

b) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari masa ke masa;

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

iv. 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;

v. Pengauditan

Pengauditan adalah tindakan untuk mengenalpasti insiden berkaitan keselamatan atau mengenalpasti 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;

vi. Pematuhan

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

vii. 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

viii. Saling Bergantungan

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

BIDANG 1 - PEMBANGUNAN DAN PENYELENGGARAAN DASAR

1.0 DASAR KESELAMATAN ICT

OBJEKTIF

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan JPNIN dan perundangan yang berkaitan.

SUB	PERKARA	TINDAKAN
1.0.1	**PELAKSANAAN DASAR**	
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah JPNIN selaku Pengerusi Jawatankuasa Keselamatan ICT (JKICT) JPNIN. JKICT ini terdiri daripada Ketua Pegawai Maklumat (CIO), Timbalan Ketua Pengarah (Operasi), Pegawai Keselamatan ICT (ICTSO) dan semua Pengarah Bahagian.	**Ketua Pengarah JPNIN**
1.0.2	**PENYEBARAN DASAR**	
	Dasar ini perlu disebarkan kepada semua pengguna JPNIN (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	**ICTSO**
1.0.3	**PENYELENGGARAAN DASAR**	
	Dasar Keselamatan ICT JPNIN adalah tertakluk kepada semakan dan pindaan dari masa ke masa 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 JPNIN: a) Kenal pasti dan tentukan perubahan yang diperlukan; b) Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT), JPNIN; c) Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JKICT; dan	**ICTSO**

	d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	
1.0.4	**PENGECUALIAN DASAR**	
	Dasar Keselamatan ICT JPNIN adalah terpakai kepada semua pengguna ICT JPNIN dan tiada pengecualian diberikan.	**Semua**

BIDANG 2 - ORGANISASI KESELAMATAN

2.0 INFRASTRUKTUR ORGANISASI DALAMAN

OBJEKTIF

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT JPNIN.

SUB	PERKARA	TINDAKAN
2.0.1	**KETUA PENGARAH JPNIN**	
	Ketua Pengarah JPNIN adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT JPNIN; b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT JPNIN; 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 JPNIN; dan e) Mempengerusikan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT), JPNIN.	**Ketua Pengarah JPNIN**
2.0.2	**KETUA PEGAWAI MAKLUMAT (CIO)**	
	Ketua Pegawai Maklumat (CIO) bagi JPNIN ialah Timbalan Ketua Pengarah (Perancangan), JPNIN. Peranan dan tanggungjawab CIO adalah seperti berikut: a) Membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b) Menentukan keperluan keselamatan ICT;	**CIO**

c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT JPNIN serta pengurusan risiko dan pengauditan; dan

d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT JPNIN.

2.0.3 PEGAWAI KESELAMATAN ICT (ICTSO)

ICTSO

Pegawai Keselamatan ICT (ICTSO) bagi JPNIN ialah Pengarah Cawangan Teknologi Maklumat, JPNIN.

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

a) Mengurus keseluruhan program-program keselamatan ICT JPNIN;

b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT JPNIN;

c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT JPNIN kepada semua pengguna;

d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT JPNIN;

e) Menjalankan pengurusan risiko;

f) Menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan JPNIN 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 Tindakbalas Insiden Keselamatan ICT Kerajaan (GCERT), MAMPU dan memaklumkannya kepada CIO;

i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baikpulih dengan segera; dan

j) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.

2.0.4 PENGURUS ICT

Pengurus ICT

Pengurus ICT bagi JPNIN ialah Penolong Pengarah (Teknologi Maklumat), Cawangan Teknologi Maklumat, JPNIN. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan JPNIN;

b) Menentukan kawalan akses pengguna terhadap aset ICT JPNIN;

c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan

d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT JPNIN.

2.0.5 PENTADBIR SISTEM ICT

Pentadbir Sistem ICT

Pentadbir Sistem ICT bagi JPNIN ialah Penolong Pegawai Teknologi Maklumat, Cawangan Teknologi Maklumat, JPNIN. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:

a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;

b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT JPNIN;

c) Memantau aktiviti capaian harian sistem aplikasi pengguna;

d) Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;

e) Menganalisis dan menyimpan rekod jejak audit;

f) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan

g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya dalam keadaan yang baik.

2.0.6 PENGGUNA

Pengguna

Pengguna mempunyai peranan dan tanggungjawab seperti berikut:

a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JPNIN;

b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;

c) Lulus tapisan keselamatan;

d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT JPNIN dan menjaga kerahsiaan maklumat JPNIN;

e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; dan

f) Menghadiri program-program kesedaran mengenai keselamatan ICT.

2.0.7 JAWATANKUASA KESELAMATAN ICT JPNIN

JKICT JPNIN

Jawatankuasa Keselamatan ICT (JKICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT JPNIN.

Mesyuarat Pengarah-Pengarah Bahagian JPNIN juga berperanan sebagai JKICT JPNIN. Keanggotaan JKICT JPNIN adalah seperti berikut:

Pengerusi : Ketua Pengarah JPNIN

Ahli :

i. CIO JPNIN
ii. Timbalan Ketua Pengarah (Operasi)
iii. Semua Pengarah Bahagian
iv. ICTSO

Urus Setia bagi JKICT JPNIN ialah urus setia yang mengendalikan Mesyuarat Pengarah-Pengarah Bahagian JPNIN.

Bidang kuasa:

a) Memperakukan/meluluskan dokumen DKICT JPNIN;

b) Memantau tahap pematuhan keselamatan ICT;

c) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam JPNIN yang mematuhi keperluan DKICT JPNIN;

d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;

e) Memastikan DKICT JPNIN selaras dengan dasar-dasar ICT kerajaan semasa;

f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa;

g) Membincang tindakan yang melibatkan pelanggaran DKICT JPNIN; dan

h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.

2.0.8 PEMILIK SISTEM

Pemilik Sistem

Pemilik sistem adalah Bahagian-bahagian yang memiliki dan bertanggungjawab ke atas maklumat untuk sistem-sistem yang berkaitan seperti :

i. Sistem Pengurusan Rukun Tetangga – Bahagian Pembangunan Komuniti

ii. Sistem Lawatan Integrasi – Bahagian Integrasi Nasional

iii. Sistem e-Sepakat – Bahagian Pengurusan Perpaduan

iv. Kandungan Laman Web Rasmi JPNIN – Bahagian Korporat

v. MyAsset – Cawangan Pentadbiran dan Aset

2.1 PIHAK KETIGA

OBJEKTIF

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

SUB	PERKARA	TINDAKAN
2.1.1	**KEPERLUAN KESELAMATAN KONTRAK DENGAN PIHAK KETIGA**	
	Ini bertujuan memastikan 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 JPNIN; b) Mengenalpasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c) Mengenalpasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d) Akses kepada aset ICT JPNIN perlu berlandaskan kepada perjanjian kontrak; e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. Dasar Keselamatan ICT JPNIN; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek.	**CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga**

BIDANG 3 - PENGURUSAN ASET

3.0 AKAUNTABILITI ASET

OBJEKTIF

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

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

3.1 PENGELASAN DAN PENGENDALIAN MAKLUMAT

OBJEKTIF

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

SUB	PERKARA	TINDAKAN
3.1.1	**PENGELASAN MAKLUMAT**	
	Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; atau d) Terhad.	**Semua**
3.1.2	**PENGENDALIAN MAKLUMAT**	
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;	**Semua**

f) Memberi perhatian kepada maklumat terperingkat terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

BIDANG 4 - KESELAMATAN SUMBER MANUSIA

4.0 KESELAMATAN SUMBER MANUSIA DALAM TUGAS HARIAN

OBJEKTIF

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

SUB	PERKARA	TINDAKAN
4.0.1	**SEBELUM PERKHIDMATAN**	
	Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan JPNIN serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan JPNIN 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; dan c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.	**Semua**
4.0.2	**DALAM PERKHIDMATAN**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Memastikan pegawai dan kakitangan JPNIN serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh JPNIN;	**Semua**

b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT JPNIN secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari masa ke masa;

c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan JPNIN serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh JPNIN; 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 Institut Kajian dan Latihan Integrasi Nasional dan Cawangan Teknologi Maklumat, JPNIN.

4.0.3 BERTUKAR ATAU TAMAT PERKHIDMATAN

Perkara-perkara yang perlu dipatuhi termasuk yang berikut: **Semua**

a) Memastikan semua aset ICT dikembalikan kepada JPNIN mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh JPNIN dan/atau terma perkhidmatan.

BIDANG 5 - KESELAMATAN FIZIKAL DAN PERSEKITARAN

5.0 KESELAMATAN KAWASAN

OBJEKTIF

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

SUB	PERKARA	TINDAKAN
5.0.1	**KAWALAN KAWASAN**	
	Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Kawasan keselamatan fizikal hendaklah dikenalpasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c) Memasang alat penggera atau kamera; d) Mengehadkan 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;	**CIO, ICTSO dan Pengawal Keselamatan Kerajaan**

j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana;

k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan

l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.

5.0.2 KAWALAN MASUK FIZIKAL

Semua

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a) Setiap pengguna JPNIN hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;

b) Semua pas keselamatan hendaklah diserahkan balik kepada JPNIN apabila pengguna berhenti atau bersara;

c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di Aras 9, Blok E2, Kompleks E, Putrajaya. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan

d) Kehilangan pas mestilah dilaporkan dengan segera.

5.0.3 KAWASAN LARANGAN

Pentadbir Sistem

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 JPNIN adalah bilik Ketua Pengarah, bilik-bilik Timbalan Ketua Pengarah, Bilik Server dan Bilik Sulit.

a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan

b) Pihak ketiga adalah dilarang sama sekali untuk

	memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	

5.1 KESELAMATAN PERALATAN

OBJEKTIF

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

SUB	PERKARA	TINDAKAN
5.1.1	**PERALATAN ICT**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif dan dikemaskini 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	**Semua**

Uninterruptable Power Supply (UPS);

j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti switches, hub, router dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;

k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai;

l) Peralatan ICT yang hendak dibawa keluar dari premis JPNIN, 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 berkuatkuasa;

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 baikpulih;

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;

u) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas

dalam keadaan "OFF" apabila meninggalkan pejabat;

v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan

w) Memastikan plag dicabut daripada suis utama bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.

5.1.2 MEDIA STORAN

Semua

Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk, flash disk, CDROM, thumb drive* dan media storan lain.

Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) 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 dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;

d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;

e) Akses dan pergerakan media storan hendaklah direkodkan;

f) Perkakasan penduaan (*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;

h) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan

i) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.

5.1.3 MEDIA PERISIAN DAN APLIKASI

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

Semua

a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan JPNIN;

b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi 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 mestilah mengikut prosedur yang ditetapkan.

5.1.4 PENYELENGGARAAN PERKAKASAN

Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.

Cawangan Teknologi Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar;

b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;

c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;

d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan;

e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan

f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.

5.1.5 PERALATAN DI LUAR PREMIS

Semua

Perkakasan yang dibawa keluar dari premis JPNIN adalah terdedah kepada pelbagai risiko.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan

b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.

5.1.6 PELUPUSAN PERKAKASAN

Semua dan Cawangan Teknologi Maklumat

Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh JPNIN dan ditempatkan di JPNIN.

Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan JPNIN.

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;

b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;

c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;

d) Pegawai Aset hendaklah mengenalpasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

f) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam sistem inventori *MyAsset*;

g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuatkuasa; dan

h) Pengguna ICT adalah DILARANG sama sekali daripada melakukan perkara-perkara seperti berikut:

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *Hardisk*, *Motherboard* dan sebagainya;

ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti *AVR*, *Speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di JPNIN;

iii. Memindah keluar dari JPNIN mana-mana peralatan ICT yang hendak dilupuskan;

iv. Melupuskan peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab JPNIN; dan

v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.

5.2 KESELAMATAN PERSEKITARAN

OBJEKTIF

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

SUB	PERKARA	TINDAKAN
5.2.1	**KAWALAN PERSEKITARAN**	

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK).

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;

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.

5.2.2 BEKALAN KUASA

Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.

Cawangan Teknologi Maklumat dan ICTSO

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.

5.2.3 KABEL

Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah.

Cawangan Teknologi Maklumat dan ICTSO

Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:

a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;

b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;

c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan

d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.

5.2.4	Prosedur Kecemasan	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ).	**Semua dan Pegawai Keselamatan Jabatan**

5.3 KESELAMATAN DOKUMEN

OBJEKTIF

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

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

BIDANG 6 - PENGURUSAN OPERASI DAN KOMUNIKASI

6.0 PENGURUSAN PROSEDUR OPERASI

OBJEKTIF

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

SUB	PERKARA	TINDAKAN
6.0.1	**PENGENDALIAN PROSEDUR**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c) Semua prosedur hendaklah dikemas kini dari masa ke masa atau mengikut keperluan.	**Semua**
6.0.2	**KAWALAN PERUBAHAN**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;	**Semua**

c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan

d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

6.0.3 PENGASINGAN TUGAS DAN TANGGUNGJAWAB

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

Pengurus ICT dan ICTSO

a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;

b) Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan

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

6.1 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PIHAK KETIGA

OBJEKTIF

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

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

6.2 PERANCANGAN DAN PENERIMAAN SISTEM

OBJEKTIF

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

SUB	PERKARA	TINDAKAN
6.2.1	**PERANCANGAN KAPASITI**	
	Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	**ICTSO dan Pentadbir Sistem ICT**
6.2.2	**PENERIMAAN SISTEM**	
	Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	**ICTSO dan Pentadbir Sistem ICT**

6.3 PERISIAN BERBAHAYA

OBJEKTIF

Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya.

SUB	PERKARA	TINDAKAN
6.3.1	**PERLINDUNGAN DARI PERISIAN BERBAHAYA**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d) Mengemas kini anti virus dengan *pattern* antivirus yang terkini; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan	**Semua**

i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

6.4 *HOUSEKEEPING*

OBJEKTIF

Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.

SUB	PERKARA	TINDAKAN
6.4.1	***BACKUP***	
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	**Semua**

6.5 PENGURUSAN RANGKAIAN

OBJEKTIF

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

SUB	PERKARA	TINDAKAN
6.5.1	**KAWALAN INFRASTRUKTUR RANGKAIAN**	
	Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d) Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Sistem ICT; f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan JPNIN; g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JPNIN;	**Semua**

i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;

j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan JPNIN adalah tidak dibenarkan;

k) Semua pengguna hanya dibenarkan menggunakan rangkaian JPNIN sahaja dan penggunaan modem adalah dilarang sama sekali melainkan dengan kebenaran ICTSO; dan

l) Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.

6.6 PENGURUSAN MEDIA

OBJEKTIF

Melindungi aset ICT dari sebarang pendedahan pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

SUB	PERKARA	TINDAKAN
6.6.1	**PENGHANTARAN DAN PEMINDAHAN**	
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	**Semua**
6.6.2	**PROSEDUR PENGENDALIAN MEDIA**	
	Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;	**Semua**

	e) Menyimpan semua media di tempat yang selamat; dan f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	
6.6.3	**KESELAMATAN SISTEM DOKUMENTASI**	
	Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b) Menyedia dan memantapkan keselamatan sistem dokumentasi;dan c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	**Semua**

6.7 PENGURUSAN PERTUKARAN MAKLUMAT

OBJEKTIF

Memastikan keselamatan pertukaran maklumat dan perisian antara JPNIN dan agensi luar terjamin.

SUB	PERKARA	TINDAKAN
6.7.1	**PERTUKARAN MAKLUMAT**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara JPNIN dengan agensi luar;	**Semua**

c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari JPNIN; dan

d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.

6.7.2 PENGURUSAN MEL ELEKTRONIK (E-MEL)

Semua

Penggunaan e-mel di JPNIN hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*" dan mana- mana undang-undang bertulis yang berkuat kuasa.

Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut:

a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh JPNIN sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh JPNIN;

c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;

d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;

e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh Megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

f) Pengguna hendaklah mengelak dari membuka

e-mel daripada penghantar yang tidak diketahui atau diragui;

g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

h) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;

i) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

j) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;

k) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;

l) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan

m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.

6.8 PEMANTAUAN

OBJEKTIF

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

SUB	PERKARA	TINDAKAN
6.8.1	**PENGAUDITAN DAN FORENSIK ICT**	
	ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a) Sebarang percubaan pencerobohan kepada sistem ICT JPNIN; b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; g) Aktiviti penyalahgunaan akaun e-mel; dan h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	**ICTSO**

6.8.2 JEJAK AUDIT

Pentadbir Sistem ICT

Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.

Jejak audit hendaklah mengandungi maklumat-maklumat berikut:

a) Rekod setiap aktiviti transaksi;

b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;

c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan

d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara.

Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.

6.8.3 SISTEM LOG

Pentadbir Sistem ICT

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:

a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;

b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik

pulih dengan segera; dan

c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.

6.8.4 PEMANTAUAN LOG

Cawangan Teknologi Maklumat

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) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala;

c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;

d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;

e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan

f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam JPNIN atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.

BIDANG 7 – KAWALAN CAPAIAN

7.0 DASAR KAWALAN CAPAIAN

OBJEKTIF

Mengawal capaian ke atas maklumat.

SUB	PERKARA	TINDAKAN
7.0.1	**KEPERLUAN KAWALAN CAPAIAN**	
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d) Kawalan ke atas kemudahan pemprosesan maklumat.	**Cawangan Teknologi Maklumat**

7.1 PENGURUSAN CAPAIAN PENGGUNA

OBJEKTIF

Mengawal capaian pengguna ke atas aset ICT JPNIN.

SUB	PERKARA	TINDAKAN
7.1.1	**AKAUN PENGGUNA**	
	Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a) Akaun yang diperuntukkan oleh JPNIN sahaja boleh digunakan; b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c) Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan JPNIN. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi empat (4) minggu; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; atau iv. Bersara/Ditamatkan perkhidmatan.	**Semua dan Pentadbir Sistem ICT**

7.1.2 HAK CAPAIAN	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	**Pentadbir Sistem ICT**

7.1.3 PENGURUSAN KATA LALUAN	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh JPNIN seperti berikut: a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c) Panjang kata laluan mestilah sekurang-kurangnya 6 aksara dengan gabungan aksara, angka dan aksara khusus; d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e) Kata laluan *windows* dan *screensaver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama; f) Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula; h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan;	**Semua dan Pentadbir Sistem ICT**

j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan

k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.

7.1.4 *CLEAR DESK / CLEAR SCREEN*

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

Semua

Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Menggunakan kemudahan *password* atau *logout* apabila meninggalkan komputer;

b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan

c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.

7.2 KAWALAN CAPAIAN RANGKAIAN

OBJEKTIF

Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.

SUB	PERKARA	TINDAKAN
7.2.1	**CAPAIAN RANGKAIAN**	
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian JPNIN, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	**Pentadbir Sistem ICT dan ICTSO**
7.2.2	**CAPAIAN INTERNET**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan Internet di JPNIN hendaklah dipantau secara berterusan oleh Pentadbir Sistem ICT bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian JPNIN; b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c) Penggunaan teknologi *(packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading)* adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; d) Penggunaan Internet hanyalah untuk kegunaan rasmi	**Pentadbir Sistem ICT**

sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;

e) Laman yang dilayari hendaklah hanya yang berkaitan dengan semua bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Pengarah/ pegawai yang diberi kuasa;

f) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;

g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian sebelum dimuat naik ke Internet;

h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

i) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh JPNIN;

j) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;

k) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali melainkan dengan kebenaran ICTSO; dan

l) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:

   i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan

   ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.

7.3 KAWALAN CAPAIAN SISTEM PENGOPERASIAN

OBJEKTIF

Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

SUB	PERKARA	TINDAKAN
7.3.1	**CAPAIAN SISTEM PENGOPERASIAN**	
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a) Mengesahkan pengguna yang dibenarkan; b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* dan c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c) Mengehadkan dan mengawal penggunaan program; dan d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	**Pentadbir Sistem ICT dan ICTSO**

7.3.2 KAD PINTAR

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: **Semua**

a) Penggunaan 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 kecurian atau digunakan oleh pihak lain;

c) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan

d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Cawangan Teknologi Maklumat, JPNIN.

7.4 KAWALAN CAPAIAN APLIKASI DAN MAKLUMAT

OBJEKTIF

Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.

SUB	PERKARA	TINDAKAN
7.4.1	**CAPAIAN APLIKASI DAN MAKLUMAT**	
	Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.	**Pentadbir Sistem ICT dan ICTSO**
	Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); c) Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	

BIDANG 8 – PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

8.0 KESELAMATAN DALAM MEMBANGUNKAN SISTEM DAN APLIKASI

OBJEKTIF

Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

SUB	PERKARA	TINDAKAN
8.0.1	**KEPERLUAN KESELAMATAN SISTEM MAKLUMAT**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	**Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO**
8.0.2	**PENGESAHAN DATA INPUT DAN OUTPUT**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	**Pemilik Sistem dan Pentadbir**

		Sistem ICT
	a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b) Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	

8.1 KAWALAN KRIPTOGRAFI

OBJEKTIF

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

SUB	PERKARA	TINDAKAN
8.1.1	**ENKRIPSI**	
	Pentadbir Sistem hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa di peringkat *Server* dan pangkalan data sistem.	**Pentadbir Sistem**
8.1.2	**PENGURUSAN INFRASTRUKTUR KUNCI AWAM (*PKI*)**	
	Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	**Pengguna e-SPKB dan e-Perolehan**

8.2 KESELAMATAN FAIL SISTEM

OBJEKTIF

Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.

SUB	PERKARA	TINDAKAN
8.2.1	**KAWALAN FAIL SISTEM**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal;dan e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	**Pentadbir Sistem ICT**

8.3 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN

OBJEKTIF

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

SUB	PERKARA	TINDAKAN
8.3.1	**PROSEDUR KAWALAN PERUBAHAN**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d) Akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e) Menghalang sebarang peluang untuk membocorkan maklumat.	**Pemilik Sistem dan Pentadbir Sistem ICT**
8.3.2	**PEMBANGUNAN PERISIAN SECARA *OUTSOURCE***	
	Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem dan pentadbir sistem. Kod sumber (*source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik JPNIN.	**Pemilik Sistem dan Pentadbir Sistem ICT**

8.4 KAWALAN TEKNIKAL KETERBUKAAN (*VULNERABILITY*)

OBJEKTIF

Memastikan kawalan teknikal keterbukaan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.

SUB	PERKARA	TINDAKAN
8.4.1	**KAWALAN DARI ANCAMAN TEKNIKAL**	
	Kawalan teknikal keterbukaan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memperoleh maklumat teknikal keterbukaan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b) Menilai tahap keterbukaan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	**Pentadbir Sistem ICT**

BIDANG 9 – PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

9.0 MEKANISME PELAPORAN INSIDEN KESELAMATAN ICT

OBJEKTIF

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

SUB	PERKARA	TINDAKAN
9.0.1	**MEKANISME PELAPORAN**	
	Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan GCERT MAMPU dengan kadar segera: a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Prosedur pelaporan insiden keselamatan ICT berdasarkan: a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan	**Semua**

Teknologi Maklumat dan Komunikasi; dan

b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.

9.1 PENGURUSAN MAKLUMAT INSIDEN KESELAMATAN ICT

OBJEKTIF

Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

SUB	PERKARA	TINDAKAN
9.1.1	**PROSEDUR PENGURUSAN MAKLUMAT INSIDEN KESELAMATAN ICT**	
	Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada JPNIN. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; d) Menyediakan tindakan pemulihan segera; dan e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	**ICTSO dan Pentadbir Sistem**

BIDANG 10 – PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

10.0 DASAR KESINAMBUNGAN PERKHIDMATAN

OBJEKTIF

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

SUB	PERKARA	TINDAKAN
10.0.1	**PELAN KESINAMBUNGAN PERKHIDMATAN**	
	Pelan Kesinambungan Perkhidmatan (*Business Continuity Management - BCM*) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JKICT JPNIN. Perkara-perkara berikut perlu diberi perhatian: a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; d) Mendokumentasikan proses dan prosedur yang telah dipersetujui; e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; f) Membuat *backup*; dan g) Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.	**Pengurus ICT dan Kontraktor**

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

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

b) Senarai personel JPNIN dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden;

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

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

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

Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

JPNIN hendaklah memastikan salinan pelan BCM sentiasa dikemaskini dan dilindungi seperti di lokasi utama.

BIDANG 11 – PEMATUHAN

11.0 PEMATUHAN DAN KEPERLUAN PERUNDANGAN

OBJEKTIF

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

SUB	PERKARA	TINDAKAN
11.0.1	**PEMATUHAN DASAR**	
	Setiap pengguna di JPNIN hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT JPNIN dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Semua aset ICT di JPNIN termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Pengarah / Pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT JPNIN selain daripada maksud dan tujuan yang telah ditetapkan adalah merupakan satu penyalahgunaan sumber JPNIN.	**Semua**
11.0.2	**PEMATUHAN DENGAN DASAR, PIAWAIAN DAN KEPERLUAN TEKNIKAL**	
	ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi *standard* pelaksanaan keselamatan ICT.	**ICTSO**
11.0.3	**PEMATUHAN KEPERLUAN AUDIT**	
	Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan	**Semua**

diselia bagi mengelakkan berlaku penyalahgunaan.

11.0.4	KEPERLUAN PERUNDANGAN	
	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di JPNIN:	**Semua**

i. Arahan Keselamatan;

ii. Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

iii. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002;

iv. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

v. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;

vi. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

vii. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

viii. 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;

ix. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

x. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan

Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

xi. Surat Pekeliling Am Bil. 2 Tahun 2000 – Peranan Jawatankuasa- jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

xii. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

xiii. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;

xiv. Akta Tandatangan Digital 1997;

xv. Akta Rahsia Rasmi 1972;

xvi. Akta Jenayah Komputer 1997;

xvii. Akta Hak Cipta (Pindaan) Tahun 1997;

xviii. Akta Komunikasi dan Multimedia 1998;

xix. Perintah-Perintah Am;

xx. Arahan Perbendaharaan;

xxi. Arahan Teknologi Maklumat 2007;

xxii. Garis Panduan Keselamatan MAMPU 2004; dan

xxiii. *Standard Operating Procedure* (SOP) dan garis panduan ICT yang dikeluarkan dari masa ke masa.

11.0.5	PELANGGARAN DASAR	
	Pelanggaran Dasar Keselamatan ICT JPNIN boleh dikenakan tindakan tatatertib mengikut Perintah Am Bab D – Kelakuan dan Tatatertib.	**Semua**