DASAR KESELAMATAN ICT

KEMENTERIAN PELANCONGAN DAN KEBUDAYAAN MALAYSIA (KPK)

BAGI

PERPUSTAKAAN NEGARA MALAYSIA

(Versi 1.0)

KANDUNGAN

TAKRIFAN

Aset ICT	Sebarang objek ICT yang mempunyai nilai kepada organisasi.
Kementerian	Kementerian Pelancongan Dan Kebudayaan Malaysia (KPK).
Jabatan	Merujuk kepada Jabatan Perpustakaan Negara Malaysia (PNM).
Agensi	Merujuk kepada Perpustakaan Negara Malaysia (PNM), Perbadanan Kemajuan Kraftangan Malaysia (KRAF), Akademi Seni Budaya Dan Warisan Negara (ASWARA), Istana Budaya (IB) dan Lembaga Pembangunan Seni
Pengurus ICT	Adalah merujuk kepada Pengarah Bahagian Teknilogi Maklumat, PNM.
Pegawai Aset	Pegawai yang dilantik oleh Pegawai Pengawal untuk menguruskan aset.
Koordinator PKP	Pegawai yang dilantik bagi melaksanakan Pelan Kesinambungan Perkhidmatan di PNM.
Backup	Salinan fail atau program yang dijanakan untuk memudahkan proses pemulihan dijalankan.
Business Impact Analysis	Analisa berkaitan keperluan sistem ICT, proses dan hubungan kait antara keduanya yang digunakan untuk menyediakan sistem kontingensi dan keutamaan yang perlu diberikan semasa bencana.
Change Management	Proses yang memastikan semua perubahan ke atas infrastruktur ICT ditaksirkan, ditentusahkan, dilaksanakan dan dikaji semula dalam keadaan terkawal untuk memastikan gangguan tidak berlaku.
Dasar	Pernyataan peringkat tinggi mengenai prinsip, matlamat dan objektif termasuk juga cara-cara untuk mencapainya bagi subjek yang spesifik.

E-mel	Mesej yang dihantar secara elektronik.
Impak	Hasil atau lanjutan dari sesuatu kejadian.
Integriti	Keadaan di mana maklumat tersimpan mengikut cara yang dibenarkan dan tiada perubahan dilakukan yang menjadikan maklumat itu berlainan dari asal.
Kawalan	Langkah-langkah penjagaan yang mana bila ia dilakukan dengan betul, akan mengurangkan risiko kemusnahan terhadap aset.
Kerahsiaan	Keadaan di mana maklumat sensitif dikawal dan diberikan kepada Pengguna ICT yang sah sahaja.
Keselamatan Fizikal	Prosedur kawalan yang wujud untuk menghalang penceroboh dari memasuki sistem atau prasarana.
Ketersediaan	Keadaan di mana maklumat atau proses sentiasa boleh dicapai dan digunakan oleh pihak yang dibenarkan.
Pengasingan Tugas	Pengasingan tugas dan tanggungjawab supaya tiada individu boleh mensabotaj sistem kritikal yang
Pengguna ICT	Kakitangan PNM (Tetap, sementara, kontrak) atau pihak ketiga (perunding, kontraktor, pembekal dan pembekal perkhidmatan) yang diberikan hak capaian kepada sistem dan aset ICT PNM.
Pihak Ketiga	Individu yang selain dari kakitangan PNM seperti perunding, pembekal, kontraktor, pembekal perkhidmatan
Risiko	Kemungkinan untuk sesuatu terjadi yang boleh memberikan impak kepada objektifnya.
Secure Areas	Kawasan di mana PNM menempatkan aset ICT yang sensitif dan kritikal seperti Pusat Data atau bilik pejabat yang mengandungi maklumat yang sulit.
Shred	Cara-cara untuk „membersihkan“ media, dengan cara merincih atau menghancurkannya kepada bahagian yang
Virus	Kod yang ditulis dengan niat jahat untuk memusnahkan cara komputer bekerja tanpa kebenaran pengguna.

Vulnerability	Kelemahan dari segi prosedur, seni bina, implementasi dan kawalan dalaman yang boleh dieksploitasi hingga mengakibatkan pelanggaran aspek keselamatan atau dasar keselamatan.

BAHAGIAN I - PENGENALAN

1.0 MAKLUMAT AM

1.1 Kertas Dasar Keselamatan ICT ini mengandungi garis panduan, peraturan dan tatacara yang wajib dibaca, difahami dan dipatuhi oleh semua kakitangan Jabatan dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) di Perpustakaan Negara Malaysia (PNM).

1.2 Dasar ini menerangkan kepada semua Pengguna ICT mengenai tanggungjawab dan peranan mereka dalam menjaga, melindungi dan memelihara aset ICT Jabatan yang diguna dan diamanahkan kepada mereka.

1.3 Dasar ini penting bagi melindungi sistem ICT daripada risiko, ancaman, kelemahan atau keterdedahan. Hal ini dapat dilakukan dengan mengurangkan kesan gangguan secara kos efektif untuk memastikan kesinambungan penyampaian perkhidmatan dan gangguan terhadap perkhidmatan dapat diminimumkan.

2.0 OBJEKTIF

2.1 Dasar Keselamatan ICT ini di wujud bagi memastikan keselamatan ICT Jabatan berada pada tahap yang terbaik, terurus dan sentiasa dilindungi dari pelbagai risiko, ancaman, kelemahan dan keterdedahan yang tidak diingini.

2.2 Ia adalah selaras dengan Arahan Teknologi Maklumat yang dikeluarkan Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) untuk melindungi aset ICT Kerajaan dari segi kerahsiaan, integriti, ketersediaan, kesahihan dan tidak boleh disangkal.

2.3 Di samping itu, ia juga bertujuan untuk memastikan kebolehgunaan ICT pada tahap yang optimum serta mengurangkan kesan insiden keselamatan ICT.

3.0 PERNYATAAN DASAR

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

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

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk memastikan ianya bebas daripada risiko yang mungkin berlaku.

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 dari segi pencerobohan, kecurian, pemindaan dan kehilangan data. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan 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 PNM merangkumi perlindungan ke atas 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 dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

4.0 SKOP

Aset ICT PNM terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT PNM 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 yang disampaikan serta melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT Jabatan/Agensi 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 PNM. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

b) Perisian

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

c) Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. 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 PNM. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod PNM, 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 PNM 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.

5.0 PRINSIP-PRINSIP

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

a) Hak Capaian atas dasar ‘perlu mengetahui’

Capaian terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna ICT tertentu atas dasar ‘perlu mengetahui’ sahaja. Hal ini bermakna capaian hanya akan diberikan sekiranya peranan dan fungsi pengguna ICT memerlukan maklumat tersebut. Pertimbangan untuk capaian adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan.

b) Hak Capaian Minimum

Hak capaian pengguna ICT hanya diberikan pada satu tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna ICT mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses akan dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna ICT (bidang/skop tugas);

c) Akauntabiliti

Semua pengguna ICT adalah bertanggungjawab penuh ke atas semua tindakannya terhadap aset ICT yang digunakannya, serta tertakluk kepada peranannya sebagai Pegawai Perakaunan seperti yang dinyatakan di dalam Arahan Perbendaharaan.

d) **Pengasingan**

Tugas mewujud, memadam, mengemaskinikan, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kegagalan, kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan pentadbiran dan kumpulan teknikal;

e) **Pengauditan**

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan ICT. Dengan itu, aset ICT seperti komputer, pelayan, '*router'*, '*firewall'* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan dan/atau jejak audit. Bagi memudahkan pengauditan dan mengekalkan integriti maklumat, log jejak audit juga perlu

dibuat penduaan (*backup*) seperti data-data penting lain sistem dan aplikasi.

f) **Pematuhan**

Dasar Keselamatan ICT ini hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk perlanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan infrastruktur ICT PNM yang boleh menyebabkan kebocoran maklumat, kegagalan fungsi serta boleh mengancam keselamatan negara.

g) **Pemulihan**

Pemulihan sistem amatlah perlu untuk memastikan kebolehfungsian dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan (*backup*) dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan; dan

h) **Saling Bergantungan**

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

6.0 TERAS DASAR

6.1 Pengguna ICT hendaklah meneliti teras dasar berikut semasa mengguna dan mengakses aset ICT Sektor Awam :

a) Semua sumber ICT Sektor Awam adalah hak milik Kerajaan; peralatan, perkakasan, perisian dan rangkaian; termasuklah data, maklumat yang tercatat atau yang diperoleh daripadanya. Kerajaan

sebagai pemilik, berhak memantau aktiviti pengguna ICT yang mengakses sumber-sumber ICT untuk mengesan salah guna atau penggunaan sumber ICT selain dari tujuan yang ditetapkan dan dibenarkan;

b) Semua pengguna ICT adalah bertanggungjawab ke atas tindakan masing-masing apabila mengakses aset ICT Sektor Awam. Pengguna ICT wajib memastikan akses yang diamanahkan kepadanya tidak disalah guna oleh dirinya sendiri atau pun pihak ketiga; dan

c) Semua pengguna ICT hanya diberikan hak akses minimum ke atas aset ICT Sektor Awam bagi mengurangkan risiko terhadap kecuaian atau penyalahgunaan sistem yang disengajakan. Kebenaran akses secara automatik tidak diberikan kepada pengguna ICT walau apa jua peringkat tapisan keselamatan pengguna ICT berkenaan.

7.0 PENILAIAN RISIKO KESELAMATAN ICT

PNM hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan vulnerability yang semakin meningkat hari ini. Justeru itu Jabatan 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.

Jabatan 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 Jabatan 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.

PNM 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.

PNM 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 agensi;

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

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

BAHAGIAN II - DASAR

01: PEMBANGUNAN DAN PENYELENGGARAAN DASAR

1.1 Dasar Pelaksanaan	**Tindakan**
Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah PNM selaku Pengerusi Jawatankuasa Pemandu ICT (JPICT) PNM, semua Pengarah Bahagian dan Pegawai Keselamatan ICT (ICTSO).	KP
1.2 Penyebaran Dasar	
Dasar ini bertujuan memastikan hala tuju pengurusan organisasi untuk melindungi aset ICT selaras dengan keperluan perundangan. Dasar ini perlu disebarkan kepada semua pengguna ICT PNM (termasuklah pegawai dan kakitangan; tetap, kontrak dan sementara, pembekal, penyedia perkhidmatan dan pakar runding yang berurusan dengan PNM.	ICTSO
1.3 Penyelenggaraan Dasar	
Dasar Keselamatan ICT PNM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Prosedur penyelenggaraan Dasar Keselamatan ICT PNM adalah seperti berikut: a) Mengkaji semula dasar ini sekurang-kurangnya satu (1) kali dalam masa satu (1) tahun bagi mengenal pasti, meneliti dan menentukan perubahan yang diperlukan jika terdapat perubahan dasar mengikut keperluan semasa ;	ICTSO

b) Mengemukakan cadangan perubahan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT); dan c) Memaklumkan perubahan dasar yang telah dipersetujui oleh JPICT kepada semua pengguna.	
1.4 Pemakaian Dasar	
Dasar Keselamatan ICT ini terpakai kepada semua pengguna ICT PNM dan **TIADA PENGECUALIAN** diberikan.	Pengguna ICT

BAHAGIAN II – DASAR

02: ORGANISASI KESELAMATAN

2.0 Ketua Pengarah PNM	**Tindakan**
Peranan dan tanggungjawab Ketua Pengarah PNM adalah seperti berikut: a) Memastikan pelaksanaan pasukan penyelaras keselamatan ICT ; b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT PNM; c) Memastikan semua keperluan (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi dan; d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT PNM.	Ketua Pengarah
2.1 Peranan Ahli Pasukan Penyelaras Keselamatan ICT	
2.1.1 Ketua Pegawai Maklumat (CIO)	
Timbalan Ketua Pengarah, adalah Ketua Pegawai Maklumat. Peranan dan tanggungjawab CIO adalah seperti berikut: a) Mewujud dan mengetuai pasukan penyelaras keselamatan ICT peringkat PNM; b) Menasihati Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; c) Menentukan keperluan keselamatan ICT;	CIO

d) Menyelaras pembangunan dan pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT dan; e) Memastikan semua pengguna ICT memahami peruntukan di bawah Dasar Keselamatan ICT PNM.	
2.1.2 Pengurus ICT	
Peranan dan tanggungjawabnya adalah seperti berikut: a) Membantu CIO dalam melaksanakan tugas-tugasnya yang melibatkan keselamatan ICT; b) Menentukan keperluan keselamatan ICT berdasarkan nasihat ICTSO; dan c) Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT.	Pengurus ICT
2.1.3 Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut : a) Mengurus keseluruhan program-program keselamatan ICT PNM; b) Menguatkuasakan dan memantau pematuhan Dasar Keselamatan ICT PNM; c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT PNM kepada semua pengguna; d) Mewujudkan garis panduan dan prosedur selaras	ICTSO

dengan keperluan Dasar Keselamatan ICT PNM; e) Menjalankan pengurusan risiko; f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan danmenyediakan 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 (GCERT) MAMPU dan memaklumkannya kepada ClO; i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT PNM dan memperakukan langkah-langkah pemulihan dengan segera; dan j) Memperakui proses pengambilan tindakan tatatertib ke atas pengguna ICT yang melanggar Dasar Keselamatan ICT PNM.	
2.1.4 Pentadbir Teknikal Operasi	
Peranan dan tanggungjawab Pengurus Teknikal Operasi yang dilantik adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT PNM; b) Menentukan kawalan akses semua pengguna ICT	Pentadbir Teknikal Operasi

terhadap aset ICT PNM; c) Melaporkan sebarang perkara atau penemuan/ ancaman keselamatan ICT PNM kepada ICTSO; dan d) Memastikan penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT dilaksanakan.	
2.1.5 Pentadbir Sistem ICT	
Peranan dan tanggungjawab Pentadbir Sistem ICT yang dilantik bagi sesuatu sistem/aplikasi adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT PNM; b) Memastikan keutuhan dan kerahsiaan kata laluan aset ICT PNM; c) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; d) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna ICT luar dan pihak ketiga yang bermula, berhenti atau tamat projek; e) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT PNM; f) Memantau aktiviti capaian pengguna;	Pentadbir Sistem ICT

g) Mengenalpasti aktiviti-aktiviti tidak normal seperti capaian tidak dibenarkan, pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; h) Menyimpan dan menganalisis rekod jejak audit; dan i) Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala dan/atau jika perlu.	
2.1.6 Jawatankuasa Keselamatan PNM	
Jawatankuasa Keselamatan ICT (JKICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT PNM. Bidang kuasa: (a) Memperakukan/meluluskan dokumen DKICT PNM; (b) Memantau tahap pematuhan keselamatan ICT; (c) Memperakukan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam Kementerian/ Jabatan/Agensi yang mematuhi keperluan DKICT; (d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; (e) Memastikan DKICT PNM selaras dengan dasar-dasar	Jawatankuasa Keselamatan ICT

ICT kerajaan semasa; (f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; (g) Membincang tindakan yang melibatkan pelanggaran DKICT PNM; (h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	
2.1.7 Pasukan Tindak Balas Insiden Keselamatan ICT CERT	
Keanggotaan Kementerian/Jabatan /Agensi CERT adalah berdasarkan Pekeliling Am Bil. 3 Tahun 2000 Rangka Dasar Keselamatan ICT Dan Komunikasi dan Surat Pekeliling Am Bilangan 4 Tahun 2006: Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam.	CERT PNM
2.1.8 Pengguna ICT PNM	
Peranan dan tanggungjawab adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT; b) Mengetahui dan memahami implikasi keselamatan ICT kesan dan tindakannya; c) Melepasi tapisan keselamatan (jika berkaitan); d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT PNM dan senantiasa menjaga kerahsiaan maklumat kerajaan; e) Melaksanakan langkah-langkah perlindungan	Pengguna ICT

seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa ketepatan dan kelengkapan maklumat dari semasa ke semasa; iii. Menentukan maklumat tersedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan dan menukarnya secara berkala; v. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberi perhatian kepada maklumat terperingkat terutamanya terutamanya semasa proses pewujudan, pemprosesan, penyimpanan, Penghantaran, penyampaian, pertukaran dan pemusnahan; vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT yang diambil untuk memastikan keselamatan maklumat dari diketahui umum; viii. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; dan ix. Mengambil tahu serta menghadiri program-program kesedaran mengenai keselamatan ICT.	
2.1.9 Pegawai Pengelasan Dokumen	

Pegawai Pengelasan Dokumen, PNM ialah seorang pegawai yang dilantik oleh Menteri Pelancongan Malaysia di bawah Akta Rahsia Rasmi 1972, perakuan di bawah Seksyen 2B yang dipertanggungjawab untuk mengelaskan apa-apa surat rasmi atau bahan sebagai 'Rahsia Besar', 'Rahsia', 'Sulit' dan 'Terhad'.	Pegawai Pengelasan Dokumen
2.1.10 Pihak Luar / Pihak Ketiga	
Pegawai dan kakitangan PNM hendaklah memastikan keselamatan penggunaan aset ICT, maklumat dan kemudahan yang digunakan oleh pihak luar/ketiga dikawal dan dipantau. Perkara-perkara berikut perlulah dipatuhi: a) Mengenal pasti segala risiko keselamatan maklumat serta melaksanakan kawalan capaian yang bersesuaian sebelum memberi kebenaran untuk mencapai aset ICT PNM; b) Capaian ke atas aset ICT PNM perlulah dihadkan dengan jelas melalui kontrak perjanjian jual beli/perkhidmatan yang dibuat dengan pihak ketiga; dan c) Perkara-perkara yang perlu diambil kira semasa menyediakan kontrak perjanjian adalah: i. Dasar Keselamatan ICT PNM; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; iv. Hak Harta Intelek; dan v. Mana-mana akta, pekeliling, garis panduan	Pengarah Bahagian, Pentadbir Teknikal Operasi, Pentadbir Sistem ICT Dan Pihak Ketiga

dan arahan yang berkaitan dengannya.	

BAHAGIAN II – DASAR

03: KAWALAN DAN PENGELASAN ASET

3.0 Inventori Aset ICT	**Tindakan**
3.0.1 Akauntabiliti Aset	
Memastikan semua aset ICT PNM diberi perlindungan yang sesuai oleh pengguna ICT yang bertanggungjawab ke atas semua aset ICT di bawah kawalannya. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua aset dikenal pasti dan maklumat aset di akaun dan direkodkan dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini; b) Memastikan semua aset ICT PNM mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan PNM; d) Bagi penggunaan aset ICT PNM hendaklah dikenal pasti, didokumen dan dilaksanakan; dan e) Setiap pengguna bertanggungjawab ke atas semua aset ICT PNM di bawah kawalannya.	Pegawai Aset dan Pengguna ICT PNM
3.2 Pengelasan Maklumat	
Memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan tahap sensitiviti masing- masing. Perkara yang perlu dipatuhi adalah seperti berikut:	Pegawai Pengelasan Dokumen

a) Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada Kerajaan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: i. Rahsia Besar; ii. Rahsia; iii. Sulit; atau iv. Terhad. b) Maklumat hendaklah dilabel dan dikendalikan berasaskan peringkat kategori keselamatan yang telah dikenal pasti selaras dengan peraturan prosedur yang ditetapkan oleh PNM.	
3.3 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengambil kira langkah- langkah keselamatan berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa, menyemak maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Memastikan maklumat tersedia untuk digunakan; d) Menjaga keutuhan dan kerahsiaan kata laluan; e) Mematuhi piawaian, prosedur dan garis panduan keselamatan yang dikeluarkan dari semasa ke	Pegawai Aset dan Pengguna ICT PNM

semasa; f) Memberikan perhatian kepada pengendalian maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	

BAHAGIAN II – DASAR

04: KESELAMATAN SUMBER MANUSIA

4.1 Tanggungjawab Keselamatan	**Tindakan**
Peranan dan tanggungjawab pengguna ICT terhadap keselamatan ICT mestilah direkod, dipatuhi dan dilaksanakan serta dinyatakan dengan jelas dan tepat di dalam fail meja atau kontrak kerja. Keselamatan ICT merangkumi tanggungjawab pengguna ICT dalam menyediakan dan memastikan perlindungan terhadap semua sumber dan aset ICT yang digunakan di dalam menjalankan tugas harian.	pengguna ICT
4.2 Terma dan Syarat Perkhidmatan	
Semua warga PNM adalah tertakluk kepada terma dan syarat perkhidmatan seperti yang ditetapkan di dalam Arahan Pentadbiran dan pekeliling-pekeliling serta arahan-arahan lain yang berkuat kuasa.	pengguna ICT
4.2.1 Sebelum Perkhidmatan	
Memastikan penjawat awam, kontraktor, pihak ketiga dan lain-lain pihak yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT Kerajaan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Peranan dan tanggungjawab penjawat awam, kontraktor, pihak ketiga dan lain-lain pihak yang berkepentingan ke atas	pengguna ICT

keselamatan ICT sebelum, semasa dan selepas perkhidmatan mestilah dinyatakan dengan lengkap dan jelas; b) Penyaringan dan pengesahan latar belakang calon untuk penjawat awam, kontraktor, pihak ketiga dan lain-lain pihak yang berkepentingan melalui tapisan keselamatan hendaklah dilakukan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c) Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	
4.2.2 Dalam Perkhidmatan	
Memastikan semua pengguna ICT di PNM sedar akan ancaman keselamatan ICT serta peranan dan tanggungjawab masing-masing untuk menyokong Dasar Keselamatan ICT dalam meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT Kerajaan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua pengguna ICT mengurus keselamatan berdasarkan perundangan dan	pengguna ICT

peraturan yang ditetapkan oleh PNM; b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan ICT diberi kepada semua pengguna ICT dan sekiranya perlu diberi kepada kontraktor, pihak ketiga dan lain-lain pihak yang berkepentingan dan semasa ke semasa; dan c) Memastikan adanya proses tindakan disiplin ke atas pengguna ICT diambil sekiranya berlaku perlanggaran dalam perundangan dan peraturan yang telah ditetapkan. 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 Khidmat Pengurusan dan Sumber Manusia, PNM.	
4.2.3 Bertukar atau Tamat Perkhidmatan	
Memastikan semua pengguna ICT PNM diurus dengan teratur apabila tamat perkhidmatan atau bertukar dari Kementerian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua aset ICT Kerajaan dikembalikan kepada mengikut peraturan	pengguna ICT

yang ditetapkan dan/atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh PNM dan/atau terma perkhidmatan.	
4.3 Peruntukan Akta Rahsia Rasmi	
Semua pengguna ICT yang menguruskan maklumat terperingkat adalah tertakluk kepada peruntukan Akta Rahsia Rasmi 1972.	pengguna ICT

BAHAGIAN II – DASAR

05: KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif: Mencegah capaian fizikal yang tidak dibenarkan ke atas aset ICT yang oleh mengakibatkan kecurian, kerosakan dan gangguan kepada aset, infrastruktur dan maklumat.

5.1 KESELAMATAN PERIMETER	**Tindakan**
Keselamatan perimeter adalah bertujuan untuk mengesan, mencegah dan menghalang cubaan untuk menceroboh ke kawasan yang menempatkan peralatan, maklumat dan kemudahan untuk mengakses dan memproses maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: a) Perimeter kawasan keselamatan fizikal hendaklah ditentukan dengan jelas dengan memberikan perlindungan yang kukuh dan munasabah kepada aset ICT penting / sensitif yang dilindungi berdasarkan hasil penilaian risiko; b) Mempamerkan papan tanda kawasan larangan c) Memperkukuhkan dan mengunci tingkap dan pintu masuk serta mengenakan kawalan keluar masuk; d) Memperkukuhkan dinding dan siling; e) Mengehadkan laluan keluar masuk; f) Mengadakan kaunter kawalan; g) Mewujudkan sistem keselamatan yang baik; h) Menyediakan tempat dan bilik khas untuk pelawat;	CIO dan ICTSO

i) Mewujudkan perkhidmatan kawalan keselamatan; dan j) Memasang alat penggera atau kamera litar tertutup.	
5.2 Kawalan Keluar Masuk	
Kawalan keluar masuk adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis / bangunan PNM. Perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap pengguna ICT hendaklah memakai atau mengenakan Kad Akses atau Tanda Nama di sepanjang waktu bertugas; b) Setiap pihak luar / pelawat hendaklah mendaftar dan diwajibkan mendapat Pas Keselamatan di kaunter perkhidmatan pelanggan yang ditempatkan di pintu masuk terlebih dahulu sebelum ke tempat berurusan dan hendaklah memulangkan semula pas setelah selesai menjalankan urusan; c) Semua Kad Akses Pejabat hendaklah diserahkan balik kepada PNM apabila penjawat awam, kontraktor, pihak ketiga dan lain-lain pihak yang berkepentingan telah tamat perkhidmatan atau bersara (jika berkaitan); d) Kehilangan Kad Akses Pejabat dan Perakam Waktu mestilah dilaporkan dengan segera kepada pihak Polis dan pihak pentadbiran PNM; e) Hanya pengguna ICT yang diberi kebenaran sahaja dibenarkan mencapai atau	pengguna ICT

menggunakan aset ICT PNM;	
5.3 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukannya kepada pegawai-pegawai PNM yang tertentu sahaja. Ia dilaksanakan bagi melindungi aset ICT yang terdapat di dalam perimeter tersebut. Kawasan larangan bagi keselamatan ICT ini meliputi Pusat Data, Bilik Server, Rak Switch di setiap bahagian dan Stor Peralatan ICT. Pihak luar / ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali dengan kebenaran oleh Pengarah Bahagian Teknologi Maklumat serta bertulis untuk memberikan perkhidmatan sokongan atau bantuan teknikal, serta hendaklah senantiasa diiringi oleh pegawai ICT yangbertanggungjawab semasa kerja – kerja berkaitan dijalankan. Pihak luar / ketiga hendaklah mengisi Buku Log Keluar / masuk Pusat Data BTM sebelum dan selepas membuat kerja – kerja penyelenggaraan dan disahkan oleh pegawai ICT daripada BTM untuk disahkan.	pengguna ICT
5.4 Keselamatan Aset ICT	
5.4.1 Perkakasan	
Perkakasan ICT yang berada di bawah kawalan pengguna ICT perlulah sentiasa dijaga dan dikawal dengan baik supaya ia boleh berfungsi apabila diperlukan. Perkara yang perlu dipatuhi adalah seperti berikut:	Pengguna ICT

a) Setiap pengguna ICT hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya lengkap seperti diterima semasa ditempatkan, berada di lokasinya (berdasarkan penempatan) serta berfungsi dengan baik; b) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan dilengkapi dengan ciri-ciri keselamatan; c) Setiap pengguna ICT adalah bertanggungjawab di atas kerosakan dan kehilangan perkakasan ICT di bawah kawalannya; d) Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada Pentadbir Teknikal Operasi. e) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera; f) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT; g) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan “OFF” apabila meninggalkan pejabat; dan h) Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan	

kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
5.4.2 Dokumen	
Langkah-langkah pengurusan dokumentasi yang baik dan selamat perlu dilaksanakan oleh pengguna ICT bagi memastikan keselamatan dan integriti maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; 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; e) Menggunakan petanda atau label keselamatan seperti ‘Rahsia Besar’, ‘Rahsia’, ‘Sulit’, ‘Terhad’ dan ‘Terbuka’ pada dokumen; f) Menggunakan enskripsi (*encryption*) ke atas dokumen terperingkat yang disediakan dan	Pengguna ICT

dihantar secara elektronik.	
5.4.3 Media Storan	
Media storan yang dimaksudkan termasuklah: a) Cakera Keras / 'Hard Drive'; b) Cakera Padat; c) Pita Magnetik; d) Pemacu Mudah Alih ('*Removable Hard Drive' / 'Thumb Drive'*); dan e) Media storan lain Keselamatan media storan perlu diberi perhatian khusus kerana ia\digunakan untuk menyimpan maklumat rasmi dan rahsia rasmi Kerajaan. Langkah-langkah pencegahan hendaklah diambil untuk memastikan kerahsiaan, integriti dan ketersediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat. Perkara yang perlu dipatuhi adalah seperti berikut: a) Menyediakan ruang penyimpanan dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b) Mengehadkan akses untuk memasuki kawasan penyimpanan media kepada mereka atau pengguna yang dibenarkan sahaja; c) Merekodkan sistem pengurusan media termasuk inventori, pergerakan, melabel dan mewujudkan penduaan (*backup*); d) Perkakasan *backup* hendaklah diletakkan di	Pengguna ICT

tempat yang terkawal; dan e) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; f) Proses pelupusan perlulah mengikut tatacara pelupusan yang ditetapkan. Penghapusan maklumat atau kandungan media yang tertentu perlulah mendapat kelulusan pemilik maklumat terlebih dahulu; dan g) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat.	
5.5 Keselamatan Prasarana Sokongan	
5.5.1 Kawalan Persekitaran	
Bagi menghindari kerosakan dan gangguan terhadap aset ICT, semua cadangan berkaitan infrastruktur sama ada untuk memperoleh, menyewa dan mengubahsuai hendaklah dirujuk terlebih dahulu kepada Ketua Pengarah PNM. Perkara yang perlu dipatuhi bagi menjamin keselamatan persekitaran adalah seperti berikut: a) Merancang dan menyediakan pelan keseluruhan susun atur bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya dengan teliti; b) Melengkapi semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti pintu	Pengguna ICT

berkunci, alat pencegah kebakaran dan pintu kecemasan; c) Memasang peralatan perlindungan di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d) Menyimpan bahan mudah terbakar di luar kawasan kemudahan penyimpanan aset ICT; e) Meletakkan semua bahan cecair di tempat yang bersesuaian dan berjauhan dan aset ICT; f) Pengguna ICT adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik, ketuhar gelombang mikro dan lain-lain berhampiran peralatan ICT; dan g) Menyemak dan menguji semua peralatan perlindungan sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	
5.5.2 Bekalan Kuasa	
Perkara yang perlu dipatuhi bagi menjamin keselamatan bekalan kuasa adalah seperti berikut: a) Melindungi semua peralatan ICT daripada kegagalan bekalan kuasa dengan menyalurkan bekalan kuasa yang sesuai dan mencukupi kepada peralatan ICT; b) Menggunakan peralatan sokongan seperti 'Uninterruptable Power Supply' (UPS) dan	Pentadbir Teknikal Operasi

Penjana Kuasa (‘Generator’) bagi peralatan ICT kritikal, terutamanya di Pusat Data; dan c) Menyemak dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.	
5.5.3 Prosedur Kecemasan	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap pengguna ICT hendaklah membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan oleh Pegawai Keselamatan Jabatan; b) Melaporkan insiden kecemasan persekitaran seperti kebakaran kepada Pegawai Keselamatan Kementerian; dan c) Mengadakan, menguji dan mengemas kini pelan kecemasan dari semasa ke semasa	Pengguna ICT
5.5.4 Keselamatan Kabel	
Kabel hendaklah dilindungi dari sebarang ancaman bagi mengelakkan kebocoran maklumat dan kegagalan fungsi sistem. Perkara berikut perlu dipatuhi dalam menjaga keselamatan pendawaian: a) Menggunakan kabel yang mengikut piawaian dan spesifikasi yang ditetapkan sahaja; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel	Pentadbir Teknikal Operasi

sepenuhnya bagi mengelakkan kerosakan dan '*wire tapping'*; dan d) Membuat pelabelan dan tetanda kabel menggunakan kod-kod tertentu untuk menjamin kerahsiaan maklumat.	
5.5.5 Penyelenggaraan dan Baik Pulih Peralatan ICT	
Perkakasan hendaklah di selenggara dengan betul bagi memastikan ketersediaan, kerahsiaan dan integriti maklumat dapat dipelihara. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua perkakasan ICT hanya boleh di selenggara dan di baik pulih oleh kakitangan teknikal IT atau kakitangan teknikal yang dibenarkan sahaja; b) Semua pengguna ICT adalah tidak dibenarkan sama sekali membuka 'casing', memformatkan, mengemaskinikan 'firmware' atau apa jua perkara berkaitan penukaran komponen pada peralatan ICT yang berada di bawah kawalannya; c) Memastikan semua perkakasan ICT perlu diselenggarakan dengan mematuhi prosedur dan spesifikasi pengeluar; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan dilakukan; dan e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut	Pentadbir Teknikal Operasi

jadual yang ditetapkan atau atas keperluan.	
5.5.6 Peminjaman Perkakasan Untuk Kegunaan Rasmi	
Perkakasan yang dipinjam untuk kegunaan rasmi di dalam dan di luar pejabat adalah terdedah kepada pelbagai risiko keselamatan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Melengkapkan borang peminjaman yang dikeluarkan, mendapat kelulusan Ketua Bahagian dan mengembalikan borang ke BTM PNM, selewat-lewatnya tiga (3) hari bekerja sebelum tarikh penggunaan bagi menjamin ketersediaan; b) Melindungi dan mengawal peralatan di sepanjang masa peminjaman; c) Mewujudkan penduaan (*backup*) bagi semua dokumen yang diwujud, disimpan dan dimanipulasikan pada peralatan yang dipinjam; d) Bertanggungjawab memastikan peralatan disimpan dan ditempatkan di tempat selamat semasa dipinjam; e) Mengadakan '*house keeping*' kepada peralatan semasa pemulangan bagi memastikan kebolehgunaan peralatan serta mengelakkan kebocoran maklumat; f) Memastikan aktiviti peminjaman dan	Pengguna ICT

pemulangan peralatan ICT direkodkan; dan g) Menyemak peralatan yang dipulangkan berada dalam keadaan baik dan lengkap.	
5.5.7 Peralatan Luar Yang Dibawa Masuk	
Bagi peralatan luar seperti komputer riba, komputer peribadi, peralatan mudah alih (PDA,Telefon pintar) dan sebagainya, yang dibawa masuk ke premis kerajaan, perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan peralatan yang dibawa masuk tidak mengancam keselamatan aset ICT PNM; b) Mendapat kelulusan Ketua Bahagian bagi membawa dan menggunakan peralatan luar yang dibawa ke pejabat; c) Mendapat kebenaran bertulis ICTSO untuk mencapai rangkaian dalaman melalui peralatan luar yang digunakan di pejabat; d) Memastikan peralatan yang dibawa bebas dari sebarang virus, '*spyware'* dan sebagainya sebelum disambungkan ke rangkaian PNM ; dan e) Memastikan peralatan luar yang dibawa keluar selepas digunakan di premis PNM tidak mengandungi sebarang maklumat Kerajaan.	Pengguna ICT
5.5.8 Pelupusan dan Kitar Semula Peralatan	

Peralatan ICT yang hendak dilupuskan perlulah melalui prosedur proses pelupusan sedia ada yang dikeluarkan melalui Arahan Perbendaharaan. Pelupusan perlulah dilakukan secara terkawal supaya ia mendatangkan faedah kepada PNM. Perkara yang perlu dipatuhi adalah seperti berikut: a) Menghapuskan semua kandungan peralatan khususnya maklumat rahsia rasmi terlebih dahulu melalui kaedah-kaedah pemadaman dan penghapusan yang ditetapkan sebelum melakukan proses pelupusan; b) Mewujudkan penduaan (*backup*) bagi semua dokumen yang masih diperlukan untuk disimpan dan rujukan pada masa hadapan; c) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan d) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut.	Pentadbir Teknikal Operasi

BAHAGIAN II – DASAR

06: PENGURUSAN OPERASI DAN KOMUNIKASI

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

6.1 PENGENDALIAN PROSEDUR OPERASI	**Tindakan**
Memastikan kemudahan pemprosesan maklumat dan beroperasi seperti yang ditetapkan dan berada dalam keadaan selamat. 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; dan c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pentadbir Teknikal Operasi
6.2 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	Pentadbir Teknikal Operasi

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

membangun, mengemaskinikan, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	
6.4 PROSEDUR PENGURUSAN INSIDEN ICT	
CERT PNM menerima aduan atau laporan daripada pengguna, laporan yang dikesan dari MYGSOC atau laporan dari sumber luar. Seterusnya, maklumat tentang insiden akan didaftarkan. Siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden tersebut. Laporan insiden kemudiannya dimaklumkan kepada GCERT MAMPU. Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan dipanjangkan kepada agensi penguatkuasaan undang-undang. CERT PNM yang diketuai oleh ICTSO akan menjalankan tindakan pengendalian secara capaian jauh (remote) atau on-site. Sekiranya laporan tersebut memerlukan bantuan GCERT MAMPU, permohonan akan dihantar bagi mendapatkan maklum balas GCERT MAMPU. Bagi laporan yang memerlukan bantuan daripada CERT agensi yang lain, permohonan akan dihantar melalui GCERT MAMPU dan khidmat nasihat akan disalurkan. CERT PNM seterusnya akan menyediakan laporan dan ICTSO mengesahkan sekiranya Pelan Kesinambungan Perkhidmatan (PKP) perlu diaktifkan atau sebaliknya. Pengesahan akan dihantar kepada CIO bagi	CERT PNM, Pentadbir Sistem ICT,Pentadbir Teknikal Operasi, Pentadbir Keselamatan ICT

mengaktifkan PKP. Laporan insiden yang tidak memerlukan PKP akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan.	
6.5 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PIHAK KETIGA	
Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga. 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.	Pentadbir Teknikal Pentadbir Sistem ICT Operasi, Pentadbir Keselamatan ICT
6.6 PERANCANGAN DAN PENERIMAAN SISTEM	
Bertujuan untuk mengurangkan risiko kegagalan fungsi dan gangguan sistem. Perkara yang perlu dipatuhi adalah seperti berikut:	Pentadbir Sistem ICT, Pentadbir Teknikal Operasi

a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus, ditentu dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; b) Keperluan kapasiti ini perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang; c) Kriteria penerimaan untuk sistem maklumat baru, peningkatan dan versi baru perlu ditetapkan dan ujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem; dan d) Penggunaan peralatan mestilah dipantau, ditala (‘*tuned*’) dan perancangan perlu dibuat bagi memenuhi keperluan kapasiti akan datang untuk memastikan prestasi sistem pada tahap optimum;	
6.7 PERLINDUNGAN DARI PERISIAN BERBAHAYA DAN MOBILE CODE	
Bertujuan melindungi integriti perisian dan maklumat daripada kebocoran atau kerosakan yang disebabkan oleh perisian-perisian yang berbahaya seperti virus, ‘*worm’*, ‘*trojan’* dan lain-lain. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memasang sistem keselamatan untuk	Pentadbir Sistem ICT, Pentadbir Teknikal Operasi, Pentadbir Keselamatan ICT

mengesan dan menyekat perisian berbahaya seperti Antivirus, *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), dan mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang berlesen dan berdaftar yang dilindungi di bawah Hak Cipta dan Harta Intelek; c) Mengimbas semua data, perisian atau sistem dengan anti virus sebelum menggunakannya; d) Mengemas kini definisi anti virus dari semasa ke semasa; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan ganti rugi sekiranya perisian tersebut mengandungi program berbahaya; h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; i) Mengedar amaran mengenai ancaman seperti	

serangan virus terhadap keselamatan aset ICT; j) Kawalan pencegahan, pengesanan dan pemulihan untuk melindungi daripada *maliCIOus code* dan program kesedaran pengguna ICT yang bersesuaian mesti dilaksanakan; k) Dalam keadaan *mobile code* dibenarkan, konfigurasinya hendaklah memastikan bahawa ianya beroperasi berdasarkan kepada dasar keselamatan yang jelas dan *mobile code* yang tidak dibenarkan perlu dielak; dan l) Penggunaan mobile code yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	
6.8 HOUSEKEEPING	
Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	Pengguna ICT
6.8.1 Penduaan (*Backup*)	
Bagi memastikan sistem dapat dipulihkan semula selepas berlakunya gangguan, salinan penduaan hendaklah dibuat secara berkala atau setiap kali konfigurasi berubah. Salinan pendua hendaklah direkodkan dan disimpan di lokasi yang berlainan (‘*off site*’). Perkara yang perlu dipatuhi adalah seperti berikut: a) Membuat salinan keselamatan ke atas semua	Pentadbir Sistem ICT

sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b) Membuat salinan penduaan ke atas semua data dan maklumat mengikut kesesuaian operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; c) Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d) Salinan maklumat dan perisian perlu dibuat dan diuji secara berkala berdasarkan kepada prosedur penduaan; dan; e) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan f) Firewall hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Sistem ICT.	
6.8.2 Data /Perisian Tidak Dibenarkan	
Bagi memastikan prestasi sistem dan mengekalkan kebolehgunaan peralatan, peralatan perlulah dibersihkan daripada data / perisian yang tidak dibenarkan seperti yang ditetapkan di dalam pekeliling dan arahan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan ruangan cakera keras storan	Pengguna ICT

sentiasa mencukupi untuk menyimpan data; b) Mengemaskinikan kandungan cakera dengan membuang data dan perisian yang tidak dibenarkan; dan c) Memastikan pengguna ICT tidak memasang perisian sendiri yang boleh mengganggu prestasi peralatan dan gangguan kepada rangkaian.	
6.9 PENGURUSAN KESELAMATAN RANGKAIAN	
Melindungi maklumat dalam rangkaian dan infrastruktur sokongan rangkaian secara bersistematik.	Pentadbir Sistem ICT, Pentadbir Keselamatan ICT
6.9.1 Kawalan Infrastruktur Rangkaian	
Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian serta mengekalkan kestabilan dan kebolehgunaan rangkaian. Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut: a) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem rangkaian; b) Ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian perlu dikenal pasti dan dimasukkan dalam mana-mana perjanjian perkhidmatan rangkaian sama ada perkhidmatan berkenaan disediakan secara	CIO, Pentadbir Sistem ICT, Pentadbir Teknikal Operasi

dalaman atau melalui khidmat luar; c) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; d) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dan risiko seperti banjir, gegaran dan habuk; e) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna ICT yang dibenarkan sahaja; f) Firewall hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan; g) Semua trafik keluar dan masuk hendaklah melalui firewall dan sistem tapisan kandungan di bawah kawalan PNM; h) Semua perisian *sniffer* atau *network analyzer* atau *Virtual Private Network* adalah dilarang dipasang pada komputer pengguna ICT kecuali mendapat kebenaran ICTSO; i) Memasang perisian *Intrusion Detection System* (IDS) , *Intrusion Prevention System* (IPS) dan *Web Application Firewall* (WAF) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat PNM;	

j) Memasang *Web Content Filter* pada *Internet Gated Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam PKPA 1/2003; k) Sebarang penyambungan rangkaian yang bukan di bawah kawalan PNM hendaklah mendapat kebenaran CIO dengan mendapat nasihat dari Pengurus ICT. l) Penggunaan modem sama ada modem berwayar (PSTN, ISDN, ADSL, SDSL, dsb) mahupun modem tanpa wayar (WiFi, iBurst, CSD, GPRS, EDGE, CDMA, WCDMA, UMTS, HSCSD, HSDPA, HSPA, LTE, dsb) adalah dilarang sama sekali bagi pengguna ICT di PNM; m) Memastikan keperluan perlindungan bersesuaian dan mencukupi bagi perkhidmatan yang lebih optimum; n) Penggunaan Rangkaian Tanpa Wayar LAN di PNM adalah terhad. Ia hendaklah mematuhi surat MAMPU dengan rujukan UPTM (5) 159/338/8 Jilid 30 (84) bertajuk 'Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-agensi Kerajaan'; o) Pengguna-pengguna ICT di bawah PNM melalui 1*Gov Net perlulah memaklumkan sebarang insiden kegagalan fungsi, kebocoran maklumat kepada ICTSO melalui Pengarah	

Bahagian masing-masing.	
6.10 PENGENDALIAN MEDIA	
Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	Pengguna ICT
6.10.1 Penghantaran Dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kelulusan dan kebenaran pemilik terlebih dahulu. Media yang mengandungi maklumat Kerajaan perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar daripada PNM.	Pengguna ICT
6.10.2 Penghapusan	
Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat. a) Rujuk Surat Pekeliling Perbendaharaan Bilangan 7 Tahun 1995 bertajuk 'Garis Panduan Pelupusan Peralatan Komputer' dan 1Pekeliling Perbendaharaan (1PP); b) Dasar Pengurusan Rekod Dan Arkib Elektronik Arkib Negara Malaysia; dan c) Garis Panduan Pengurusan Rekod Elektronik dibaca bersama-sama dokumen Rekod Elektronik dan Akta Arkib Negara 2003.	Pengurus Aset, Pentadbir Teknikal Operasi

6.10.3 Prosedur Pengendalian Media Dan Maklumat	
Prosedur ini bertujuan untuk mengendali dan melindungi maklumat daripada terdedah tanpa kebenaran atau disalah guna. Perkara yang perlu dipatuhi adalah seperti berikut: a) Semua media hendaklah dilabelkan mengikut tahap kelas kategori sesuatu maklumat; b) Mengehadkan dan menentukan capaian terhadap media dan maklumat kepada pengguna ICT yang dibenarkan sahaja; c) Mengehadkan pengedaran data untuk tujuan rasmi dan dibenarkan sahaja; d) Penyelenggaraan media dan maklumat hendaklah dikawal dan direkodkan bagi mengelakkan sebarang kerosakan dan kejadian yang tidak diingini; dan e) Semua media hendaklah disimpan di tempat yang berkunci dan selamat.	Pengguna ICT
6.10.4 Keselamatan Sistem Dokumentasi	
Dokumentasi sistem perlu dilindungi dari capaian yang tidak dibenarkan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b) Menyediakan dan memantapkan lagi keselamatan sistem dokumentasi dalam	Pentadbir Sistem ICT

rangkaian; dan c) Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	
6.10.5 Pengurusan Komunikasi Maklumat	
Memastikan keselamatan pertukaran maklumat dan perisian dalam PNM dan mana-mana entiti luar terjamin. Perkara yang perlu dipatuhi adalah seperti berikut: a) Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b) Perjanjian dan kontrak perlu diwujudkan untuk pertukaran maklumat dan perisian di antara PNM dan pihak luar; c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan dan penerimaan; d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan; e) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat PNM.	Pengguna ICT
6.11 INTERNET	
Capaian Internet perlu dikawal dan diurus bagi menjamin kebolehgunaan rangkaian dan mengelakkan	Pengguna ICT

gangguan kepada sistem dalam talian kementerian. Antara perkara yang perlu dipatuhi adalah seperti berikut: a) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan sahaja; b) Bahan yang diperoleh dan Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan; c) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet; d) Pengguna ICT hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah Hak Cipta dan Harta Intelek; e) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh PNM sahaja; f) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti newsgroup atau bulletin board atau media sosial. Walau bagaimana pun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Ketua Jabatan terlebih dahulu tertakluk kepada arahan dan peraturan yang	

telah ditetapkan; dan g) Maklumat lanjut mengenai keselamatan Internet bolehlah dirujuk melalui PKPA 1 / 2003 bertajuk 'Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan' dan mana-mana polisi berkaitan yang dikeluarkan oleh organisasi keselamatan ICT Kementerian.	
6.11.1 Pengurusan Mel Elektronik	
Maklumat yang terdapat dalam Mel Elektronik perlu dilindungi sebaik-baiknya bagi menghindari capaian atau sebaran maklumat yang tidak dibenarkan. Antara perkara yang perlu dipatuhi adalah seperti berikut: a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh PNM adalah untuk kegunaan rasmi sahaja; b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan; 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 kepilkan, sekiranya perlu, tidak melebihi	Pengguna ICT

sepuluh Megabait (10MB) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; f) Pengguna hendaklah mengelak dan membuka e-mel daripada penghantar yang tidak diketahui atau diragui, dan / atau kandungan / tajuk e-mel berunsur hasutan dan bermaksud negatif; 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 perlulah dihapuskan; j) Tapisan terhadap kandungan mel dibuat oleh pelayan bagi memastikan kandungan mel bersih, namun pengguna masih perlu berwaspada dalam membuka kandungan mel; k) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; l) Pentadbir E-mel akan memantau peti mel pengguna dari semasa ke semasa untuk memastikan keboleh gunaannya, dan melakukan housekeeping jika perlu atau jika	

pengguna tidak mematuhi peraturan yang berkuat kuasa; m) Pengguna perlu memastikan menggunakan kuota mel yang diberikan dengan sewajarnya; n) Tatacara penggunaan mel elektronik perlu merujuk PKPA 1/ 2003 bertajuk 'Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan' dan mana-mana polisi berkaitan yang dikeluarkan oleh organisasi keselamatan ICT PNM; o) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; p) Pengguna hendaklah bertanggungjawab ke atas pembersihan dan pengemaskinian mailbox masing-masing; q) Pembersihan e-mel hendaklah dibuat sekiranya mailbox didapati tidak aktif selama satu (1) bulan; dan r) Penghantaran lampiran dalam format / extension " *.exe, *.bat " dan " *.com" tidak dibenarkan;	
6.11.2 Perkhidmatan E-Dagang Dan Transaksi Dalam Talian	
Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta	Pengguna ICT, Pentadbir keselamatan ICT

pindaan yang tidak sah dapat dihalang. 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; c) Integriti maklumat yang disediakan dalam sistem untuk kegunaan awam perlu dilindungi untuk mengelakkan daripada pengubahsuaian yang tidak dibenarkan; dan d) Maklumat yang melibatkan transaksi dalam talian perlu dilindungi bagi mengelakkan transmisi yang tidak lengkap, mis-routing, pendedahan, pertindihan dan perubahan yang tidak dibenarkan.	
6.11.3 Paparan Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat umum adalah seperti berikut: a) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; b) Memastikan segala maklumat yang hendak dipaparkan telah disahkan dan diluluskan	Pentadbir sistem ICT

sebelum dimuat naik ke laman web; dan c) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian.	
6.11.4 Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding Dan Pihak-Pihak Lain Yang Terlibat	
Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal, pakar runding dan pihak-pihak lain yang terlibat. Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Memasukkan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat; b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari masa ke semasa; dan c) Pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyelenggarakan dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan	Pengurus ICT, Pentadbir Sistem ICT, Pentadbir keselamatan ICT

proses yang terlibat serta penilaian semula risiko.	
6.11.5 Pemantauan Dan Pengesanan	
Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Log Jejak 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 diwujudkan dan hasilnya perlu dipantau secara berkala; c) Kemudahan merekodkan dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; e) Kesalahan yang dilakukan perlu di log (rekod), di analisa dan di ambil tindakan sewajarnya; dan f) Masa yang berkaitan dengan sistem pemprosesan maklumat dalam PNM atau domain keselamatan perlu diselaraskan dengan satu sumber tepat yang dipersetujui.	Pentadbir Sistem ICT

6.12 PENGAUDITAN DAN FORENSIK ICT	
CERT ICTSO mestilah bertanggungjawab merekodkan dan menganalisis: a) Sebarang percubaan pencerobohan kepada sistem ICT PNM; b) Serangan kod perosak (*MaliCIOus Code*), halangan pemberian perkhidmatan (*Denial Of Service*), Spam, pemalsuan (*Forgery*), 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 bandwidth rangkaian; g) Aktiviti penyalahgunaan akaun e-mel; dan h) Aktiviti penukaran IP address selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Teknikal Operasi. Langkah-langkah yang perlu diambil adalah seperti berikut:	ICTSO

a) CERT ICTSO akan menentukan prosedur pengumpulan bahan bukti (cakera keras/media storan) yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan; b) Proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat; dan c) Sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, format laporan khas perlu disediakan. Semua proses dan hasil siasatan adalah **SULIT**.	
6.13 JEJAK AUDIT	
Setiap sistem mestilah mempunyai jejak audit. Jejak audit merekodkan aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan berdasarkan susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi ciri-ciri 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 ICT ke atas sistem ICT sama ada secara sah atau sebaliknya;	Pentadbir Sistem ICT, Pentadbir Teknikal Operasi

d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan; e) Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Akta Arkib Negara; f) Pentadbir Sistem hendaklah menyemak catatan jejak audit dari masa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
6.14 SISTEM LOG	
Fail log hendaklah disimpan untuk tempoh sekurang-kurangnya enam (6) bulan. Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti berikut: a) Fail log sistem pengoperasian; b) Fail log servis (contoh: web, e-mel); c) Fail log aplikasi (*Audit Trail*); dan d) Fail log rangkaian (Contoh: *Switch*, *Firewall*, *and IPS*). Pentadbir Sistem hendaklah melaksanakan perkara-perkara berikut: a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;	Pentadbir Sistem ICT, Pentadbir Teknikal Operasi

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 tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	

BAHAGIAN II – DASAR

07: KAWALAN CAPAIAN

7.0 KEPERLUAN KAWALAN CAPAIAN	
7.1 KAWALAN CAPAIAN	
Objektif: Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset dan sistem ICT PNM. Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna ICT yang berbeza. Ia perlu diwujudkan, direkodkan, didokumentasikan dan dikaji semula berasaskan keperluan keselamatan.	Pentadbir Sistem ICT
7.2 PENGURUSAN CAPAIAN PENGGUNA	
Mengawal capaian pengguna ICT ke atas aset ICT dan Sistem PNM.	Pentadbir Sistem ICT
7.2.1 Akaun Pengguna	
Setiap pengguna ICT adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna ICT dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a) Akaun yang diperuntukkan oleh PNM sahaja boleh digunakan; b) Akaun pengguna ICT mestilah unik dan hendaklah mencerminkan identiti pengguna; c) Akaun pengguna ICT 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	Pengguna ICT

sistem ICT terlebih dahulu; d) Pemilikan akaun pengguna ICT bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan PNM. 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 ICT atas sebab-sebab berikut: i. Pengguna ICT yang bercuti panjang dalam tempoh waktu melebihi sebulan; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	
7.2.2 Hak Capaian (Privileges)	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
7.2.3 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 PNM seperti berikut:	Pengguna ICT dan Pentadbir sistem ICT

a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;

b) Pengguna ICT hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;

c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus;

d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun;

e) Kata laluan windows dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;

f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;

g) Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula;

h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

i) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan;

j) Kata laluan hendaklah ditukar selepas 90 hari atau

selepas tempoh masa yang bersesuaian; k) Mengelakkan penggunaan semula kata laluan yang baru digunakan. l) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; m) Penggunaan kata laluan lama semasa proses penukaran kata laluan tidak dibenarkan; n) Kata laluan hendaklah disimpan dalam bentuk yang telah dienkripkan; dan o) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	
7.3 KAWALAN CAPAIAN RANGKAIAN	
Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	Pentadbir rangkaian keselamatan ICT
7.3.1 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Mewujudkan segmen rangkaian yang bersesuaian bagi membezakan di antara rangkaian PNM dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna ICT dengan peralatan yang	Pentadbir rangkaian keselamatan ICT

menepati kesesuaian penggunaannya; c) Memantau dan menguatkuasakan kawalan capaian pengguna ICT terhadap perkhidmatan rangkaian ICT; d) Capaian pengguna ICT jarak jauh (*remote user*) perlulah dikawal; e) Capaian fizikal dan logikal ke atas perkakasan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal; dan f) Semua rangkaian yang dikongsi (*Shared Networks*), terutama sekali yang keluar daripada rangkaian PNM, polisi perlu diwujudkan untuk mengawal capaian oleh pengguna.	
7.3.2 Capaian Internet	
Penggunaan internet di PNM hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan malicious code, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian PNM. Penggunaan internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna ICT yang dibenarkan menggunakan Internet atau sebaliknya. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan. Penggunaan proksi yang telah ditetapkan oleh PNM bagi mengawal akses Internet mengikut fungsi kerja dan mematuhi	Pentadbir rangkaian keselamatan ICT

pekeliling semasa yang dikeluarkan. Penggunaan teknologi (*Packet Shaper*) untuk mengawal aktiviti (*Video Streaming, Chat, Downloading*) adalah perlu bagi menguruskan penggunaan bandwidth yang maksimum dan lebih berkesan. Penggunaan modem peribadi untuk tujuan sambungan ke internet tidak dibenarkan sama sekali di pejabat. Pengguna ICT adalah dilarang melakukan aktiviti-aktiviti seperti berikut: a) Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; b) Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah; c) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;	
7.4 KAWALAN CAPAIAN SISTEM PENGOPERASIAN	
Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	Pentadbir rangkaian keselamatan ICT
7.4.1 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan	Pentadbir

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 ICT yang dibenarkan; dan b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a) Mengesahkan pengguna ICT yang dibenarkan; b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna ICT bertaraf super user; dan; c) Menjana amaran (*Alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem.	Sistem ICT
7.4.2 *Public Key Infrastructure* (PKI)	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan PKI hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; b) PKI hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c) Perkongsian PKI untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. PKI yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan d) Sebarang kehilangan, kerosakan dan kata laluan disekat	Pentadbir rangkaian keselamatan ICT

perlu dimaklumkan kepada Unit Perolehan, Bahagian Kewangan / MAMPU / JANM.	
7.5 CAPAIAN APLIKASI DAN MAKLUMAT	
Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di PNM adalah terhad kepada pengguna ICT dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi: a) Pengguna ICT hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna ICT hendaklah direkodkan bagi mengesan aktiviti-aktiviti yang tidak diingini; c) Memaparkan notis amaran pada skrin komputer pengguna ICT sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; f) Maklumat tarikh login terakhir hendaklah dipamerkan;	Pengguna ICT Dan Pentadbir Sistem ICT

dan g) Session timeout hendaklah dilaksanakan.	
7.6 KAWALAN CAPAIAN JARAK JAUH	
Capaian jarak jauh yang dimaksudkan merangkumi: a) Capaian daripada sistem rangkaian dalaman; dan b) Capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan *telecommuting*. Penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (*encryption*). Lokasi bagi akses ke sistem ICT PNM hendaklah dipastikan selamat. Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pengurus ICT. Pengguna ICT yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	Pengguna ICT, Pentadbir Sistem ICT, Pentadbir rangkaian keselamatan ICT
7.7 PERALATAN MUDAH ALIH	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan pergerakan perkakasan tersebut daripada kehilangan atau kerosakan; b) Peralatan mudah alih hendaklah disimpan atau dikunci di tempat yang selamat apabila tidak digunakan; c) Memastikan peralatan mudah alih yang dibawa keluar dari pejabat perlu disimpan dan dijaga dengan baik bagi	Pentadbir teknikal operasi

mengelakkan daripada kecurian; dan d) Mengaktifkan *remote wipe* sekiranya ada.	
7.8 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media storan hendaklah disimpan dengan teratur di tempat yang selamat dan berkunci bagi mengelakkan kebocoran maklumat, kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan sensitif dan penting terdedah sama ada di atas meja pengguna ICT atau di paparan skrin apabila pengguna ICT tidak berada di tempatnya. Perkara yang perlu dipatuhi adalah seperti berikut: a) Menggunakan kemudahan password screen saver atau logout apabila meninggalkan komputer; b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; c) Memastikan pemacu storan seperti disket, 'flash drive' , cakera padat, cakera keras luaran yang mengandungi maklumat Kerajaan dikeluarkan / dilucutkan daripada komputer; dan; d) Memastikan semua dokumen diambil dari mesin pencetak, mesin pengimbas, mesin fotokopi esin faksimili.	Pengguna ICT

BAHAGIAN II – DASAR

08: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

Objektif: Memastikan system yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

8.1 KEPERLUAN KESELAMATAN SISTEM MAKLUMAT	**Tindakan**
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.	Pentadbir Sistem ICT dan ICTSO, Pentadbir rangkaian keselamatan ICT
8.1.1 Pengesahan Data Input Dan Output	

Data input dan data output bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.	Pentadbir Sistem ICT
8.1.2 Kawalan Prosesan	
Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan.	Pentadbir Sistem ICT
8.2 KAWALAN KRIPTOGRAFI	
Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi yang merangkumi data di dalam sistem rangkaian, sistem aplikasi dan pangkalan data. Kriptografi turut merangkumi kaedah-kaedah seperti berikut: a) Enkripsi Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (*Encryption*) pada setiap masa. b) Tandatangan Digital Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. c) Pengurusan Infrastruktur Kunci Awam/Public Key Infrastructure (PKI) Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.	Pentadbir Sistem ICT
8.3 KESELAMATAN FAIL SISTEM	

Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau/dan pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b) Kod atau atur cara sistem yang telah dikemaskinikan 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) Mengaktifkan log audit bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; dan e) Data ujian hendaklah dipilih dan penggunaannya dikawal serta dilindungi.	Pentadbir Sistem ICT
8.4 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN	
Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	Pentadbir Sistem ICT
8.4.1 Prosedur Kawalan Perubahan	
Perubahan atau pengubahsuaian ke atas sistem maklumat,sistem pengoperasian dan aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum diguna pakai.	Pentadbir Sistem ICT
8.4.2 Pembangunan Secara *Outsource*	
Pembangunan perisian aplikasi secara *outsource* perlu dipantau	Pengarah,

oleh Pengarah Bahagian / Pengurus ICT. Source Code adalah menjadi hak milik Kerajaan Malaysia.	Pengurus ICT
8.4.3 Kebocoran Maklumat	
Sebarang peluang untuk membocorkan maklumat melalui apa cara sekalipun mestilah dihalang.	ICTSO, Pengurus ICT
8.4.4 Kawalan Terhadap Keterdedahan Teknikal	
Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memperoleh maklumat keterdedahan teknikal sistem maklumat yang digunakan; b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT

BAHAGIAN II – DASAR

09: PENGURUSAN INSIDEN KESELAMATAN ICT

9.1 MEKANISME PELAPORAN INSIDEN KESELAMATAN ICT	
a) Pelaporan Insiden Keselamatan ICT Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO dan CERT PNM untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah **SULIT**, dan hanya boleh didedahkan kepada pihak- pihak yang dibenarkan. b) CERT PNM Pasukan CERT PNM akan bertindak dan menghubungi GCERT sebagai makluman atau bagi mendapatkan bantuan. c) Tanggung jawab Pengguna Semua kakitangan, pembekal, pakar runding dan pihak-pihak lain yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden keselamatan ICT bagi mengelakkan kerosakan bahan bukti. d) Tindakan Dalam Keadaan Berisiko Tinggi Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian	CIO, ICTSO, Pengarah, Pengurus ICT

insiden merebak.

e) Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan GCERT dengan kadar segera:

   i. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak- pihak yang tidak diberi kuasa;

   ii. Sistem maklumat digunakan tanpa kebenaran atau yang disyaki sedemikian;

   iii. Kata laluan atau mekanisme kawalan akses yang hilang, dicuri, didedahkan atau yang disyaki sedemikian;

   iv. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal berfungsi atau dicapai, dan komunikasi tersalah hantar; dan

   v. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka yang boleh menjejaskan keselamatan ICT.

f) Prosedur pelaporan insiden keselamatan ICT berdasarkan:

   i. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan

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

Rajah 1: Aliran Proses Pelaporan Insiden Keselamatan ICT	
9.2 PENGURUSAN MAKLUMAT INSIDEN KESELAMATAN ICT	
Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT. Pasukan perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur pengurusan pelaporan dan pengendalian insiden keselamatan ICT CERT PNM Pengendalian insiden keselamatan ICT perlu diuruskan dengan cepat, teratur dan berkesan, mengikut prosedur dengan mengambil kira kawalan-kawalan berikut: a) Mengenal pasti semua jenis insiden keselamatan ICT; b) Mematuhi Pelan Pemulihan Bencana (DRP) seperti yang telah digariskan dalam Pelan Kesinambungan Perkhidmatan (PKP); c) Menyimpan jejak audit dan memelihara bahan bukti dan rekod; d) Menyediakan tindakan pencegahan supaya insiden serupa tidak berulang; dan e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	CERT PNM

BAHAGIAN II – DASAR

10: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

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

10.1 DASAR KESINAMBUNGAN PERKHIDMATAN	
10.1.1 Pelan Pengurusan Kesinambungan Perkhidmatan	**Tindakan**
Kesinambungan Perkhidmatan (*Business Continuity Management* - BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh iambil bagi mengekalkan kesinambungan perkhidmatan. 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 bisness 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 ICT mengenai prosedur kecemasan; f) Membuat salinan pendua (*backup*); dan	**Koordinator PKP**

g) Menguji dan mengemas kini pelan sekurang - kurangnya setahun sekali. Pengurusan Kesinambungan Perkhidmatan (*Business Continuity Planning*) adalah mekanisme bagi mengurus dan memastikan kepentingan stakeholder sistem penyampaian perkhidmatan dilindungi dan imej PNM terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan PNM di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan. Ketua Jabatan adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT PNM. Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; b) Senarai pegawai PNM dan vendor berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai kebarangkalian berlaku dan kesan sekiranya berlaku; c) Merancang dan melaksana peraturan kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; Hanya satu rangka pelan kesinambungan perkhidmatan yang menyeluruh dibangunkan, didokumentasikan, dipersetujui oleh	

pengurusan; dan Menguji dan mengemas kini pelan kesinambungan perkhidmatan untuk memastikan ia berkesan. 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 pegawai yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. PNM hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

BAHAGIAN II – DASAR

11: PEMATUHAN

Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran Dasar Keselamatan ICT PNM.

11.1 PEMATUHAN DAN KEPERLUAN PERUNDANGAN	
11.1.1 Pematuhan Dasar	**Tindakan**
Semua pengguna ICT di PNM wajib membaca, memahami dan mematuhi Dasar Keselamatan ICT PNM di dalam undang-undang, akta-akta, pekeliling-pekeliling, peraturan-peraturan dan arahan-arahan lain yang berkaitan yang berkuat kuasa dari masa ke semasa. Kesemua aset ICT di PNM termasuk maklumat yang disimpan di dalamnya adalah hak milik kerajaan. Ketua Jabatan / Bahagian melalui Pegawai Kanan yang dipertanggungjawabkan perlu memantau perlakuan dan tindak- tanduk kakitangan di bawah seliaannya dari melakukan perkara-perkara yang mengarah kepada pelanggaran Dasar Keselamatan ICT.	Pengguna ICT
11.2 KEPERLUAN PERUNDANGAN	
Dasar ini bertujuan memastikan reka bentuk, operasi, penggunaan dan pengurusan sistem maklumat adalah selaras serta berkeupayaan menghalang perlanggaran mana-mana keperluan perundangan, peraturan dan perjanjian yang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut: a) Semua perlembagaan, undang-undang, peraturan, perjanjian yang dimeterai dan lain-lain perkara yang relevan kepada keselamatan sistem maklumat dan	Pengguna ICT

organisasi hendaklah dikenal pasti, di dokumentasikan dan dikemas kini; b) Peraturan yang sesuai dilaksanakan untuk pematuhan ke atas perlembagaan, undang-undang dan keperluan kontrak mengenai penggunaan bahan yang tertakluk kepada hak milik Harta Intelek; c) Rekod penting hendaklah dilindungi daripada hilang, rosak dan dipalsukan selaras dengan keperluan undang-undang, peraturan dan keperluan perjanjian Kementerian; d) Perlindungan ke atas data dan hak milik peribadi hendaklah mematuhi perundangan, peraturan dan terma perjanjian jika perlu; e) Pengguna ICT dilarang menggunakan kemudahan proses maklumat untuk tujuan yang tidak dibenarkan; dan f) Penggunaan kriptografi dikawal selaras dengan perjanjian, perundangan dan peraturan yang berkuat kuasa. g) Berikut adalah keperluan perundangan atau peraturan- peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna ICT di PNM : i. Arahan Teknologi Maklumat; ii. Arahan Keselamatan; iii. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk ‘Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan’;	

iv. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk ‘Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)’; v. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk ‘Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan’; vi. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk ‘Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam’; vii. Akta Tanda Tangan Digital 1997; viii. Akta Jenayah Komputer 1997; ix. Akta Hak cipta (Pindaan) Tahun 1997; x. Akta Komunikasi dan Multimedia 1998;Keselamatan Teknologi Maklumat dan Komunikasi (ICT)’; xi. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk ‘Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan’; xii. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk ‘Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam’; xiii. Akta Tanda Tangan Digital 1997; xiv. Akta Jenayah Komputer 1997; xv. Akta Hak cipta (Pindaan) Tahun 1997;	

xvi. Akta Komunikasi dan Multimedia 1998;	
11.3 PEMATUHAN KEPADA DASAR, PIAWAIAN DAN TEKNIKAL KESELAMATAN	
Dasar ini bertujuan memastikan keselamatan maklumat disemak secara berkala supaya patuh dan selaras dengan dasar dan piawaiankeselamatan PNM. Perkara yang perlu dipatuhi adalah seperti Berikut: a) Pegawai penyelia hendaklah memastikan bahawa semua peraturan keselamatan di bawah kawal selia masing–masing dipatuhi selaras dengan perundangan, peraturan dan lain-lain keperluan keselamatan; dan b) Sistem maklumat hendaklah disemak dan diuji secara berkala untuk pastikan mematuhi pelaksanaan standard keselamatan yang ditetapkan.	Pengguna ICT
11.4 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.	Pentadbir Sistem ICT

LAMPIRAN 1

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT PNM

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 PNM; dan

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

Tanda Tangan : ……..

Tarikh : ……

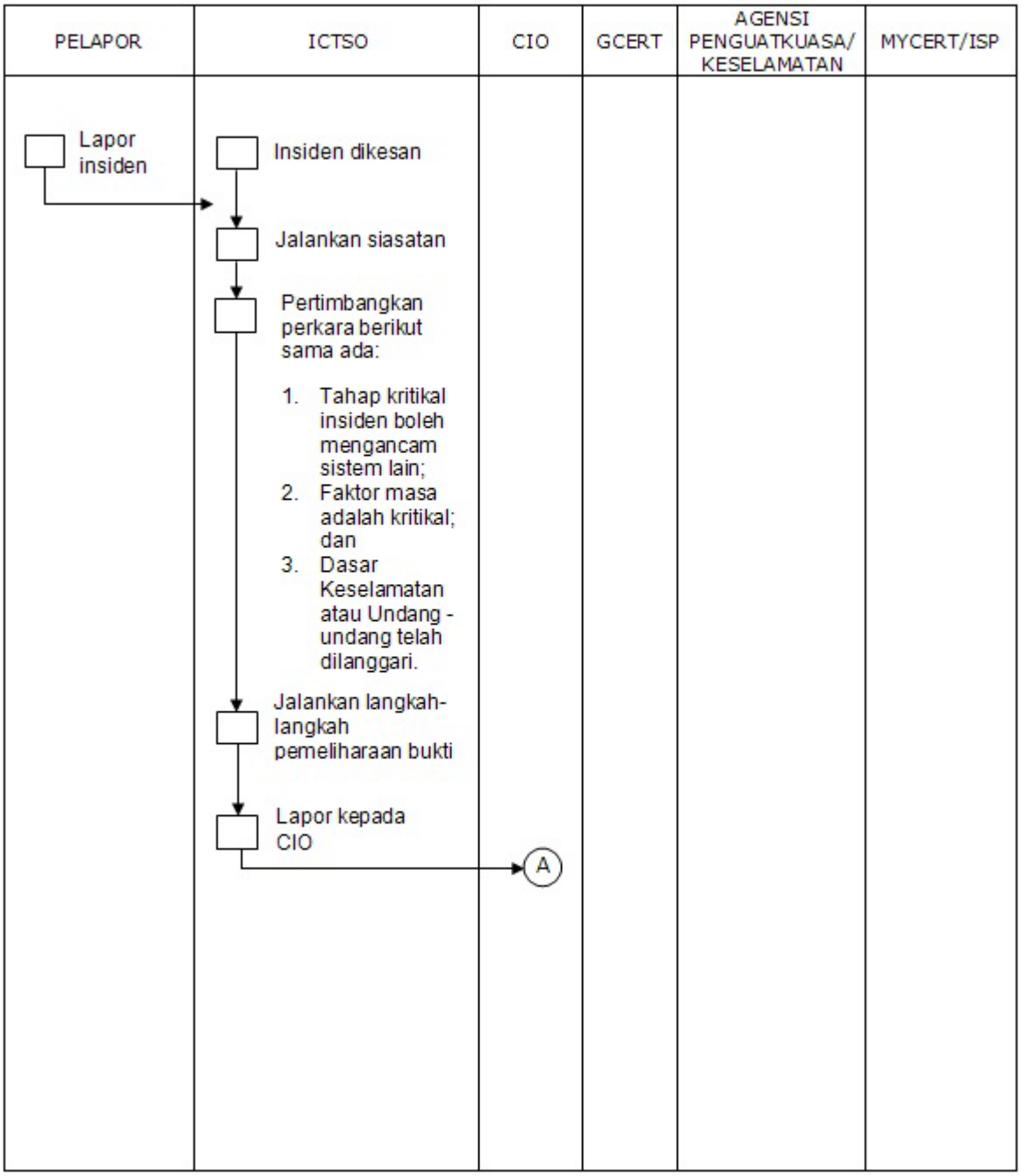
Pengesahan Pegawai Keselamatan ICT

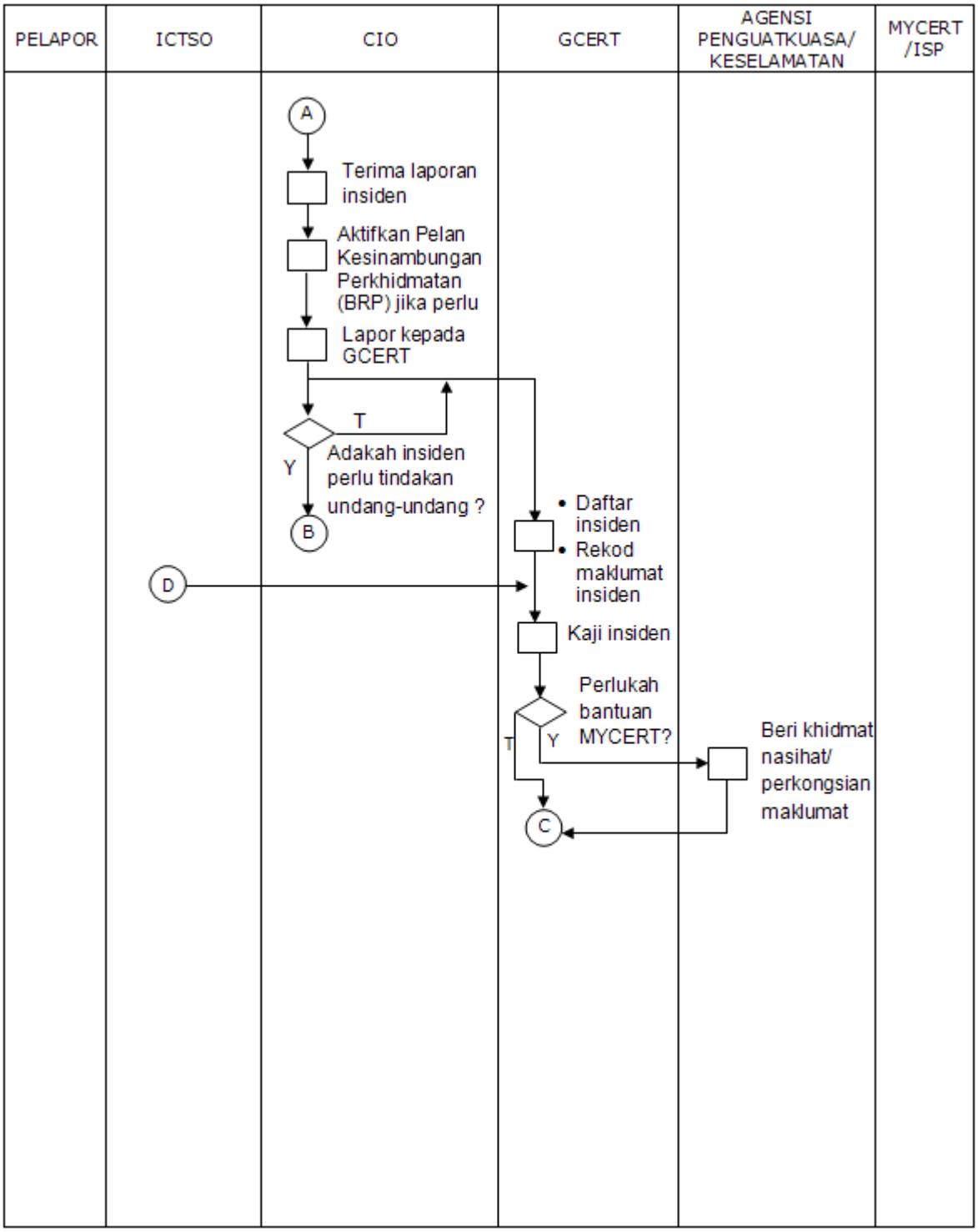
.....

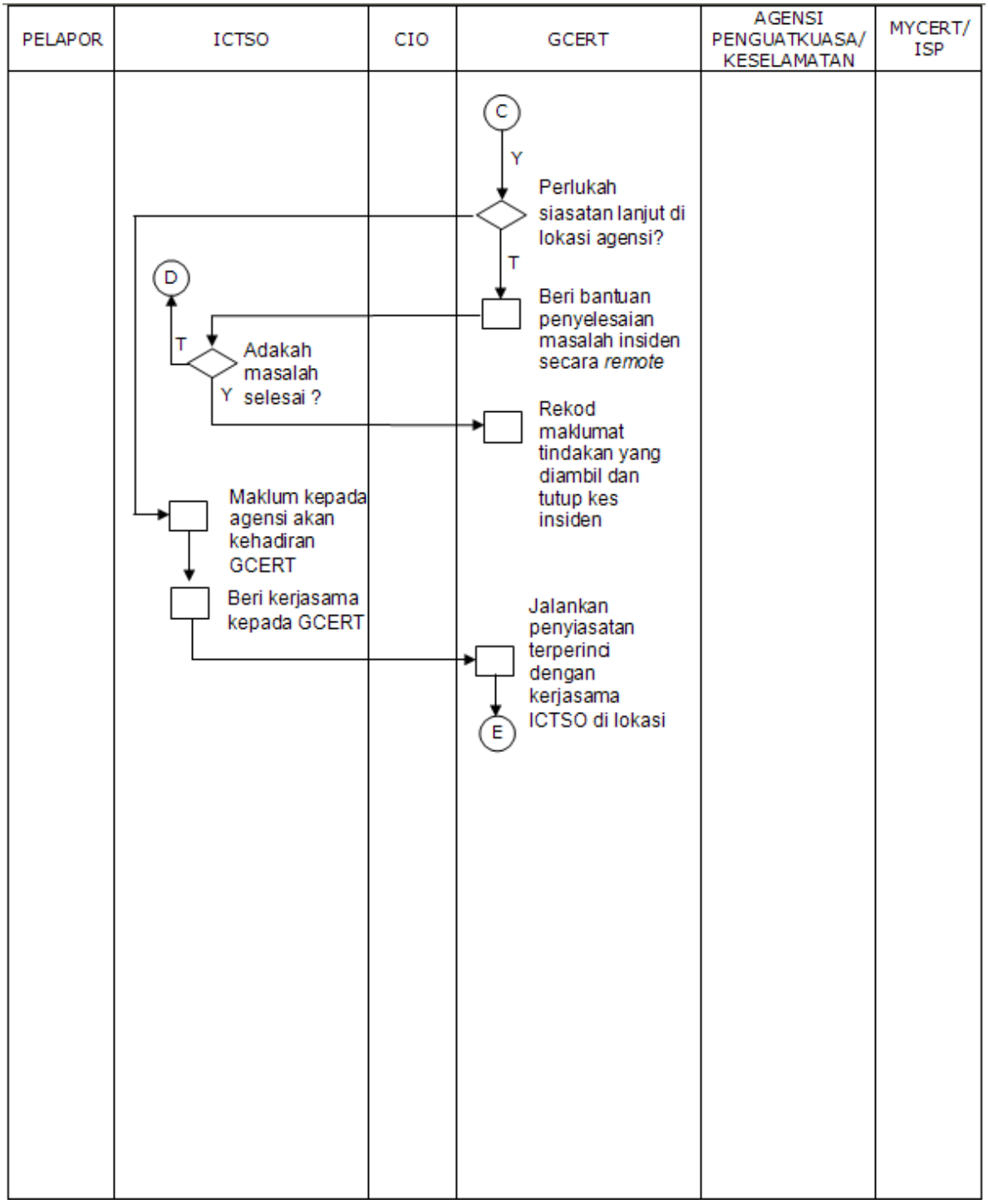
(Nama Pegawai CIO)

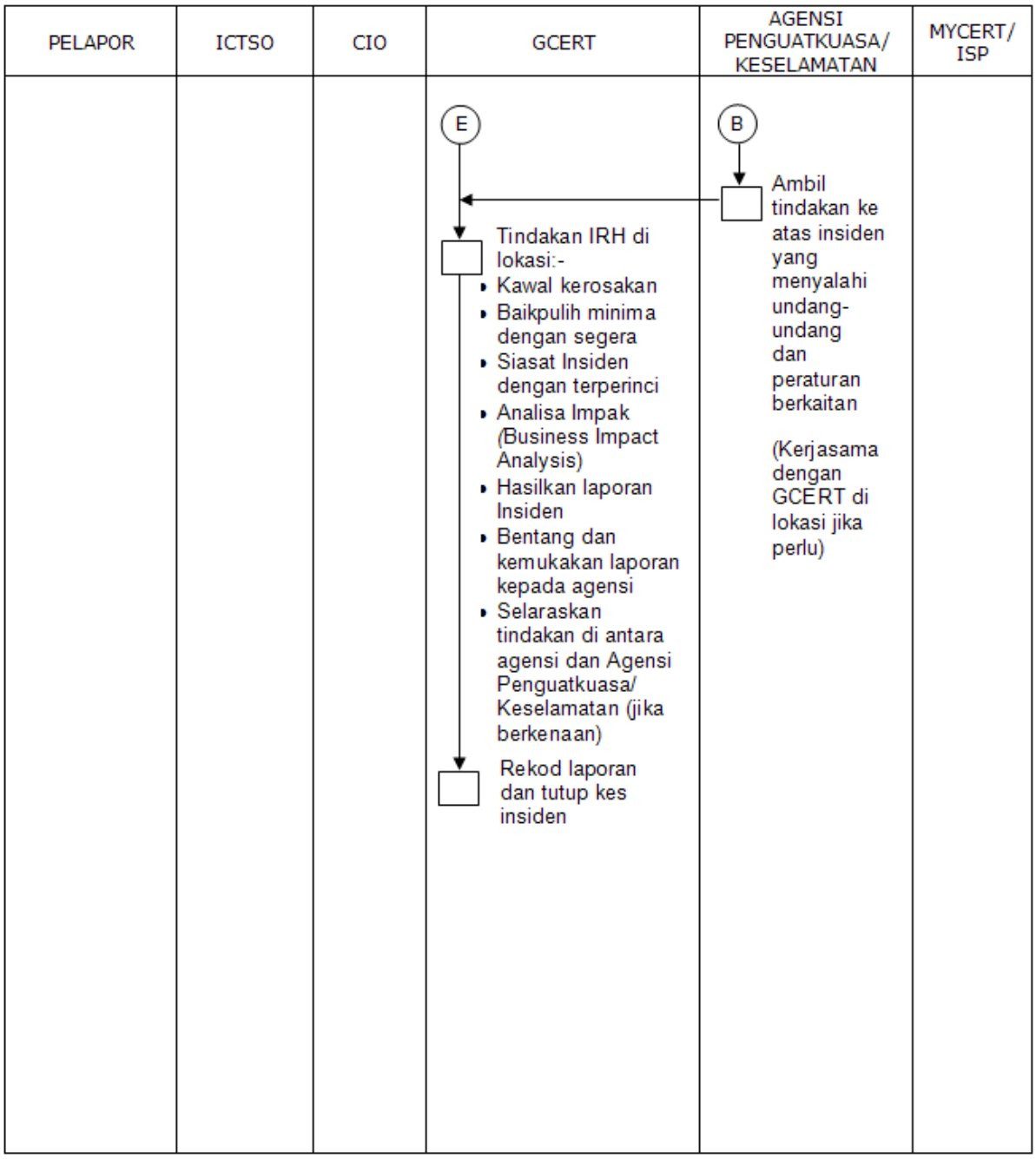
Tarikh: .....

Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT KPK




PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT /ISP
A
Terima laporan insiden
Aktifkan Pelan Kesinambungan Perkhidmatan (BRP) jika perlu
Lapor kepada GCERT
T
Y
Adakah insiden perlu tindakan undang-undang ?
B
D
• Daftar insiden
• Rekod maklumat insiden
Kaji insiden
Perlukah bantuan MYCERT?
T
Y
Beri khidmat nasihat/ perkongsian maklumat
C


PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT/ ISP
C
Y
Perlukah siasatan lanjut di lokasi agensi?
T
Beri bantuan penyelesaian masalah insiden secara remote
D
T
Adakah masalah selesai ?
Y
Rekod maklumat tindakan yang diambil dan tutup kes insiden
Maklum kepada agensi akan kehadiran GCERT
Beri kerjasama kepada GCERT
Jalankan penyiasatan terperinci dengan kerjasama ICTSO di lokasi
E


PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT/ ISP
E
B
Ambil tindakan ke atas insiden yang menyalahi undang-undang dan peraturan berkaitan
(Kerjasama dengan GCERT di lokasi jika perlu)
Tindakan IRH di lokasi:-
Kawal kerosakan
Baikpulih minima dengan segera
Siasat Insiden dengan terperinci
Analisa Impak (Business Impact Analysis)
Hasilkan laporan Insiden
Bentang dan kemukakan laporan kepada agensi
Selaraskan tindakan di antara agensi dan Agensi Penguatkuasa/ Keselamatan (jika berkenaan)
Rekod laporan dan tutup kes insiden