ISI KANDUNGAN

PENGENALAN 6
OBJEKTIF 7
PERNYATAAN DASAR 8
SKOP 10
PRINSIP-PRINSIP 13
PENILAIAN RISIKO KESELAMATAN ICT 17
PERKARA 1.0 PEMBANGUNAN DAN PENYELENGGARAAN DASAR 19
1.1 Dasar Keselamatan ICT 19
1.1.1 Pelaksanaan Dasar 19
1.1.2 Penyebaran Dasar 19
1.1.3 Penyelenggaraan Dasar 19
1.1.4 Pengecualian Dasar 20
PERKARA 2.0 ORGANISASI KESELAMATAN 21
2.1 Infrastuktur Organisasi Dalaman 21
2.1.1 Ketua Eksekutif PTPTN 21
2.1.2 Ketua Pegawai Maklumat (CIO) 22
2.1.3 Pegawai Keselamatan ICT (ICTSO) 22
2.1.4 Pengurus ICT 24
2.1.5 Pentadbir Sistem ICT 24
2.1.6 Pengguna 25
2.1.7 JawatanKuasa Keselamatan ICT PTPTN 26
2.1.8 Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (GCERT) 28
2.2 Pihak Ketiga 29
2.2.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga 29
PERKARA 3.0 PENGURUSAN ASET 31
3.1 Akauntabiliti Aset 31
3.1.1 Inventori Aset ICT 31

3.2 Pengelasan dan Pengendalian Maklumat..... 32
3.2.1 Pengelasan Maklumat..... 32
3.3.2 Pengendalian Maklumat..... 32
PERKARA 4.0 KESELAMATAN SUMBER MANUSIA..... 34
4.1 Keselamatan Sumber Manusia Dalam Tugasan Harian..... 34
4.1.1 Sebelum Perkhidmatan 34
4.1.2 Dalam Perkhidmatan..... 35
4.1.3 Bertukar Atau Tamat Perkhidmatan..... 35
PERKARA 5.0 KESELAMATAN FIZIKAL DAN PERSEKITARAN..... 37
5.1 Keselamatan Kawasan..... 37
5.1.1 Kawalan Keselamatan..... 37
5.1.2 Kawalan Masuk Fizikal..... 38
5.1.3 Kawalan Larangan..... 39
5.2 Keselamatan Peralatan..... 40
5.2.1 Peralatan ICT..... 40
5.2.2 Media Storan..... 43
5.2.3 Media Tandatangan Digital..... 44
5.2.4 Media Perisian dan Aplikasi..... 44
5.2.5 Penyelenggaraan Perkakasan..... 45
5.2.6 Peralatan di Luar Premis..... 46
5.2.7 Pelupusan Perkakasan..... 46
5.3 Keselamatan Persekitaran..... 48
5.3.1 Kawalan Persekitaran..... 48
5.3.2 Bekalan Kuasa..... 49
5.3.3 Kabel..... 50
5.3.4 Prosedur Kecemasan..... 51
5.4 Keselamatan Dokumen..... 51
5.4.1 Dokumen..... 51
PERKARA 6.0 PENGURUSAN OPERASI DAN KOMUNIKASI..... 53
6.1 Pengurusan Prosedur Operasi 53
6.1.1 Pengendalian Prosedur 53

6.1.2 Kawalan Perubahan..... 53
6.1.3 Pengasingan Tugas dan Tanggungjawab..... 54
6.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga 55
6.2.1 Perkhidmatan Penyampaian 55
6.3 Perancangan dan Penerimaan Sistem..... 55
6.3.1 Perancangan Kapasiti..... 56
6.3.2 Penerimaan Sistem..... 56
6.4 Perisian Berbahaya..... 56
6.4.1 Perlindungan dari Perisian Berbahaya..... 56
6.4.2 Perlindungan dari *Mobile Code*..... 58
6.5 *Housekeeping*..... 58
6.5.1 *Backup*..... 58
6.6 Pengurusan Rangkaian..... 59
6.6.1 Kawalan Infrastuktur Rangkaian..... 59
6.7 Pengurusan Media..... 61
6.7.1 Penghantaran dan Perpindahan..... 61
6.7.2 Prosedur Pengendalian Media..... 61
6.7.3 Keselamatan Sistem Dokumentasi..... 62
6.8 Pengurusan Pertukaran Maklumat..... 62
6.8.1 Pertukaran Maklumat..... 62
6.8.2 Pengurusan Mel Elektronik (E-mel)..... 63
6.9 Perkhidmatan E-Dagang (*Electronic Commerce Services*)..... 65
6.9.1 E-Dagang..... 65
6.9.2 Maklumat Umum..... 66
6.10 Pemantauan..... 66
6.10.1 Pengauditan dan Forensik ICT..... 66
6.10.2 Jejak Audit..... 67
6.10.3 Sistem Log..... 68
6.10.4 Pemantauan Log..... 69
PERKARA 7.0 KAWALAN CAPAIAN..... 71
7.1 Dasar Kawalan Capaian..... 71

7.1.1 Keperluan Kawalan Capaian..... 71
7.2 Pengurusan Capaian Pengguna..... 72
7.2.1 Akaun Pengguna..... 72
7.2.2 Hak Capaian..... 73
7.2.3 Pengurusan Kata Laluan..... 73
7.2.4 *Clear Desk* dan *Clear Screen*..... 75
7.3 Kawalan Capaian Rangkaian..... 75
7.3.1 Capaian Rangkaian..... 75
7.3.2 Capaian Internet..... 76
7.4 Kawalan Capaian Sistem Pengoperasian..... 79
7.4.1 Capaian Sistem Pengoperasian..... 79
7.5 Kawalan Capaian Aplikasi dan Maklumat..... 78
7.5.1 Capaian Aplikasi dan Maklumat..... 78
7.6 Peralatan Mudah Alih dan Kerja Jarak Jauh..... 81
7.6.1 Peralatan Mudah Alih..... 82
7.6.2 Kerja Jarak Jauh..... 82
PERKARA 8.0 PEROLEHAN, PEMBANGUNAN, DAN PENYELENGGARAAN SISTEM..... 83
8.1 Keselamatan Dalam Membangunkan Sistem dan Aplikasi..... 83
8.1.1 Keperluan Keselamatan Sistem Maklumat..... 83
8.1.2 Pengesahan Data *Input* dan *Output*..... 84
8.2 Kawalan Kriptografi..... 84
8.2.1 Enkripsi..... 84
8.2.2 Tandatangan Digital..... 84
8.2.3 Pengurusan Infrastuktur Kunci Awam (PKI)..... 85
8.3 Keselamatan Fail Sistem..... 85
8.3.1 Kawalan Fail Sistem..... 85
8.4 Keselamatan Dalam Proses Pembangunan dan Sokongan 86
8.4.1 Prosedur Kawalan Perubahan..... 86
8.4.2 Pembangunan Perisian Secara *Outsource* 87
8.5 Kawalan Teknikal Keterdedahan (*Vulnerability*) 87

8.5.1 Kawalan dari Ancaman Teknikal..... 87

PERKARA 9.0 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN 88

9.1 Mekanisme Pelaporan Insiden Keselamatan ICT..... 88

9.1.1 Mekanisme Pelaporan..... 88

9.2 Pengurusan Maklumat Insiden Keselamatan ICT..... 89

9.2.1 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT 89

PERKARA10.0 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN..... 91

10.1 Dasar Kesinambungan Perkhidmatan..... 91

10.1.1 Pelan Kesinambungan Perkhidmatan..... 91

PERKARA11.0 PEMATUHAN..... 94

11.1 Pematuhan dan Keperluan Perundangan..... 94

11.1.1 Pematuhan Dasar..... 94

11.1.2 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal 95

11.1.3 Pematuhan Keperluan Audit..... 95

11.1.4 Keperluan Perundangan..... 95

11.1.5 Pelanggaran Dasar..... 95

GLOSARI..... 96

Lampiran 1..... 100

Lampiran 2..... 101

Lampiran 3..... 105

PENGENALAN

Peningkatan penggunaan ICT dalam tugasan seharian terutama yang melibatkan Internet dan e-mel telah mendedahkan maklumat penting kepada pihak luar. Untuk memastikan maklumat-maklumat penting PTPTN bebas daripada ancaman, semua pengguna adalah disarankan untuk mematuhi Dasar Keselamatan ICT yang telah ditetapkan.

Dasar Keselamatan ICT (DKICT) PTPTN yang dikeluarkan oleh Bahagian Teknologi Maklumat (BTM) PTPTN adalah berdasarkan garis panduan yang dikeluarkan oleh Unit Permodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia (MyMIS) dan *CyberSecurity* Malaysia (sebelum ini dikenali sebagai NISER). Keselamatan ICT adalah meliputi semua data, peralatan, perisian, rangkaian dan kemudahan ICT yang lain selaras dengan Pekeliling Am Bil. 3 Tahun 2000 Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan, Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan dan Pekeliling Perbendaharaan Bil. 5 Tahun 2007 Tatacara Pengurusan Aset Alih Kerajaan yang bertujuan untuk memperkemas dan memantapkan peraturan pengurusan aset alih kerajaan serta arahan keselamatan yang bermaksud untuk mengenal pasti peringkat-peringkat dokumen tidak terdedah kerana ia mengandungi rahsia-rahsia kerajaan yang diamanahkan kepada penjawat awam.

OBJEKTIF

Tujuan utama garis panduan keselamatan ICT PTPTN adalah sebagai panduan **untuk menjamin kesinambungan urusan kerajaan dan menghindar insiden keselamatan**. Keselamatan maklumat adalah untuk melindungi aset ICT PTPTN daripada **disalahgunakan** oleh orang-orang yang tidak bertanggungjawab. Maklumat adalah berharga kerana kebanyakan maklumat tersebut adalah sensitif dan terperingkat. Jika berlaku penyalahgunaan aset berkenaan kepada orang yang tidak bertanggungjawab ia bukan sahaja memudaratkan PTPTN malahan juga kepada keselamatan dan maruah negara. Justeru itu, perlindungan keselamatan yang bijaksana perlu diwujudkan dan disesuaikan bagi menjamin kerahsiaan, kesahihan, keutuhan dan kebolehsediaan (*availability*) maklumat yang berterusan.

BTM adalah **bertanggungjawab** untuk melindungi maklumat terperingkat kerajaan dari dicapai oleh kuasa yang tidak sah, menjamin setiap maklumat adalah tepat dan sempurna, memastikan ketersediaan maklumat apabila diperlukan oleh pengguna dan memastikan capaian diberi hanya kepada pengguna-pengguna yang sah sahaja.

PERNYATAAN DASAR

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

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

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

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

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

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

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

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

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

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

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

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

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

SKOP

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

(a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

(b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT PTPTN 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 PTPTN. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) Perisian

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

(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 PTPTN. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod PTPTN, 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 PTPTN bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

(f) Premis Komputer Dan Komunikasi

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

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

PRINSIP-PRINSIP

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

(a) Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

(b) Hak akses minimum

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

(c) Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:

(i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

(ii) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;

(iii) Menentukan maklumat sedia untuk digunakan;

(iv) Menjaga kerahsiaan kata laluan;

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

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

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

(d) Pengasingan

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

(e) Pengauditan

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

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

(f) Pematuhan

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

(g) Pemulihan

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

(h) Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

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

PTPTN 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 PTPTN 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.

PTPTN 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.

PTPTN 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.

PERKARA 1.0 PEMBANGUNAN DAN PENYELENGGARAAN DASAR	
1.1 Dasar Keselamatan ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan PTPTN dan perundangan yang berkaitan.	
1.1.1 Pelaksanaan Dasar	
Pelaksanaan dasar ini akan dijalankan oleh Ketua Eksekutif PTPTN selaku Pengerusi Jawatankuasa Keselamatan ICT (JKICT) PTPTN. JKICT ini terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), semua Pengurus Kanan Bahagian dan semua Timbalan Pengurus Kanan Bahagian.	Ketua Eksekutif PTPTN
1.1.2 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna PTPTN (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	ICTSO
1.1.3 Penyelenggaraan Dasar	
Dasar Keselamatan ICT PTPTN adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT PTPTN: (a) Kenal pasti dan tentukan perubahan yang diperlukan;	ICTSO

(b) Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT), PTPTN; (c) Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JKICT; dan (d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	
1.1.4 Pengecualian Dasar	
Dasar Keselamatan ICT PTPTN adalah terpakai kepada semua pengguna ICT PTPTN dan tiada pengecualian diberikan.	Pegawai PTPTN

PERKARA 2.0 ORGANISASI KESELAMATAN	
2.1 Infrastruktur Organisasi Dalaman	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT PTPTN.	
2.1.1 Ketua Eksekutif PTPTN	
Ketua Eksekutif PTPTN adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT PTPTN; (b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT PTPTN; (c) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT PTPTN; dan (e) Mempengerusikan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT), PTPTN.	Ketua Eksekutif PTPTN

2.1.2 Ketua Pegawai Maklumat (CIO)	
Ketua Pegawai Maklumat (CIO) bagi PTPTN ialah Ketua Pegawai Operasi, PTPTN. Peranan dan tanggungjawab CIO adalah seperti berikut: (a) Membantu Ketua Eksekutif dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (b) Menentukan keperluan keselamatan ICT; (c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT PTPTN serta pengurusan risiko dan pengauditan; dan (d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT PTPTN.	CIO
2.1.3 Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) bagi PTPTN ialah Pengurus, Seksyen Infrastruktur ICT, PTPTN. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Mengurus keseluruhan program-program keselamatan ICT PTPTN; (b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT PTPTN;	ICTSO

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

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

(e) Menjalankan pengurusan risiko;

(f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan PTPTN berdasarkan hasil penemuan dan menyediakan laporan mengenainya;

(g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;

(h) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT Kerajaan (GCERT), MAMPU dan memaklumkannya kepada CIO;

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

(j) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT;

(k) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur IC supaya insiden baru dapat dielakkan.

2.1.4 Pengurus ICT	
Pengurus ICT bagi PTPTN ialah Timbalan Pengurus Unit Khidmat Rangkaian dan Keselamatan ICT. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: (a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan PTPTN; (b) Menentukan kawalan akses pengguna terhadap aset PTPTN; (c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan (d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT PTPTN.	Timbalan Pengurus Unit Khidmat Rangkaian dan Keselamatan ICT
2.1.5 Pentadbir Sistem ICT	
Pentadbir Sistem ICT bagi PTPTN ialah semua pegawai Bahagian Teknologi Maklumat. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (b) Menentukan ketetapan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang	Bahagian Teknologi Maklumat

telah ditetapkan di dalam Dasar Keselamatan ICT PTPTN; (c) Memantau aktiviti capaian harian sistem aplikasi pengguna; (d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (e) Menganalisis dan menyimpan rekod jejak audit; (f) Menyediakan laporan aktiviti capaian secara berkala; dan (g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	
2.1.6 Pengguna	
Pengguna mempunyai peranan dan tanggungjawab seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT PTPTN; (b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; (d) Malaksanakan prinsip-prinsip Dasar Keselamatan ICT PTPTN dan menjaga kerahsiaan maklumat PTPTN;	Pegawai PTPTN

(e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO degan segera; (f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan (g) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT PTPTN sebagaimana Lampiran I.	
2.1.7 Jawatankuasa Keselamatan ICT PTPTN	
Jawatankuasa Keselamatan ICT (JKICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi ICT PTPTN. Di PTPTN, Mesyuarat Pengurusan PTPTN juga berperanan sebagai JKICT PTPTN. Keanggotaan JKICT PTPTN adalah seperti berikut: Pengerusi : Ketua Eksekutif PTPTN Ahli : (1) CIO PTPTN (2) Semua Pengurus Kanan Bahagian (3) Semua Timbalan Pengurus Kanan Bahagian (4) ICTSO PTPTN	JKICT PTPTN

(5) Pengurus Bahagian (Bahagian Koporat dan Dasar, Bahagian Khidmat Pengurusan dan Bahagian Call Center)

(6) Timbalan Pengurus (Bahagian Undang-Undang, Bahagian Teknologi Maklumat dan Unit Audit Dalam)

Urusetia bagi JKICT PTPTN ialah Timbalan Pengurus Unit Khidmat Rangkaian dan Keselamatan ICT.

Bidang Kuasa:

(a) Memperakukan/meluluskan dokumen DKICT PTPTN;

(b) Memantau tahap pematuhan keselamatan ICT;

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

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

(e) Memastikan DKICT PTPTN selaras dengan dasar-dasar ICT Kerajaan semasa;

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

(g) Membincangkan tindakan yang melibatkan pelanggaran DKICT PTPTN; dan

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

2.1.8 Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (GCERT)

Keanggotaan GCERT adalah seperti berikut:

Pengurus : Timbalan Pengarah, Seksyen Pengurusan Serangan Siber, Bahagian Pematuhan ICT, MAMPU.

Ahli :

(1) Pegawai Teknologi Maklumat Di Seksyen Pengurusan Serang Siber, Bahagian Pematuhan ICT,MAMPU; dan

(2) Penolong Pegawai Teknologi Maklumat di Seksyen Pengurusan Serangan Siber, Bahagian Pematuhan ICT,MAMPU.

Peranan dan tanggungjawab GCERT adalah seperti berikut:

(a) Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden;

(b) Merekod dan menjalankan siasatan awal insiden yang diterima;

(c) Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;

(d) Menasihati PTPTN mengambil tindakan pemulihan dan pengukuhan; (e) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada MAMPU.	
2.2 Pihak Ketiga	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).	
2.2.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT PTPTN; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; (d) Akses kepada aset ICT PTPTN perlu berlandaskan kepada perjanjian kontrak;	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga

(e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai.

i. Dasar Keselamatan ICT PTPTN;

ii. Tapisan Keselamatan

ii . Perakuan Akta Rahsia Rasmi 1972; dan

iv. Hak Harta Intelek.

(f) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT PTPTN sebagaimana **Lampiran 1**.

PERKARA 3.0
PENGURUSAN ASET

3.1 Akauntabiliti Aset

Objektif:

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

3.1.1 Inventori Aset ICT

Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini; (b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di PTPTN; (d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan (e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pegawai PTPTN

3.2 Pengelasan dan Pengendalian Maklumat	
Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
3.2.1 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad.	Pegawai PTPTN
3.2.2 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;	Pegawai PTPTN

(b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;

(c) Menentukan maklumat sedia untuk digunakan;

(d) Menjaga kerahsiaan kata laluan;

(e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

(f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pepprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

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

PERKARA 4.0
KESELAMATAN SUMBER MANUSIA

4.1 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif:

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

4.1.1 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan PTPTN serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan PTPTN serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Pegawai PTPTN

4.1.2 Dalam Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan pegawai dan kakitangan PTPTN serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh PTPTN; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT PTPTN secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan PTPTN serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh PTPTN; dan (d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Khidmat Pengurusan dan Sumber Manusia, PTPTN.	Pegawai PTPTN
4.1.3 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada PTPTN	Pegawai PTPTN

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

PERKARA 5.0
KESELAMATAN FIZIKAL DAN PERSEKITARAN

5.1 Keselamatan Kawasan

Objektif:

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

5.1.1 Kawalan kawasan	
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (c) Memasang alat penggera atau kamera; (d) Menghadkan jalan keluar masuk; (e) Mengadakan kaunter kawalan; (f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat;	Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK), CIO dan ICTSO

(g) Mewujudkan perkhidmatan kawalan keselamatan; (h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; (k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
5.1.2 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Setiap pengguna PTPTN hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan balik kepada PTPTN apabila pengguna berhenti atau bersara;	Pegawai PTPTN

(c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama Kompleks Jabatan Perdana Menteri. Amalan ini juga perlu dipatuhi di kompleks pejabat utama PTPTN Sabah dan Sarawak. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (d) Kehilangan pas mestilah dilaporkan dengan segera.	
5.1.3 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di PTPTN adalah bilik Ketua Pengarah, bilik Timbalan Ketua Pengarah, pejabat Seksyen Pemantauan Siber (PRISMA), bilik server, bilik Operasi GOE-EGDMS dan Pusat Data (*Data Centre*). (a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan (b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah di ringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Pentadbir Sistem

5.2 Keselamatan Peralatan

Objektif:

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

5.2.1 Peralatan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; (d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; (e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini disamping melakukan imbasan ke atas media storan yang digunakan;	Pegawai PTPTN

(g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

(h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;

(i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS);

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

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

(l) Peralatan ICT yang hendak dibawa keluar dari premis PTPTN,perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan;

(m) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;

(n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

(o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

(p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk di baik pulih;

(q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

(r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;

(s) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT;

(t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;

(u) Pengguna hendaklah memastikan semua perkakasan komputer,pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat;

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

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

5.2.2 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; (b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; (c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; (e) Akses dan pergerakan media storan hendaklah direkodkan; (f) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal;	Pegawai PTPTN

(g) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; (h) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan (i) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
5.2.3 Media Tandatangan Digital	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan (c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Pegawai PTPTN
5.2.4 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan PTPTN;	Pegawai PTPTN

(b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; (c) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada *CD-rom*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan (d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	
5.2.5 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; (b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan;	Unit Pentadbir Pangkalan Data dan Khidmat Teknikal

(e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	
5.2.6 Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari premis PTPTN adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Pegawai PTPTN
5.2.7 Pelupusan Perkakasan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh PTPTN dan ditempatkan di PTPTN. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan PTPTN. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Unit Pentadbir Pangkalan Data dan Khidmat Teknikal

(a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran;

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

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

(d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

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

(f) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan

(g) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:

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

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

ii . Memindah keluar dari PTPTN mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab PTPTN; dan v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
5.3 Keselamatan Persekitaran	
Objektif: Melindungi aset ICT PTPTN dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
5.3.1 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: (a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;	Pegawai PTPTN

(b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; (c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; (d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; (e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; (f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; (g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan (h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	
5.3.2 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.	Bahagian Teknologi Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; (b) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan (c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	
5.3.3 Kabel	
Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan	Bahagian Teknologi Maklumat

(d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	
5.3.4 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MAMPU 2004; dan (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras.	Pegawai PTPTN
5.4 Keselamatan Dokumen	
Objektif: Melindungi maklumat PTPTN dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
5.4.1 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;	Pegawai PTPTN

(b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan;

(c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan;

(d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan

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

PERKARA 6.0 PENGURUSAN OPERASI DAN KOMUNIKASI	
6.1 Pengurusan Prosedur Operasi	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
6.1.1 Pengendalian Prosedur	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pegawai PTPTN
6.1.2 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	Pegawai PTPTN

terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
6.1.3 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 di manipulasi; dan (c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari	Bahagian Teknologi Maklumat

perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	

6.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

Objektif:

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

6.2.1 Perkhidmatan Penyampaian

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

6.3 Perancangan dan Penerimaan Sistem

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

6.3.1 Perancangan Kapasiti	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Seksyen Infrastruktur ICT
6.3.2 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Seksyen Pembangunan dan Pengurusan Aplikasi
6.4 Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.	
6.4.1 Perlindungan Dari Perisian Berbahaya	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;	Pegawai PTPTN

(b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;

(c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;

(d) Mengemas kini anti virus dengan *pattern* antivirus yang terkini;

(e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;

(f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;

(g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;

(h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan

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

6.4.2 Perlindungan dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	
6.5 *Housekeeping*	
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
6.5.1 *Backup*	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; (c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan;	Unit Pentadbir Pangkalan Data dan Khidmat Teknikal

(c) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; (d) Tempoh penyimpanan data *backup* adalah terbahagi kepada tiga peringkat iaitu secara mingguan, bulanan dan tahunan; dan (e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	
6.6 Pengurusan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
6.6.1 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;	Unit Khidmat Rangkaian dan Keselamatan ICT

(d) Semua peralatan mestilah melalui proses *User Acceptance Test* (UAT) semasa pemasangan dan konfigurasi;

(e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh ICTSO;

(f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan PTPTN;

(g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;

(h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat PTPTN;

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

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

(k) Semua pengguna hanya dibenarkan menggunakan rangkaian PTPTN sahaja dan penggunaan modem adalah dilarang sama sekali; dan

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

6.7 Pengurusan Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
6.7.1 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Pegawai PTPTN
6.7.2 Prosedur Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Menyimpan semua media di tempat yang selamat; dan	Pegawai PTPTN

(f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	
6.7.3 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan (c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Pegawai PTPTN
6.8 Pengurusan Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara PTPTN dan agensi luar terjamin.	
6.8.1 Pertukaran Malumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;	Pegawai PTPTN

(b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara PTPTN dengan agensi luar; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari PTPTN; dan (f) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	
6.8.2 Pengurusan Mel Elektronik (E-mel)	
Penggunaan e-mel di PTPTN hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*" dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: (a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh PTPTN sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh PTPTN;	Pegawai PTPTN

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

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

(e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi dua megabait (2Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

(f) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;

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

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

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

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

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

(l) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamys.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan (m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing.	
6.9 Perkhidmatan E-Dagang (*Electronic Commerce Services*)	
Objektif: Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
6.9.1 E-dagang	
Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; (b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan	Pegawai PTPTN

(c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	
6.9.2 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: (a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; (b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan (c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Pegawai PTPTN
6.10 Pemantauan	
Objektif: Memastikan aktiviti penggunaan dan pemprosesan maklumat mengikut prosedur yang telah ditetapkan.	
6.10.1 Pengauditan dan Forensik ICT	
ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT PTPTN;	ICTSO, Unit Khidmat Rangkaian dan

(b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; (g) Aktiviti penyalahgunaan akaun e-mel; dan (h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	Keselamatan ICT
6.10.2 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.	Bahagian Teknologi Maklumat

Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi; (b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan (g) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
6.10.3 Sistem Log	
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;	Bahagian Teknologi Maklumat

(b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pegawai BTM hendaklah melaporkan kepada ICTSO dan CIO.	
6.10.4 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; (b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; (c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; (d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; (e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan	Bahagian Teknologi Maklumat

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

PERKARA 7.0
KAWALAN CAPAIAN

7.1 Dasar Kawalan Capaian

Objektif:

Mengawal capaian ke atas maklumat.

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

7.2 Pengurusan Capaian Pengguna

Objektif:

Mengawal capaian pengguna ke atas aset ICT PTPTN

7.2.1 Akaun Pengguna	
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan oleh PTPTN sahaja boleh digunakan; (b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (c) Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; (d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan PTPTN. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan	Pegawai PTPTN

(f) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Bertukar bidang tugas kerja (jika perlu); ii. Bertukar ke agensi lain; iii. Bersara; atau iv. Ditamatkan perkhidmatan.	
7.2.2 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pegawai PTPTN
7.2.3 Pengurusan Kata Laluan	
Pemilihan, pengunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh PTPTN seperti berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara, angka dan aksara khusus;	Pegawai PTPTN

(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; dan

(k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.

7.2.4 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	Pegawai PTPTN

7.3 Kawalan Capaian Rangkaian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaraan ke atas perkhidmatan rangkaian.	
7.3.1 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:	ICTSO, Unit Khidmat

(a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian PTPTN, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian IC.	Rangkaian dan Keselamatan ICT
7.3.2 Capaian Internet	
Teknologi Internet telah memudahkan perhubungan antara pengguna dan menyediakan capaian kepada maklumat dalam pelbagai bentuk/format dalam urusan penyelidikan, analisis, rujukan dan bahan-bahan lain yang berfaedah. Penggunaan Internet dengan cara yang tidak bertanggungjawab adalah dianggap sebagai tatacara yang boleh mengancam keselamatan, keutuhan dan kerahsiaan maklumat, melemahkan dan mengganggu sistem dan rangkaian ICT PTPTN. Demi untuk menjamin keselamatan ICT PTPTN pihak pengurusan telah menghadkan penggunaan Internet kepada Gred 48 dan ke atas sahaja. Namun begitu, bagi mana-mana pegawai yang memerlukan kemudahan Internet ini perlu untuk mendapatkan kelulusan daripada Ketua Bahagian dan Ketua Eksekutif. Bagaimanapun, capaian internet bagi semua warga PTPTN dibuka pada jam 12.00 tengah hari hingga 2.00 petang (waktu rehat) bagi memberi kemudahan kepada pengguna melakukan transaksi secara dalam talian dan lain-lain urusan selagi tidak melanggar garis panduan yang telah ditetapkan.	Pegawai PTPTN

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Penggunaan Internet di PTPTN 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 PTPTN;

(b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;

(c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan;

(d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;

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

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

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

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

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

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

(k) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan

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

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

ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	
7.4 Kawalan Capaian Sistem Pengoperasian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasi.	
7.4.1 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: (a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan (b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah PTPTN menyokong perkara-perkara berikut: (a) Mengesahkan pengguna yang dibenarkan; (b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* dan	Bahagian Teknologi Maklumat

(c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Menghadkan dan mengawal penggunaan program; dan (d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
7.5 Kawalan Capaian Aplikasi Dan Maklumat	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.	
7.5.1 Capaian Aplikasi Dan Maklumat	
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.	Pegawai PTPTN

Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi:

(a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;

(b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);

(c) Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;

(d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan

(e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.

7.6 Peralatan Mudah Alih Dan Kerja Jarak Jauh

Objektif:

Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.

7.6.1 Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Pegawai PTPTN
7.6.2 Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Pegawai PTPTN

PERKARA 8.0
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

8.1 Keselamatan Dalam Membangunkan Sistem Aplikasi

Objektif:

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

8.1.1 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (b) Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; (c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan	Bahagian Teknologi Maklumat

(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.	
8.1.2 Pengesahan Data Input Dan Output	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan (b) Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pegawai PTPTN
8.2 Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integrasi dan kesahihan maklumat melalui kawalan kriptrografi.	
8.2.1 Enkripsi	
Pengguna hendaklah membuat enkripsi (encryption) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Pegawai PTPTN
8.2.2 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Pegawai PTPTN

8.2.3 Pengurusan Infrastruktur Kunci Awam (PKI)	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pegawai PTPTN
8.3 Keselamatan Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikehendalikan dengan baik dan selamat.	
8.3.1 Kawalan Fail Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; (b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; (c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan	Bahagian Teknologi Maklumat

(e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	
8.4 Keselamatan Dalam Proses Pembangunan Dan Sokongan	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi	
8.4.1 Prosedur Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (d) Akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan	Bahagian Teknologi Maklumat

(e) Menghalang sebarang peluang untuk membocorkan maklumat.	
8.4.2 Pembangunan Perisian Secara Outsource	
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik PTPTN.	Seksyen Pembangunan dan Pengurusan Aplikasi
8.5 Kawalan Teknikal Keterdedahan (*Vulnerability*)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesananya.	
8.5.1 Kawalan Dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Seksyen Infrastruktur ICT

PERKARA 9.0
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

9.1 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:

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

9.1.1 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan Bahagian Teknologi Maklumat dengan kadar segera: (a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan	Pegawai PTPTN

(e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di PTPTN sepertimana **Lampiran 2**. Prosedur pelaporan insiden keselamatan ICT berdasarkan: (a) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan (b) Surat Pekeliling Am Bilangan 4 Tahun 2000 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
9.2 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
9.2.1 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada PTPTN.	ICTSO

Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:

(a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;

(b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;

(c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;

(d) Menyediakan tindakan pemulihan segera; dan

(e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

PERKARA 10.0
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

10.1 Dasar Kesinambungan Perkhidmatan

Objektif:

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

10.1.1 Pelan Kesinambungan Perkhidmatan	
Pelan Kesinambungan Perkhidmatan (*Business Continuity Management - BCM*) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh Pengurusan PTPTN. Perkara-perkara berikut perlu diberi perhatian: (a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; (c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;	Bahagian Korporat dan Dasar

(d) Mendokumentasikan proses dan prosedur yang telah dipersetujui;

(e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;

(f) Membuat *backup*; dan

(g) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.

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

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

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

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

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

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

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

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

PTPTN hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

PERKARA 11.0 PEMATUHAN	
11.1 Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada dasar keselamatan ICT PTPTN.	
11.1.1 Pematuhan Dasar	
Setiap pengguna di PTPTN hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT PTPTN dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di PTPTN termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT PTPTN selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber PTPTN.	Semua

11.1.2 Pematuhan Dengan Dasar, Piawaian Dan Keperluan Teknikal	
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO, Unit Khidmat Rangkaian dan Keselamatan ICT
11.1.3 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua
11.1.4 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di PTPTN adalah seperti di Lampiran 3.	Semua
11.1.5 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT PTPTN boleh dikenakan tindakan tatatertib.	Semua

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Jalur Lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of services	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan.

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

Instrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian kawasan setempat yang menghubungkan komputer.
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi kompter.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
Modem	*MOdulator DEModulator* Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi

	yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastruction	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Tthreat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptable power supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT PTPTN

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 PTPTN; dan

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

Tandatangan : .....

Tarikh : .....

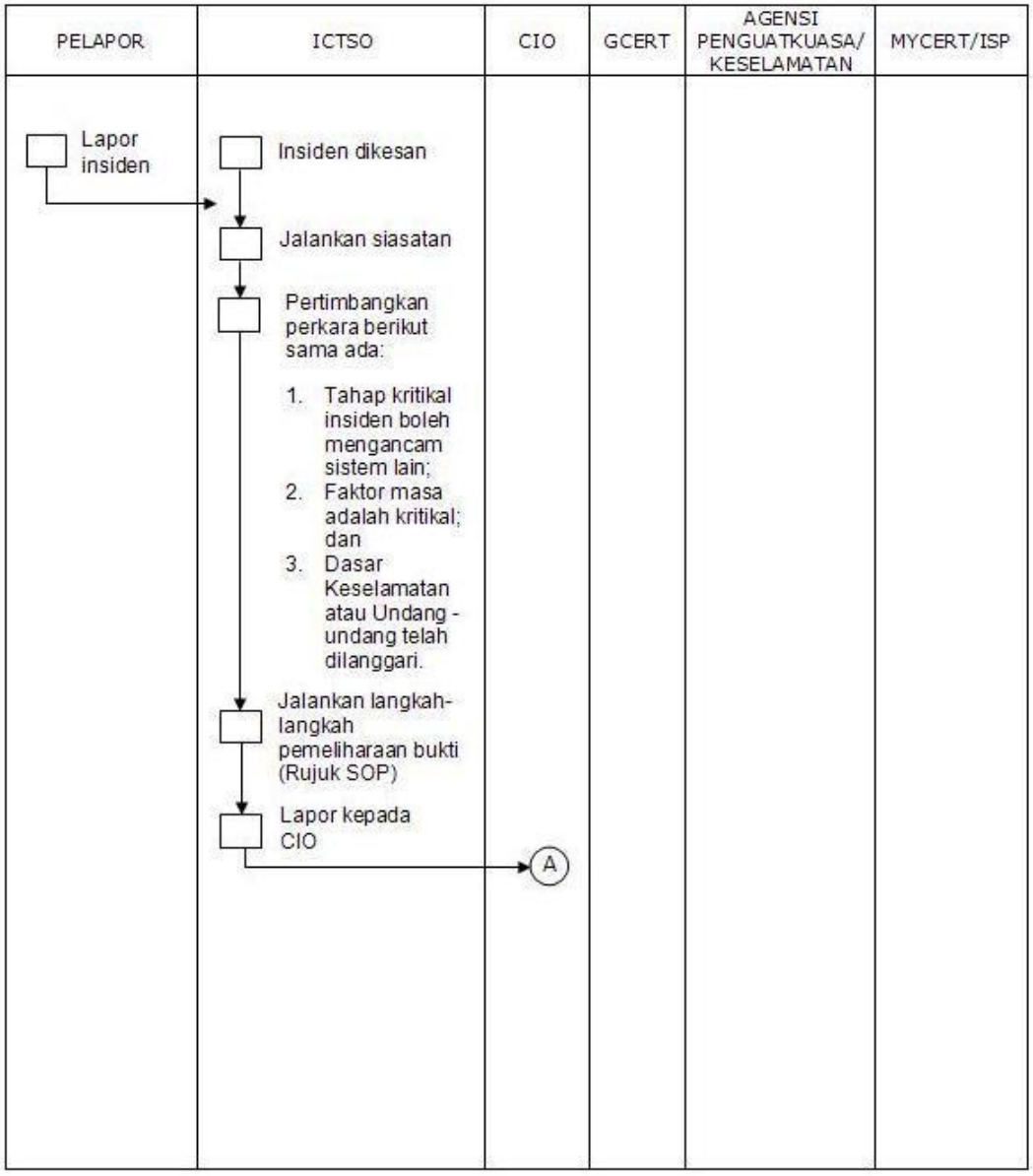
Pengesahan Pegawai Keselamatan ICT

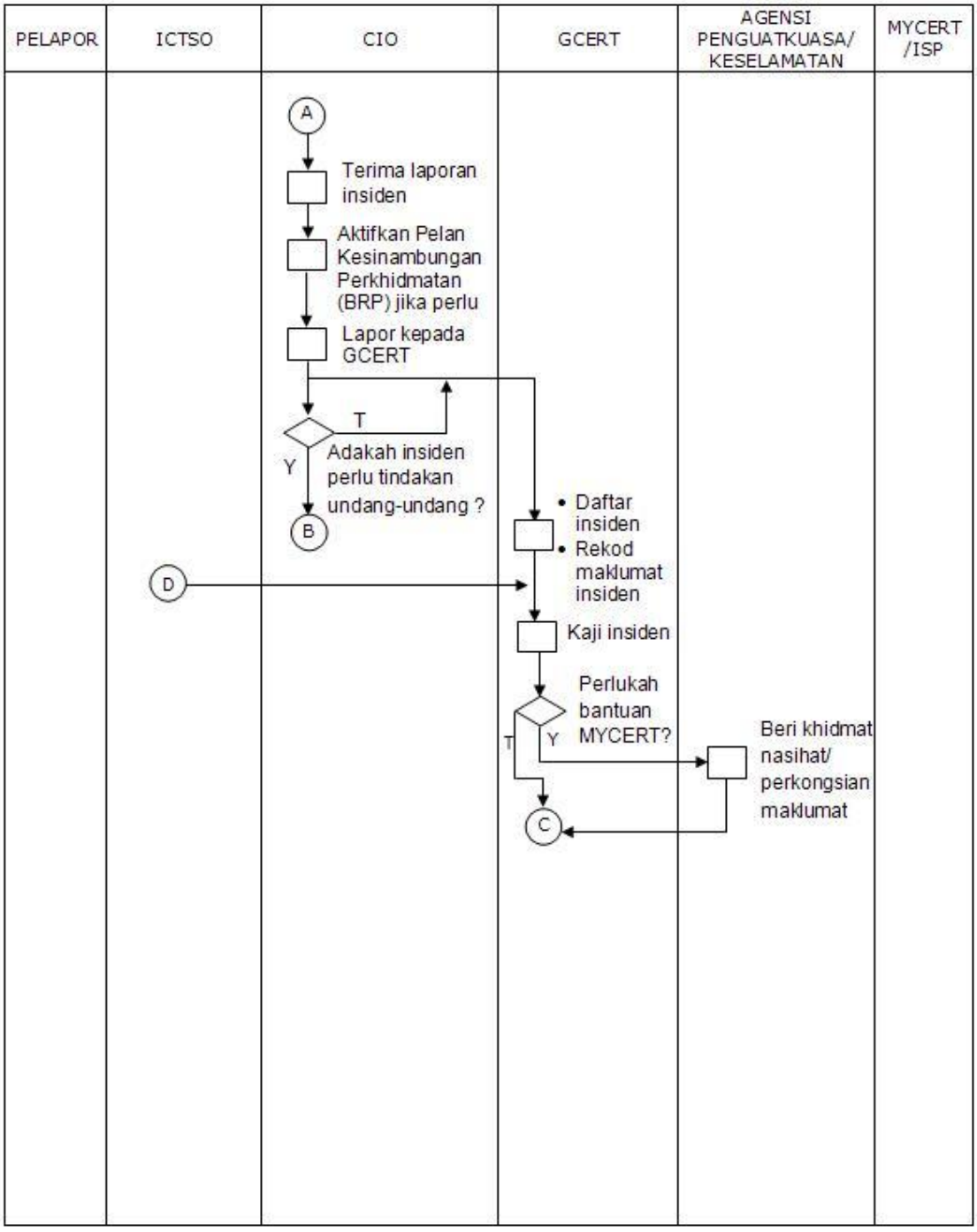
.....
(Nama Pegawai Keselamatan ICT)
b.p. Ketua Eksekutif PTPTN

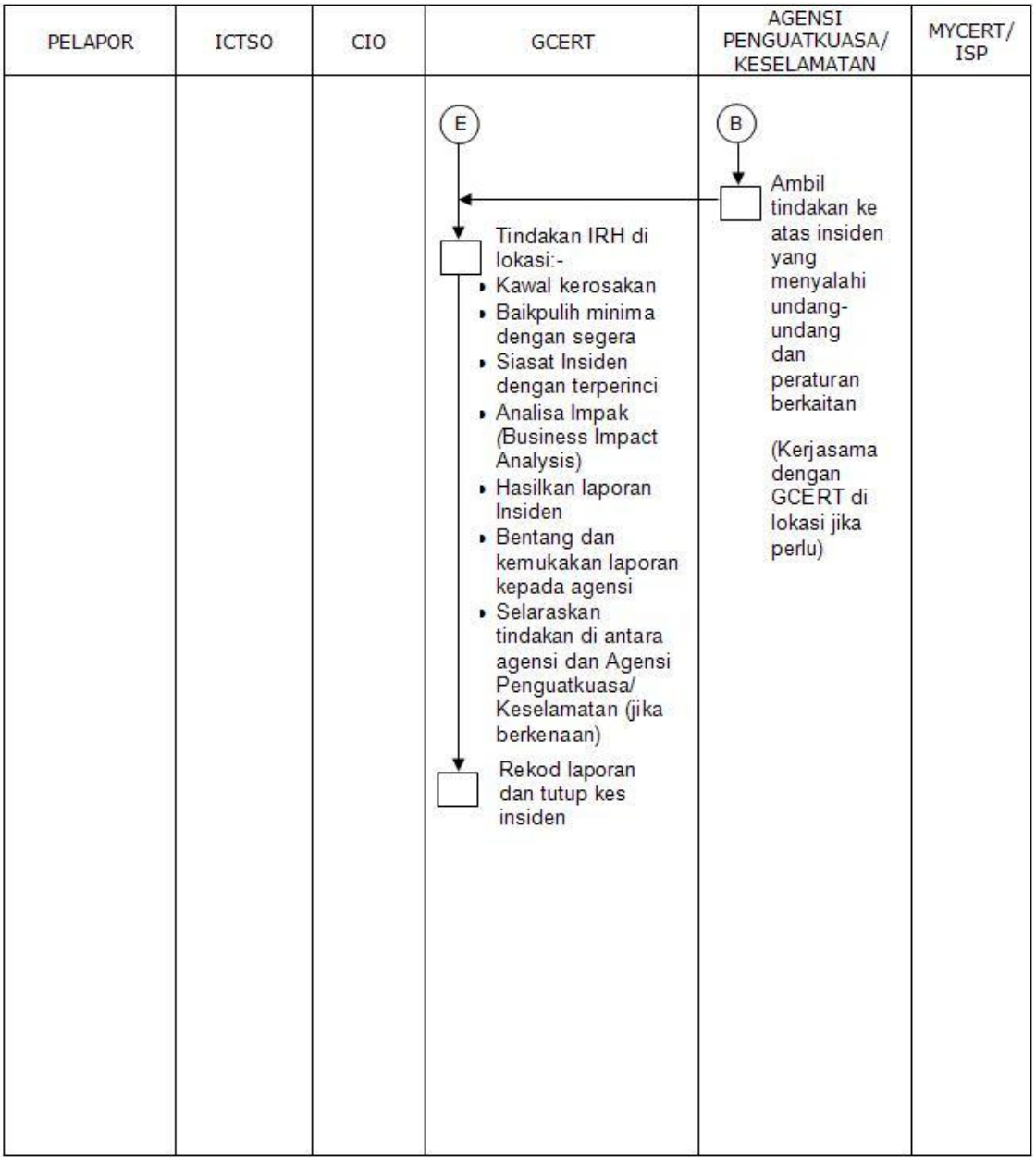
Tarikh: .....

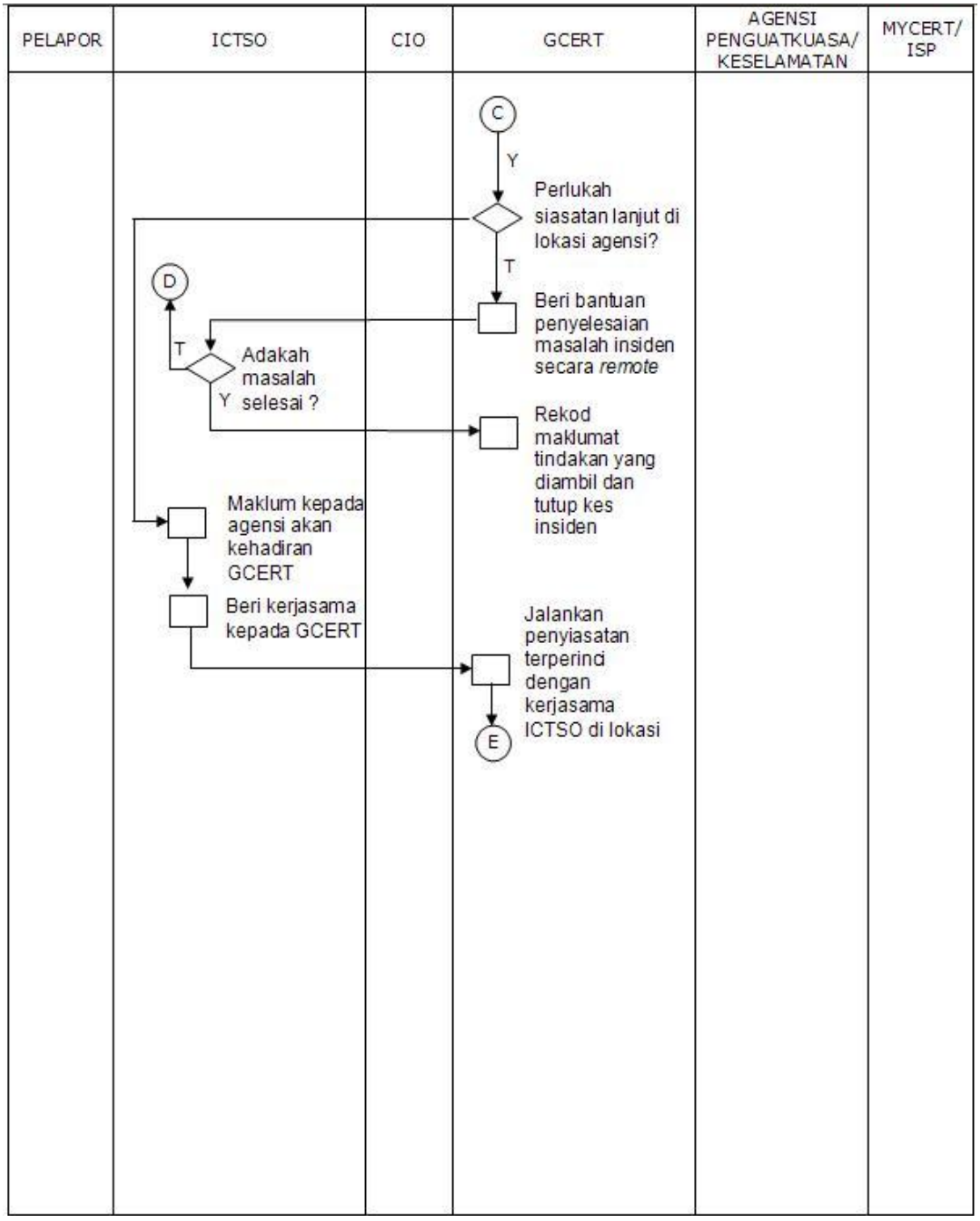
Lampiran 2

Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT PTPTN









Petunjuk:

SOP – *Standard Operating Procedure*;

Lampiran 3

SENARAI PERUNDANGAN DAN PERATURAN

(a) Arahan Keselamatan;

(b) Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

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

(d) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

(e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;

(f) Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

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

(h) Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;

(i) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

(j) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

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

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

(m) Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;

(n) Akta Tandatangan Digital 1997;

(o) Akta Rahsia Rasmi 1972;

(p) Akta Jenayah Komputer 1997;

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

(r) Akta Komunikasi dan Multimedia 1998;

(s) Perintah-Perintah Am;

(t) Arahan Perbendaharaan;

(u) Arahan Teknologi Maklumat 2007;

(v) Garis Panduan Keselamatan MAMPU 2004;

(w) *Standard Operating Procedure* (SOP) ICT MAMPU;

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

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