KERAJAAN MALAYSIA

POLISI ICT PERBENDAHARAAN

VERSI 5.0

PERBENDAHARAAN MALAYSIA

KEMENTERIAN KEWANGAN

REKOD PINDAAN DOKUMEN

TARIKH	NO. KELUARAN/PINDAAN	BAB/ MUKASURAT	KETERANGAN PINDAAN
25/01/2013	Ver 5.0	Rujuk Jadual Pindaan Polisi ICT Perbendaharaan	

ISI KANDUNGAN

PENGENALAN 1
OBJEKTIF 1
PENYATAAN POLISI 1
SKOP 2
PRINSIP-PRINSIP 4
PENILAIAN RISIKO KESELAMATAN ICT 6

Perkara 1 - PEMBANGUNAN DAN PENYELENGGARAAN POLISI
1.1 Polisi ICT 8
1.1.1 Pelaksanaan Polisi 8
1.1.2 Penyebaran Polisi 8
1.1.3 Penyelenggaraan Polisi 8
1.1.4 Pengecualian 8

Perkara 2 - ORGANISASI ICT
2.1 Infrastruktur Organisasi Dalaman 9
2.1.1 Ketua Setiausaha Perbendaharaan 9
2.1.2 Ketua Pegawai Maklumat (CIO) 9
2.1.3 Pengurus ICT 9
2.1.4 Pegawai Keselamatan ICT (ICTSO) 10
2.1.5 Jawatankuasa Pemandu ICT Kementerian Kewangan (JPICT MOF) 11
2.1.6 Pasukan Tindakbalas Insiden Keselamatan ICT Kementerian Kewangan (CERTMOF) 13
2.1.7 Pengurus Pusat Data dan Pusat Pemulihan Bencana (DRC) 13
2.1.8 Pentadbir Sistem ICT 14
2.1.9 Pentadbir Rangkaian 15
2.1.10 Pentadbir Pangkalan Data 16
2.1.11 Pentadbir Sistem Aplikasi 16
2.1.12 Koordinator ICT Bahagian 17
2.1.13 Koordinator Web Bahagian 18
2.1.14 Pengguna 19
2.2 Pihak Ketiga 19
2.2.1 Pembekal, Pakar Runding, Pelawat dan Pihak-Pihak Luar Lain 20

Perkara 3 - PENGURUSAN ASET
3.1 Perolehan Aset ICT 21
3.1.1 Perolehan Perkakasan dan Perisian ICT 21
3.2 Peruntukan / Perkongsian Perkakasan dan Perisian ICT 21
3.2.1 PC, Komputer Riba, Projektor LCD dan Peralatan Mudah Alih 21
3.2.2 Pencetak 21
3.3 Akauntabiliti Aset 22
3.3.1 Inventori Aset 22

3.4 Pengelasan dan Pengendalian Maklumat 22
3.4.1 Pengelasan Maklumat 22
3.4.2 Pengendalian Maklumat 23

Perkara 4 - KESELAMATAN SUMBER MANUSIA
4.1 Keselamatan Sumber Manusia Dalam Tugas Harian 24
4.1.1 Sebelum Memulakan Perkhidmatan 24
4.1.2 Semasa Perkhidmatan 24
4.1.3 Bertukar Atau Tamat Perkhidmatan 25
4.2 Pendidikan 25
4.2.1 Program Kesedaran Keselamatan ICT 25

Perkara 5 - KESELAMATAN FIZIKAL DAN PERSEKITARAN
5.1 Keselamatan Kawasan 27
5.1.1 Kawasan Larangan 27
5.2 Keselamatan Peralatan 27
5.2.1 Peralatan ICT 27
5.2.2 Media Storan 28
5.2.3 Media Tandatangan Digital 29
5.2.4 Media Perisian dan Aplikasi 29
5.2.5 Penyelenggaraan Perkakasan 30
5.2.6 Peralatan di Luar Premis 31
5.2.7 Pelupusan Perkakasan 31
5.3 Keselamatan Persekitaran 32
5.3.1 Kawalan Persekitaran 32
5.3.2 Bekalan Kuasa 33
5.3.3 Kabel 34
5.3.4 Prosedur Kecemasan 34
5.4 Keselamatan Dokumen 34
5.4.1 Dokumen 34

Perkara 6 - PENGURUSAN OPERASI DAN KOMUNIKASI
6.1 Pengurusan Prosedur Operasi 36
6.1.1 Pengendalian Prosedur 36
6.1.2 Kawalan Perubahan 36
6.2 Perancangan dan Penerimaan Sistem 37
6.2.1 Perancangan Kapasiti 37
6.2.2 Penerimaan Sistem Aplikasi 37
6.2.3 Penerimaan Perkakasan dan Perisian Sistem Baru 38
6.3 Perisian Berbahaya 38
6.3.1 Perlindungan dari Perisian Berbahaya 38
6.3.2 Perlindungan dari *Mobile Code* 39
6.4 *Housekeeping* 39
6.4.1 Penduaan 39
6.5 Pengurusan Rangkaian 40
6.5.1 Kawalan Infrastruktur Rangkaian 40
6.6 Pengurusan Media 41
6.6.1 Penghantaran dan Pemindahan 41

	6.6.2	Prosedur Pengendalian Media	41
	6.6.3	Keselamatan Sistem Dokumentasi	42
6.7	Pengurusan Pertukaran Maklumat		42
	6.7.1	Pengurusan Mel Elektronik (E-mel)	42
6.8	Pemantauan		45
	6.8.1	Pengauditan dan Forensik ICT	45
	6.8.2	Jejak Audit	45
	6.8.3	Sistem Log	46
	6.8.4	Pemantauan Log	47
Perkara 7 -	**KAWALAN CAPAIAN**		
7.1	Kawalan Capaian		48
	7.1.1	Keperluan Kawalan Capaian	48
7.2	Pengurusan Capaian Pengguna		48
	7.2.1	ID Pengguna	48
	7.2.2	Hak Capaian	49
	7.2.3	Pengurusan Kata Laluan	49
	7.2.4	*Clear Desk* dan *Clear Screen*	50
7.3	Penggunaan dan Pengurusan Rangkaian		50
	7.3.1	Infrastruktur Rangkaian	50
	7.3.2	Sambungan Rangkaian	51
	7.3.3	Pengurusan Alamat IP	51
	7.3.4	Talian Internet Persendirian	52
	7.3.5	Antivirus	52
7.4	Keselamatan Internet		53
	7.4.1	Internet	53
	7.4.2	Melayari Internet	54
7.5	Kawalan Capaian Sistem Pengoperasian		55
	7.5.1	Capaian Sistem Pengoperasian	55
	7.5.2	Kad Pintar/*Soft Cert*	56
7.6	Kawalan Capaian Sistem dan Aplikasi		57
	7.6.1	Sistem Maklumat dan Aplikasi	57
7.7	Peralatan Mudah Alih dan Kerja Jarak Jauh		58
	7.7.1	Penggunaan Peralatan Mudah Alih	58
	7.7.2	Kerja Jarak Jauh	58
Perkara 8 -	**PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM**		
8.1	Keselamatan Dalam Membangunkan Sistem dan Aplikasi		59
	8.1.1	Keselamatan Aplikasi	59
8.2	Kawalan Kriptografi		60
	8.2.1	Penyulitan	60
	8.2.2	Tandatangan Digital	60
	8.2.3	Pengurusan Infrastruktur Kunci Awam (*PKI*)	60
8.3	Pembangunan Perisian		60
	8.3.1	Pembangunan Sistem Aplikasi	60
	8.3.2	Permohonan Perubahan / Keperluan Tambahan Sistem Aplikasi Sedia Ada	62

8.4 Fail Sistem 62
8.4.1 Kawalan Fail Sistem 62
8.5 Pembangunan dan Proses Sokongan 63
8.5.1 Kawalan Perubahan 63
8.6 Pembayaran *Online* 63
8.6.1 Pembayaran *Online* bagi Sistem 63
8.7 Penamatan Sistem Aplikasi 64
8.7.1 Penamatan Penggunaan Sistem Aplikasi 64
8.8 Portal dan Aplikasi Web 64
8.8.1 Portal dan Aplikasi Web 65

Perkara 9 - PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT
9.1 Menangani Insiden Keselamatan ICT 66
9.1.1 Mekanisme Pelaporan Insiden Keselamatan ICT 66
9.2 Pengurusan Maklumat Insiden Keselamatan ICT 67
9.2.1 Prosedur Pengurusan Insiden 67

Perkara 10 - PENGURUSAN KESINAMBUNGAN PERKHIDMATAN
10.1 Kesinambungan Perkhidmatan 68
10.1.1 Pelan Kesinambungan Perkhidmatan 68

Perkara 11 - PEMATUHAN
11.1 Pematuhan dan Keperluan Perundangan 70
11.1.1 Pematuhan Polisi 70
11.1.2 Keperluan Perundangan 70
11.1.3 Pelanggaran Polisi 70

LAMPIRAN 1 71
LAMPIRAN 2 72
LAMPIRAN 3 76
LAMPIRAN 4 77
LAMPIRAN 5 78

GLOSARI 80

PENGENALAN

Polisi ICT Perbendaharaan mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) Perbendaharaan. Polisi ini juga menerangkan kepada semua pengguna di Perbendaharaan mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT Perbendaharaan.

OBJEKTIF

Polisi ICT Perbendaharaan diwujudkan untuk menjamin kerahsiaan, integriti dan kebolehsediaan urusan maklumat Perbendaharaan melalui kemudahan ICT dengan meminimumkan kesan insiden keselamatan ICT.

PENYATAAN POLISI

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 daripada sumber yang sah.

Polisi ICT Perbendaharaan 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 Perbendaharaan terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Polisi ICT Perbendaharaan 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, Polisi ICT Perbendaharaan 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 Perbendaharaan. 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 Perbendaharaan;

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 Perbendaharaan. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod Perbendaharaan, 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 Perbendaharaan 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 Polisi ICT Perbendaharaan 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 kepada pengguna hanya diberi pada tahap akses yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas adalah diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu data atau 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 Perbendaharaan. Tanggungjawab ini perlu dinyatakan dengan jelas, sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

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

iii. Menentukan maklumat sedia untuk digunakan;

iv. Menjaga kerahsiaan kata laluan;

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

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

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

Semua pengguna adalah bertanggungjawab terhadap semua tindakannya ke atas aset ICT Perbendaharaan;

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 keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan atau jejak audit. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*. Rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta merta;

f. Pematuhan

Polisi ICT Perbendaharaan hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan aset ICT Perbendaharaan;

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

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

Perbendaharaan 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 Perbendaharaan 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.

Perbendaharaan 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.

Perbendaharaan 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 kepada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

Perkara 1 Pembangunan dan Penyelenggaraan Polisi

1.1 Polisi ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan aset ICT selaras dengan keperluan Perbendaharaan dan perundangan yang berkaitan.	
1.1.1 Pelaksanaan Polisi	
Pelaksanaan Polisi ini akan dijalankan oleh KSP dibantu oleh Pasukan Pengurusan ICT yang terdiri daripada CIO, ICTSO dan semua Setiausaha Bahagian.	KSP
1.1.2 Penyebaran Polisi	
Polisi ini perlu disebarkan kepada semua Pengguna Perbendaharaan.	Pengurus ICT
1.1.3 Penyelenggaraan Polisi	
Polisi adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan arahan serta keperluan semasa. Berikut adalah prosedur berhubung dengan penyelenggaraan Polisi ini: a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Kemuka cadangan pindaan untuk persetujuan Mesyuarat Jawatankuasa Pemandu ICT Kementerian Kewangan (JPICT MOF); c. Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JPICT; dan d. Polisi ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	Pengurus ICT
1.1.4 Pengecualian	
Polisi adalah terpakai kepada semua Pengguna dan tiada pengecualian diberikan.	Semua

Perkara 2 Organisasi ICT

2.1 Infrastruktur Organisasi Dalaman

Objektif:
Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi ICT Perbendaharaan.

2.1.1 Ketua Setiausaha Perbendaharaan

Peranan dan tanggungjawab KSP adalah seperti berikut: a. memastikan semua Pengguna memahami peruntukan-peruntukan di bawah Polisi; b. memastikan semua Pengguna mematuhi Polisi; c. memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan d. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Polisi ICT Perbendaharaan.	KSP

2.1.2 Ketua Pegawai Maklumat (CIO)

CIO bertanggungjawab ke atas perancangan, pengurusan, penyelarasan dan pemantauan program ICT di Perbendaharaan.	CIO

2.1.3 Pengurus ICT

Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. merangka, merumus dan menguatkuasakan Polisi ICT Perbendaharaan; b. menentukan semua pengguna mendapat pendedahan, bantuan dan mematuhi Polisi ICT Perbendaharaan; c. menetapkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan;	Pengurus ICT

d. menentukan kawalan akses semua Pengguna terhadap aset ICT Perbendaharaan; e. memastikan kawalan capaian ke atas aset ICT termasuk maklumat, perkhidmatan rangkaian dan kemudahan-kemudahan yang berkaitan diwujudkan dan dilaksanakan dengan berkesan berasaskan keperluan urusan dan keselamatan; f. mengkaji semula dan memperhalus pengurusan kerahsiaan maklumat dan kawalan capaian secara berkala; g. memastikan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Perbendaharaan disimpan; dan h. merangka, membangun dan merumus *Disaster Recovery Plan* (DRP) Perbendaharaan yang menyeluruh untuk menjamin perkhidmatan tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
2.1.4 Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Mengurus keseluruhan program-program keselamatan ICT Perbendaharaan; b. Menguatkuasakan perihal keselamatan ICT Perbendaharaan; c. Memberi penerangan dan pendedahan berkenaan keselamatan ICT kepada semua pengguna; d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan keselamatan ICT di Perbendaharaan; e. Menjalankan pengurusan risiko; f. Menjalankan audit keselamatan, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan	ICTSO

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 Sektor Awam (GCERT) 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. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Polisi ICT Perbendaharaan; k. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan l. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
2.1.5 Jawatankuasa Pemandu ICT Kementerian Kewangan (JPICT MOF)	
Agensi yang perlu mendapat kelulusan projek ICT di JPICT MOF adalah seperti berikut: a. Perbendaharaan Malaysia; b. Jabatan Kastam Diraja Malaysia (JKDM); c. Jabatan Akauntan Negara Malaysia (JANM); d. Lembaga Hasil Dalam Negeri Malaysia (LHDNM); e. Jabatan Penilaian dan Perkhidmatan Harta (JPPH); f. Lembaga Pembangunan Langkawi (LADA); g. Labuan Financial Services Authority (LFSA); dan h. Perbadanan Kemajuan Ekonomi Negeri (PKEN). Peranan dan tanggungjawab JPICT MOF adalah seperti berikut: a. Menetapkan arah tuju dan strategi untuk pelaksanaan ICT	JPICT MOF

Kementerian Kewangan;

b. Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/strategi ICT kementerian/agensi;

c. Merancang dan menyelaras pelaksanaan program/projek-projek ICT Kementerian Kewangan dan agensi-agensi di bawahnya supaya selaras dengan Pelan Strategik ICT Kementerian Kewangan;

d. Menyelaras dan menyeragamkan pelaksanaan ICT antara Kementerian Kewangan dan agensi-agensi di bawahnya dengan Pelan Strategik ICT Sektor Awam;

e. Mempromosi dan menggalakkan perkongsian pintar projek ICT antara kementerian dan agensi-agensi di Kementerian Kewangan;

f. Merancang dan menentukan langkah-langkah keselamatan ICT;

g. Mengikuti dan memantau perkembangan program ICT Kementerian Kewangan, serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT;

h. Menilai dan meluluskan semua perolehan ICT Kementerian Kewangan dan agensi-agensi di bawahnya berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan;

i. Menyelaras dan mengemukakan kertas cadangan perolehan ICT bagi kementerian dan agensi-agensi di bawahnya kepada Urus Setia JTICT untuk kelulusan teknikal;

j. Mengemukakan laporan projek ICT yang diluluskan di peringkat JPICT dan dibuat perolehan kepada Urus Setia JTICT; dan

k. Mengemukakan laporan kemajuan projek ICT Kementerian Kewangan dan agensi-agensi di bawahnya yang telah diluluskan oleh JTICT kepada Urus Setia JTICT mengikut tempoh-tempoh yang telah ditetapkan.

Sila rujuk **Lampiran 3** untuk Carta Organisasi JPICT MOF.

2.1.6 Pasukan Tindakbalas Insiden Keselamatan ICT Kementerian Kewangan (CERTMOF)

Keanggotaan CERTMOF adalah seperti berikut: Pengarah: Setiausaha Bahagian Pengurusan Teknologi Maklumat (SBTM) Pengurus: Timbalan Setiausaha Bahagian Pengurusan Teknologi Maklumat, Seksyen Infrastruktur, Keselamatan dan Logistik (TSBTM(O)) Ahli: Pegawai Teknologi Maklumat/ Penolong Pegawai Teknologi Maklumat yang dilantik dari Bahagian/ Agensi di bawah MOF Bahagian/ Agensi yang menjadi ahli dalam CERTMOF adalah: a. Bahagian Pengurusan Teknologi Maklumat (BPTM); b. Bahagian Pinjaman Perumahan (BPP); c. Unit e-Perolehan (eP); d. Jabatan Penilaian & Perkhidmatan Harta (JPPH); e. Jabatan Akauntan Negara Malaysia (JANM); f. Jabatan Kastam DiRaja Malaysia (JKDM); dan g. Lembaga Hasil Dalam Negeri Malaysia (LHDNM). Peranan dan tanggungjawab CERTMOF adalah seperti berikut: a. Mengesan atau menerima aduan keselamatan ICT serta menilai tahap dan jenis insiden; b. Merekod dan menjalankan siasatan awal insiden yang diterima; c. Mengambil tindakan pemulihan dan pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; dan d. Menjalankan ujian penilaian dari semasa ke semasa untuk memastikan tahap keselamatan ICT terjamin.	CERTMOF

2.1.7 Pengurus Pusat Data dan Pusat Pemulihan Bencana (*Disaster Recovery Centre* – DRC)

Peranan dan tanggungjawab Pengurus Pusat Data/DRC adalah seperti berikut:	Pengurus Pusat Data/DRC

a. Mengurus dan mentadbir Pusat Data/DRC Perbendaharaan termasuk persekitaran dan keselamatan fizikal peralatan ICT; b. Memantau keadaan fizikal peralatan ICT di Pusat Data/DRC; c. Mengendalikan urusan perolehan peralatan di Pusat Data/DRC termasuk penyediaan kertas kerja berkaitan; d. Mengendalikan penerimaan serta penempatan peralatan ICT di Pusat Data/DRC; e. Mengendalikan penyediaan peralatan ICT bagi kegunaan pengguna; f. Menyelia dan mengendalikan proses penyelenggaraan terhadap peralatan ICT di Pusat Data/DRC; g. Memastikan peralatan di Pusat Data/DRC sentiasa berfungsi dan boleh dicapai oleh pengguna serta menyelesaikan masalah-masalah yang timbul; h. Mengurus dan menyelenggara pengoperasian backup secara berpusat; i. Mengendalikan pengujian *restore* dan *recovery* secara berkala; dan j. Mengurus dan mengendalikan pelupusan peralatan ICT di Pusat Data/DRC.	
2.1.8 Pentadbir Sistem ICT	
Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a. Memantau ketersediaan dan prestasi server; b. Menyimpan dan menganalisa rekod jejak audit; c. Mengambil tindakan pengukuhan bagi meningkatkan tahap keselamatan server seperti yang dimaklumkan oleh	Pentadbir Sistem ICT

CERTMOF; d. Melaksanakan pengemaskinian *patches* Sistem Pengoperasian (*OS*); e. Melaksanakan penyelenggaraan pencegahan *(preventive maintenance)* mengikut jadual yang ditetapkan; f. Melaksanakan amalan terbaik dalam menjaga keselamatan maklumat terperingkat di bawah kawalan masing-masing daripada pencerobohan dalaman atau luaran, seperti sentiasa melakukan penduaan *(backup)* ke atas data-data penting mengikut jadual yang ditetapkan; dan g. Mengendalikan penduaan maklumat, sistem, sistem pengoperasian dan data pada server dan disimpan di luar kawasan *(off site)* secara berkala.	
2.1.9 Pentadbir Rangkaian	
Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut: a. Merancang dan mereka bentuk penggunaan dan perkhidmatan rangkaian LAN dan WAN; b. Memastikan pengguna mendapat segala kemudahan rangkaian termasuk kemudahan internet serta mengawal dan memantau sistem rangkaian bagi memastikan ia beroperasi ke tahap yang paling berkesan; c. Bertanggungjawab mengurus dan mengendalikan segala jenis gangguan berkaitan perkhidmatan rangkaian; d. Mengurus perkhidmatan pengalamatan IP menggunakan DHCP dan statik bagi server serta *Domain Controller* Perbendaharaan; e. Mengendalikan urusan permohonan *public* IP, pembukaan port serta pendaftaran DNS dalaman dan luaran bagi server dan sistem aplikasi yang memerlukan; f. Mengenal pasti dan mengkaji keperluan perlaksanaan dan peningkatan kawalan keselamatan ke atas rangkaian;	Pentadbir Rangkaian

g. Menyelenggara semua peralatan-peralatan rangkaian yang terdapat di Perbendaharaan serta mengemas kini inventori peralatan-peralatan rangkaian tersebut; h. Mengendalikan urusan perolehan peralatan rangkaian termasuk menyediakan kertas kerja berkaitan dengannya; i. Memberi bantuan teknikal kepada pengguna projek kerajaan seperti eSPKB dan ePerolehan; dan j. Membangun, mengurus dan menyelenggara Sistem Pemantauan Infrastruktur ICT Perbendaharaan (TopMetrics).	
2.1.10 Pentadbir Pangkalan Data	
Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut: a. Menjalankan tugas pentadbir pangkalan data dengan memastikan semua pangkalan data yang dibangunkan diurus secara optima dan bertanggungjawab terhadap integriti data dan penggunaan pangkalan data; b. Bertanggungjawab terhadap pengoperasian harian pangkalan data termasuklah membaiki prestasi, *recovery, tuning* dan lain-lain; c. Bertanggungjawab untuk menganalisa log-log server melalui perisian penganalisa log yang diperolehi bagi tujuan untuk menganalisa *behaviour* setiap server dan pangkalan data yang berkaitan; dan d. Mengendalikan urusan perolehan perkakasan dan perisian komputer termasuk penyediaan kertas kerja berkaitan.	Pentadbir Pangkalan Data
2.1.11 Pentadbir Sistem Aplikasi	
Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut: a. Mengambil tindakan yang bersesuaian dengan segera	Pentadbir Sistem Aplikasi

apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ICT Perbendaharaan; c. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; d. Melaporkan aktiviti-aktiviti tidak normal kepada ICTSO dengan segera; e. Menyediakan laporan mengenai aktiviti capaian yang mencurigakan kepada pemilik maklumat sekiranya perlu; dan f. Melaksanakan amalan terbaik dalam menjaga keselamatan maklumat terperingkat di bawah kawalan masing-masing dari pencerobohan dalaman atau luaran seperti: i. Melakukan penyulitan (*encryption*) ke atas maklumat terperingkat terutamanya fail yang mengandungi maklumat id dan kata laluan bagi capaian sistem/server atau *network diagram*; ii. Gunakan kemudahan *password screensaver* atau *lock* PC apabila tiada di tempat; dan iii. Menutup PC sebelum balik atau selepas waktu pejabat.	
2.1.12 Koordinator ICT Bahagian	
Setiap Bahagian akan melantik Koordinator ICT masing-masing. Peranan dan tanggungjawab Koordinator ICT Bahagian adalah seperti berikut: a. Sebagai pegawai perhubungan (*liaison officer*) bagi perkara berkaitan dengan kemudahan ICT Bahagian;	Koordinator ICT Bahagian

b. Menyelaras keperluan ICT Bahagian dan mengemukakan isu-isu berkaitan ICT kepada Pengurus ICT; c. Menyelaras pemulangan aset ICT pegawai yang akan bertukar di Bahagian; d. Mengurus pergerakan peralatan ICT yang dibawa keluar dari premis Perbendaharaan; e. Menguruskan kes kehilangan perkakasan ICT di Bahagian; f. Mengemaskini rekod aset ICT Bahagian dalam Sistem Pengurusan Aset (SPA); g. Menyelaras keperluan kemudahan emel Bahagian; dan h. Menyelaras keperluan latihan ICT Bahagian;	
2.1.13 Koordinator Web Bahagian	
Setiap Bahagian akan melantik Koordinator Web masing-masing. Peranan dan tanggungjawab Koordinator Web Bahagian adalah seperti berikut: a. Mengemaskini maklumat Bahagian/Pegawai melalui Modul Info Perhubungan. Contohnya mengemaskini maklumat pegawai baru masuk/bertukar ke Bahagian seperti nama pegawai, jawatan, seksyen/unit dan nombor telefon; b. Memaklumkan mengenai perkhidmatan yang dikendalikan oleh Bahagian; c. Melakukan pemantauan ke atas soalan yang diterima menerusi Portal sama ada telah dijawab atau tidak; d. Menyemak soalan lazim Bahagian; dan e. Menyemak dan memastikan maklumat Bahagian seperti berikut dikemaskini: • Visi • Misi • Objektif • Fungsi	Koordinator Web Bahagian

• Carta Organisasi • Piagam Pelanggan	
2.1.14 Pengguna	
Peranan dan tanggungjawab Pengguna adalah seperti berikut: a. Membaca, memahami dan mematuhi Polisi ICT Perbendaharaan; b. Lulus tapisan keselamatan atau yang setaraf dengannya; c. Melaksanakan prinsip-prinsip Polisi ICT Perbendaharaan dan menjaga kerahsiaan maklumat Perbendaharaan; d. Melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Menjaga kerahsiaan kata laluan; iii. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; iv. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; v. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; dan vi. Menandatangani Surat Akuan Pematuhan Polisi ICT Perbendaharaan sebagaimana **Lampiran 1**.	Pengguna
2.2 Pihak Ketiga	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga.	

2.2.1 Pembekal, Pakar Runding, Pelawat dan Pihak-Pihak Luar Lain	
Peranan dan tanggungjawab Pihak Luar/Asing adalah seperti berikut: a. Membaca, memahami dan mematuhi Polisi ICT Perbendaharaan di mana berkenaan; b. Bertanggungjawab ke atas sebarang perlanggaran keselamatan disebabkan tindakannya sendiri; c. Melaporkan insiden keselamatan ICT dengan kadar segera kepada ICTSO; dan d. Menjaga kerahsiaan data dan maklumat Perbendaharaan.	Pihak Ketiga (Pembekal, Pakar Runding, Pelawat dan Pihak-Pihak Luar Lain)

Perkara 3 Pengurusan Aset

3.1 Perolehan Aset ICT	
Objektif: Memastikan perolehan Aset ICT mengikut prosedur yang telah ditetapkan.	
3.1.1 Perolehan Perkakasan dan Perisian ICT	
Tatacara perolehan perkakasan dan perisian ICT hendaklah merujuk kepada pekeliling terpakai sedia ada. Garis panduan untuk perolehan perkakasan dan perisian ICT Perbendaharaan adalah seperti di **Lampiran 2.**	Semua
3.2 Peruntukan / Perkongsian Perkakasan dan Perisian ICT	
Objektif: Memastikan perkakasan dan perisian ICT diagihkan mengikut kelayakan dan keperluan.	
3.2.1 PC, Komputer Riba, Projektor LCD dan Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pegawai layak diperuntukkan satu (1) unit PC mengikut keperluan dan jenis yang sesuai. Pegawai gred 48 ke atas diberi pilihan untuk dibekalkan sama ada satu (1) unit PC atau satu (1) unit komputer riba; b. Peralatan-peralatan seperti *Notebook* dan *LCD Projector* perlu diguna secara guna sama di Bahagian-bahagian; c. Pegawai yang membuat peminjaman peralatan guna sama haruslah bertanggungjawab sepenuhnya terhadap keselamatan peralatan yang dipinjam; dan d. Peralatan *mobile* layak dibekalkan kepada pegawai mengikut justifikasi keperluannya.	Pengguna, Koordinator ICT Bahagian
3.2.2 Pencetak	
Perkara yang perlu dipatuhi adalah seperti berikut:	BPTM/ Koordinator ICT

a. Setiap Bahagian layak diperuntukkan satu unit pencetak warna untuk diguna sama di kalangan pegawai dan kakitangan; b. Pencetak berwarna jenis kapasiti tinggi yang dibekalkan di Perbendaharaan adalah untuk diguna sama oleh Bahagian-bahagian; c. Pegawai gred 48 ke atas layak dan boleh dibekalkan dengan sebuah pencetak *light duty* setiap pegawai; dan d. Untuk pegawai-pegawai selain daripada (c) di atas, pencetak perlulah diguna secara '*pool*' dengan nisbah yang difikirkan sesuai untuk kelancaran kerja dan jenis kerja yang dilakukan seperti kerahsiaan maklumat, kedudukan tempat dan proses kerja.	Bahagian
3.3 Akauntabiliti Aset	
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Perbendaharaan.	
3.3.1 Inventori Aset	
Semua aset ICT Perbendaharaan hendaklah direkodkan dalam Sistem Pengurusan Aset (SPA). Ini termasuklah merekodkan maklumat penempatan dan penyelenggaraan sehingga pelupusan aset berkenaan. Setiap Pengguna adalah bertanggung jawab ke atas semua aset ICT di bawah kawalannya.	BPTM/ Koordinator ICT Perbendaharaan/ Pegawai Aset Bahagian Semua
3.4 Pengelasan dan Pengendalian Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
3.4.1 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap	Semua

maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: • Rahsia Besar; • Rahsia; • Sulit; atau • Terhad.	
3.4.2 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menjaga kerahsiaan kata laluan; d. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; e. Melakukan penyulitan *(encryption)* bagi maklumat terperingkat sebelum transmisi; dan f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.	Semua

Perkara 4 Keselamatan Sumber Manusia

4.1 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif:

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

4.1.1 Sebelum Memulakan Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan Perbendaharaan serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan Perbendaharaan 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.	Semua

4.1.2 Semasa Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan pegawai dan kakitangan Perbendaharaan serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Perbendaharaan; b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna	Semua

ICT Perbendaharaan 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 Perbendaharaan serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh Perbendaharaan; 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.	
4.1.3 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan semua aset ICT dikembalikan kepada Perbendaharaan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; b. Memulangkan dan menghapuskan sebarang dokumen atau maklumat rasmi yang berkaitan dengan tugas atau tempat di mana ia ditugaskan;dan c. Membatalkan atau menghapuskan semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh Perbendaharaan dan/atau terma perkhidmatan.	Semua BPTM
4.2 Pendidikan	
Objektif: Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.	
4.2.1 Program Kesedaran Keselamatan ICT	
Pengguna ICT Perbendaharaan harus menyertai program kesedaran, latihan atau kursus mengenai keselamatan ICT yang dikendalikan BPTM, bertujuan untuk meningkatkan kesedaran dan	ICTSO

pengetahuan serta diamalkan semasa melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden bagi membangun kepakaran Unit Keselamatan ICT amat perlu sebagai langkah proaktif dalam mengurangkan ancaman keselamatan ICT Perbendaharaan.	

Perkara 5 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 Kawasan Larangan

Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Pusat Data dan Pusat Pemulihan Bencana (DRC) adalah kawasan larangan, di mana: a. Akses kepada kawasan tersebut hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; b. Pihak ketiga adalah dibenarkan memasuki Pusat Data dan DRC bagi memberi perkhidmatan sokongan atau bantuan teknikal. Walau bagaimanapun, mereka hendaklah diiringi sepanjang masa sehingga tugas selesai; dan c. Semua aktiviti dan penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat hendaklah dikawal dan mendapat kebenaran daripada Pengurus Pusat Data/DRC.	Semua

5.2 Keselamatan Peralatan

Objektif:
Melindungi peralatan ICT Perbendaharaan daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

5.2.1 Peralatan ICT

Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Semua

a. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; c. 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; dan d. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.	
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*, CD/DVD ROM, *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 sesuai dan mempunyai ciri-ciri keselamatan berpadanan dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; c. Akses dan pergerakan media storan hendaklah direkodkan; d. Sebarang aktiviti penghapusan maklumat yang terkandung dalam media storan, mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; e. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan	Semua

kehilangan data; dan f. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat.	
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.	Semua
5.2.4 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perisian-perisian ICT yang disokong oleh BPTM untuk pemasangan, penyelenggaraan dan latihan adalah termasuk: i. MS Office yang terdiri daripada: • MS Word • MS Excel • MS Powerpoint • MS Outlook ii. Internet Explorer / Mozilla Firefox iii. Acrobat Reader iv. WinZip v. Antivirus vi. Dewan Eja b. Sokongan untuk perisian yang tidak tersenarai di item (a) seperti perisian Open Office, SAS, SPSS dan eViews hanya akan diberikan sekiranya ada tenaga kepakaran di BPTM; c. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan Perbendaharaan. Pengguna dilarang memasang (*install*) perisian ICT yang tidak berdaftar, berlesen, cetak	Semua

rompak atau perisian yang dibeli sendiri pada mana-mana aset ICT Perbendaharaan; d. Pihak BPTM boleh mengesan dan berhak membuang *(uninstall)* perisian yang tidak diperakui tanpa perlu mendapat kebenaran pengguna; e. Pengguna tidak dibenarkan membuang sebarang perisian yang telah dipasang oleh BPTM di dalam PC atau komputer riba masing-masing; f. Pengguna mesti memastikan media storan *(disket, CD/DVD* atau *thumb drive)* yang menyimpan dokumen terperingkat disimpan di tempat yang selamat; dan g. Pengguna mesti memastikan maklumat rahsia rasmi yang terkandung dalam media storan seperti pita magnetik, cakera keras, CD/DVD, *optical disk, removal disk (thumb/PenDrive)* dan lain-lain, dikawal dan dilindungi dengan perisian penyulitan *(encryption)* yang disyorkan oleh BPTM.	
5.2.5 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi yang telah ditetapkan oleh pengeluar; b. Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c. Semua perkakasan hendaklah disemak serta diuji sebelum dan selepas proses penyelenggaraan *(Preventive Maintenance)* dilakukan; d. Penyelenggaraan peralatan perkakasan ICT di Bahagian-bahagian perlulah di selaras oleh BPTM bagi memudahkan pemantauan dan inventori; e. *Housekeeping*/penyelenggaraan PC seperti *disk cleanup*, *error-checking*, *defragment* dan *backup* perlu dilaksanakan	Semua, Pegawai Aset dan BPTM

sendiri oleh pengguna bagi memastikan keupayaan PC adalah sentiasa dalam keadaan optimum. BPTM bertanggungjawab menyediakan tatacara *housekeeping*/ penyelenggaraan PC dari masa ke semasa; f. Perisian sistem pengoperasian bagi perkakasan ICT di Bahagian-bahagian, dikonfigurasi supaya dikemas kini *patches* dan dinaiktarafkan (*upgrades*) kepada versi terkini secara automatik; dan g. Bantuan teknikal/aduan tentang masalah-masalah yang dihadapi dalam penggunaan ICT perlu diajukan kepada: i. *Helpdesk* Perbendaharaan – 8882 4444; ii. *Helpdesk* BPP – 8880 2714/2733	
5.2.6 Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari premis Perbendaharaan adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan/Koordinator ICT dan tertakluk kepada tujuan yang dibenarkan; b. Bagi peralatan gunasama yang dipinjam, aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan; c. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan d. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua
5.2.7 Pelupusan Perkakasan	
Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan Perbendaharaan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Semua

a. Semua kandungan dan maklumat dalam peralatan ICT khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degaussing, electronic data erasure* atau pembakaran; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; dan c. Pelupusan adalah tertakluk kepada Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk ”Tatacara Pengurusan Aset Alih Kerajaan” atau pekeliling terbaru yang berkuatkuasa.	

5.3 Keselamatan Persekitaran

Objektif:
Melindungi aset ICT Perbendaharaan daripada 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, mengubahsuai atau pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: a. Merancang dan menyediakan pelan keseluruhan susun atur Pusat Data/DRC (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Semua kawasan larangan khususnya bilik pemprosesan	Semua

maklumat dan perkakasan ICT yang menyimpan data dan maklumat rahsia rasmi tidak boleh dilabel. Ia perlu dilindungi dari sebarang pendedahan dan akses oleh individu yang tidak dibenarkan; e. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; f. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; g. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan h. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	
5.3.2 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data/DRC Perbendaharaan supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Penyenggara Bangunan dan BPTM

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; dan c. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Semua
5.3.4 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap Pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Perbendaharaan.	Semua
5.4 Keselamatan Dokumen	
Objektif: Melindungi maklumat Perbendaharaan daripada 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. Sistem dokumentasi atau penyimpanan maklumat hendaklah dipastikan selamat dan terjamin; b. Setiap dokumen hendaklah difail dan dilabelkan mengikut	Semua

klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; c. Dokumen yang mengandungi bahan atau maklumat sensitif hendaklah diambil segera dari pencetak; dan d. Menggunakan penyulitan (*encryption*) ke atas dokumen sulit dan terhad yang disediakan dan dihantar secara elektronik.	

Perkara 6 Pengurusan Operasi dan Komunikasi

6.1 Pengurusan Prosedur Operasi

Objektif:
Memastikan operasi ICT berfungsi dengan lancar dan efisien serta selamat daripada sebarang ancaman dan gangguan.

6.1.1 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Prosedur pengurusan operasi ICT hendaklah didokumen dan diguna pakai; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti turutan aktiviti, peranan dan tanggungjawab, kekerapan dikendalikan dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua

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 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	Semua

ada secara sengaja atau pun tidak.	

6.2 Perancangan dan Penerimaan Sistem

Objektif:
Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

6.2.1 Perancangan Kapasiti

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. 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; dan b. 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.	Pentadbir Sistem ICT/Pentadbir Sistem Aplikasi/ Pentadbir Pangkalan Data dan ICTSO

6.2.2 Penerimaan Sistem Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui; b. Sebarang penyerahan atau penerimaan sistem baru perlu mendapat pengesahan/kelulusan pemilik sistem dan perlu melalui proses UAT *(User Acceptance Test)* dan FAT *(Final Acceptance Test);* dan c. Penyelenggaraan sistem tersebut adalah berdasarkan manual operasi dan prosedur yang ditetapkan.	BPTM, Pentadbir Sistem Aplikasi dan Pemilik Sistem

6.2.3 Penerimaan Perkakasan dan Perisian Sistem Baru	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan dan perisian sistem baru (termasuklah pengemaskinian *patches*) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui; b. Sebarang penyerahan atau penerimaan perkakasan dan perisian sistem perlu mendapat pengesahan/kelulusan pemilik sistem dan perlu melalui proses PAT *(Provisional Acceptance Test)* dan FAT *(Final Acceptance Test);* dan c. Penyelenggaraan sistem tersebut adalah berdasarkan manual operasi dan prosedur yang ditetapkan.	BPTM, Pentadbir Sistem ICT dan Pemilik Sistem

6.3 Perisian Berbahaya
Objektif: Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya.

6.3.1 Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus dan *Intrusion Detection System* (IDS), *Intrusion Protection System* (IPS) dan mengikut prosedur penggunaan yang betul dan selamat; b. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; c. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; d. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; e. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian.	Semua

Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; f. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan g. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
6.3.2 Perlindungan dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
6.4 *Housekeeping*	
Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.	
6.4.1 Penduaan	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat salinan penduaan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; dan c. Menguji sistem penduaan sedia ada bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.	Semua

6.5 Pengurusan Rangkaian

Objektif:
Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

6.5.1 Kawalan Infrastruktur Rangkaian

Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengasingan antara kerja-kerja pengoperasian rangkaian dan pengkomputeran perlu dilaksanakan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas daripada risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. Peralatan rangkaian harus di selenggara secara berkala oleh kakitangan atau pihak yang dibenarkan sahaja; e. Peralatan rangkaian yang kritikal harus mempunyai kontrak penyelenggaraan yang menyeluruh dan berkala; f. Semua peralatan mestilah melalui proses *User Acceptance Test (UAT)* dan *Final Acceptance Test* (FAT) selepas pemasangan dan konfigurasi; g. Semua aliran trafik keluar/masuk rangkaian hendaklah melalui *Firewall* di bawah kawalan Perbendaharaan; h. Semua jenis perisian *sniffer* atau *network analyzer* adalah dilarang dipasang kecuali mendapat kebenaran ICTSO; i. Memasang perisian *Intrusion Detection System* (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat Perbendaharaan;	Pentadbir Rangkaian

j. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan"; k. Sebarang penyambungan rangkaian yang bukan di bawah kawalan Perbendaharaan hendaklah mendapat kebenaran ICTSO; dan l. Semua Pengguna hanya dibenarkan menggunakan rangkaian Perbendaharaan sahaja. Penggunaan 3G *Broadband* dan seumpamanya adalah dilarang sama sekali.	
6.6 Pengurusan Media	
Objektif: Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
6.6.1 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	Semua
6.6.2 Prosedur Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Mengehadkan dan menentukan capaian media kepada pengguna yang sah sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan	Semua

yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	
6.6.3 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	BPTM
6.7 Pengurusan Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara Perbendaharaan dan agensi luar terjamin.	
6.7.1 Pengurusan Mel Elektronik (E-mel)	
Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: a. Akaun e-mel bukanlah hak mutlak seseorang. Ia adalah kemudahan yang tertakluk kepada peraturan jabatan dan boleh ditarik balik jika penggunaannya melanggar peraturan; b. Pewujudan akaun e-mel adalah berdasarkan standard yang telah ditetapkan iaitu nama_pengguna.nama_bapa@treasury.gov.my; c. Warga Perbendaharaan adalah bertanggungjawab kepada akaun e-mel masing-masing. Perbendaharaan tidak akan	Semua

bertanggungjawab ke atas sebarang kesalahan jenayah dan seumpamanya berkaitan e-mel;

d. Warga Perbendaharaan wajib menggunakan e-mel Perbendaharaan dalam urusan rasmi dan urusan pentadbiran harian;

e. Warga Perbendaharaan tidak dibenarkan menggunakan kemudahan e-mel percuma seperti *Hotmail, GMail* dan *Yahoo* untuk tujuan rasmi;

f. Warga Perbendaharaan adalah dinasihatkan menggunakan kemudahan e-mel secara rutin sekurang-kurangnya sekali sehari;

g. Pengguna TIDAK dibenarkan menghantar maklumat Rahsia atau Rahsia Besar melalui e-mel;

h. Setiap akaun e-mel yang disediakan adalah untuk kegunaan individu berkenaan sahaja. Penggunaan akaun milik orang lain adalah dilarang;

i. Pengguna dilarang melakukan pencerobohan atau percubaan untuk menceroboh masuk ke mana-mana akaun pengguna lain;

j. Menyebar perisian cetak rompak atau maklumat berbau politik, hasutan atau perkauman atau apa-apa maklumat yang menjejaskan reputasi Perbendaharaan dan Perkhidmatan Awam melalui kemudahan e-mel Perbendaharaan adalah dilarang;

k. Elakkan dari menerima dan membuka e-mel di mana penghantarnya tidak diketahui dan diragui dan pengguna perlulah memadam terus e-mel tersebut;

l. Had saiz kotak e-mel *(mailbox)* setiap pengguna adalah 1GB, manakala had penghantaran e-mel termasuk bahan kepilan yang dibenarkan adalah tidak melebihi 10 MB;

m. Pengguna adalah bertanggungjawab untuk mengurus dan memastikan saiz e-mel yang disimpan di dalam peti mail *(mailbox)* masing-masing tidak melebihi kuota yang telah ditetapkan;

n. Warga Perbendaharaan diminta menukarkan kata laluan masing-masing setiap tiga (3) bulan bagi mengelakkan kata laluan bocor kepada pihak yang tidak bertanggungjawab;	
o. Warga Perbendaharaan dikehendaki merahsiakan identiti pengguna dan kata laluan daripada pengetahuan orang lain;	
p. Pengguna harus menggunakan perisian penyulitan yang disyorkan oleh BPTM untuk menghantar dokumen dan maklumat terperingkat melalui e-mel;	
q. Warga Perbendaharaan juga hendaklah memastikan fail yang akan dihantar atau yang diterima melalui kepilan *(attachment)* bebas dari virus dengan melakukan *scanning* dengan perisian antivirus;	
r. Aktiviti *spamming*, penyebaran virus, bahan-bahan negatif dan surat berantai adalah dilarang. Jika didapati dilakukan oleh Warga Perbendaharaan, akaun mereka boleh dibatalkan tanpa sebarang notis;	
s. Koordinator ICT Bahagian perlu memaklumkan sebarang perubahan status pengguna kepada Pentadbir e-mel jika terdapat pertukaran masuk dan keluar jabatan, bersara, diberhentikan dan lain-lain bagi tujuan kawalan keselamatan dan pengemaskinian akaun pengguna Perbendaharaan;	Koordinator ICT Bahagian
t. Akaun e-mel yang tidak digunakan untuk tempoh melebihi 30 hari akan dibekukan penggunaannya dan seterusnya dihapuskan selepas tiga (3) bulan kecuali telah dimaklumkan kepada BPTM;	Pentadbir Sistem ICT
u. Capaian e-mel Warga Perbendaharaan yang tidak lagi berkhidmat di Perbendaharaan akan dihentikan serta-merta;	Pentadbir Sistem ICT
v. Pentadbir Sistem ICT berhak memasang sebarang jenis perisian atau perkakasan penapisan e-mel dan virus yang difikirkan sesuai dan boleh menggunakannya untuk mencegah, menapis, menyekat atau menghapuskan mana-mana e-mel yang disyaki mengandungi virus atau berunsur *spamming* daripada memasuki komputer; dan	Pentadbir Sistem ICT
w. Pihak Pengurusan atau Pentadbir Sistem ICT boleh	Pentadbir

memantau semua e-mel Perbendaharaan jika perlu tanpa mendapat kebenaran Warga Perbendaharaan.	Sistem ICT

6.8 Pemantauan

Objektif:
Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

6.8.1 Pengauditan dan Forensik ICT

ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT Perbendaharaan; 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 Rangkaian.	ICTSO

6.8.2 Jejak Audit

Setiap sistem mestilah mempunyai jejak audit *(audit trail).* Jejak audit	Pentadbir

merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi tujuan pemeriksaan dan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: a. Rekod setiap aktiviti transaksi; b. Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh/masa aktiviti, rangkaian dan aplikasi yang digunakan; c. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan d. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT dan Pentadbir Sistem Aplikasi 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 daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Sistem Aplikasi dan Pentadbir Sistem ICT
6.8.3 Sistem Log	
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian Pengguna; b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti tidak sah seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	Pentadbir Sistem ICT

6.8.4 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 dan menganalisa log perlu diwujudkan dan hasilnya dipantau secara berkala; c. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d. Aktiviti *housekeeping* perlu direkod dan dilaksanakan secara berkala; e. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan, dianalisis dan diambil tindakan sewajarnya; dan f. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Perbendaharaan atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	Pentadbir Sistem ICT

Perkara 7 Kawalan Capaian

7.1 Kawalan Capaian	
Objektif: Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT Perbendaharaan.	
7.1.1 Keperluan Kawalan Capaian	
Capaian kepada sistem dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong polisi kawalan capaian pengguna sedia ada.	BPTM
7.2 Pengurusan Capaian Pengguna	
Objektif: Mengawal capaian pengguna ke atas aset ICT Perbendaharaan.	
7.2.1 ID Pengguna	
Pengguna adalah bertanggungjawab ke atas ID Pengguna yang diberi untuk capaian sistem aplikasi. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: a. ID Pengguna yang diperuntukkan oleh Perbendaharaan sahaja boleh digunakan. Penggunaan id milik orang lain atau id yang dikongsi bersama adalah dilarang; b. ID Pengguna mestilah unik; c. ID Pengguna yang diwujud 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 ID Pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. ID boleh ditarik balik jika penggunaannya melanggar peraturan;	Semua

e. Pentadbir Sistem Aplikasi harus menyemak ID Pengguna dan hak aksesnya bagi menentukan ketepatan dan kesempurnaan sesuatu tahap capaian secara berkala; dan f. Pentadbir Sistem Aplikasi boleh menggantung *(suspend)* dan menamatkan ID Pengguna atas sebab-sebab berikut: i. Bertukar bidang tugas kerja; 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.	Pentabir Sistem Aplikasi
7.2.3 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh Perbendaharaan seperti berikut: a. Semua Pengguna baru hendaklah memohon id pengguna dengan mengisi borang yang disediakan; b. Penukaran kata laluan perlulah dibuat oleh Pengguna setiap tiga (3) bulan; c. Kata laluan hendaklah tidak dipaparkan semasa input; d. Panjang kata laluan sekurang-kurangnya 12 aksara; e. Kata laluan mesti menggunakan kombinasi daripada aksara, angka dan simbol-simbol lain; f. Kata laluan tidak boleh dikongsi dengan orang lain; g. Menggunakan kata laluan yang selamat dan tidak mudah dicerobohi. Penggunaan kata laluan yang sukar diramal oleh	Semua

penggodam adalah digalakkan; h. Cubaan capaian dihadkan kepada tiga (3) kali sahaja. Akaun berkenaan akan disekat selepas tiga (3) kali cubaan gagal secara berturutan. Akaun akan diaktifkan kembali selepas pengesahan identiti pengguna sebenar berjaya dilakukan; i. Pengguna dilarang menggunakan kata laluan yang sama dengan id pengguna; dan j. Kata laluan hendaklah diingat dan tidak digalakkan dicatat, disimpan atau didedahkan dengan apa cara sekalipun.	
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* bermaksud tidak meninggalkan dokumen terperingkat terdedah sama ada atas meja warga atau di paparan skrin apabila anggota Perbendaharaan tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; dan b. Dokumen terperingkat hendaklah disimpan dalam laci atau kabinet fail yang berkunci.	Semua
7.3 Penggunaan dan Pengurusan Rangkaian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
7.3.1 Infrastruktur Rangkaian	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Semua komunikasi rangkaian dari Perbendaharaan ke sistem luar hendaklah melalui rangkaian berpusat Perbendaharaan	Semua

untuk memudahkan pengurusan, penguatkuasaan dan pemantauan terhadap sebarang ancaman keselamatan ICT; b. Hanya warga Perbendaharaan sahaja yang dibenarkan mengguna rangkaian Perbendaharaan; dan c. Pengguna luar yang ingin menggunakan kemudahan rangkaian Perbendaharaan hendaklah mendapat kebenaran Pentadbir Rangkaian.	
7.3.2 Sambungan Rangkaian	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Semua permohonan untuk mendapatkan sambungan rangkaian Perbendaharaan mestilah mendapatkan kebenaran BPTM; b. Pengguna tidak dibenarkan menyambung sebarang peralatan peribadi ke dalam rangkaian Perbendaharaan tanpa kebenaran BPTM; c. Pengguna tidak dibenarkan sama sekali memasang sebarang *access point* untuk capaian secara tanpa wayar (*wireless)* ke dalam rangkaian Perbendaharaan; d. Pengguna tidak dibenarkan memutuskan/menyambung sambungan kabel UTP pada mana-mana *port* dalam rak peralatan rangkaian di Bilik Telco tanpa kebenaran dari pihak BPTM; e. Perbuatan yang boleh merosakkan UTP port, kabel UTP atau rak peralatan rangkaian serta peralatannya adalah dilarang; f. Pengguna tidak dibenarkan menukar maklumat yang terdapat pada *faceplate* (UTP port); dan g. Sebarang kerosakan pada kabel UTP atau masalah capaian rangkaian hendaklah dilaporkan kepada BPTM.	Semua
7.3.3 Pengurusan Alamat IP	
Perkara yang perlu dipatuhi adalah seperti berikut:	Semua

a. Pengguna adalah dilarang sama sekali menukar konfigurasi IP di dalam komputer masing-masing tanpa kebenaran BPTM; b. Sebarang keperluan menggunakan IP statik hendaklah dipohon kepada BPTM; dan c. IP statik yang diberikan kepada Pengguna tidak boleh digunakan untuk kepentingan sendiri. Sekiranya Pengguna didapati menyalahgunakan IP statik, PC Pengguna berkenaan akan dihalang daripada membuat capaian ke rangkaian Perbendaharaan.	
7.3.4 Talian Internet Persendirian	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Kemudahan talian internet persendirian seperti *3G Broadband* dan seumpamanya hanya dibenarkan untuk tujuan rasmi dan mendapat kebenaran daripada BPTM; b. Pengguna hendaklah memutuskan (*disable/disconnect)* sambungan ke rangkaian Perbendaharaan terlebih dahulu sebelum menggunakan talian internet persendirian. Penggunaan talian persendirian dan rangkaian Perbendaharaan secara serentak adalah dilarang; dan c. Setelah menggunakan kemudahan tersebut pengguna dikehendaki mengimbas keseluruhan komputer yang digunakan sebelum menyambung semula ke rangkaian Perbendaharaan bagi memastikan tiada virus masuk ke rangkaian Perbendaharaan.	Semua
7.3.5 Antivirus	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Kesemua perkakasan seperti PC dan komputer riba yang bersambung ke rangkaian Perbendaharaan mesti mempunyai antivirus yang dibekalkan oleh BPTM; b. Pengguna tidak dibenarkan memasang antivirus lain selain	Semua

yang dibekalkan oleh BPTM; c. Sebarang perkakasan yang didapati menyebarkan virus dan setara dengannya, akan diputuskan hubungan ke rangkaian Perbendaharaan sehinggalah virus berkenaan dihapuskan; d. Semua Pengguna hendaklah membuat *scanning* semua fail yang telah dimuat turun dari mana-mana sumber termasuklah e-mel; e. Sebarang media seperti disket, *thumb drive* dan CD/DVD perlu diimbas sebelum sebarang fail dibaca atau disalin ke PC masing-masing; dan f. Mana-mana pegawai yang didapati menjadi pembawa atau penyebar virus akan dilaporkan terus kepada pihak pengurusan.	
7.4 Keselamatan Internet	
Objektif: Melindungi aset ICT melalui sistem komunikasi Internet yang selamat.	
7.4.1 Internet	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan/Pegawai yang diberi kuasa; b. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan; c. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Setiausaha Bahagian sebelum dimuat naik ke Internet; d. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;	Semua

e. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh Perbendaharaan; f. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*; dan g. Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".	
7.4.2 Melayari Internet	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna yang melayari aplikasi dan laman web adalah bertanggungjawab sepenuhnya ke atas maklumat yang dikunci masuk serta capaian yang dilakukan; b. Pengguna tidak dibenarkan menggunakan rangkaian *3G Broadband* dan seumpamanya untuk melayari aplikasi dan laman web tanpa kebenaran daripada BPTM; c. Penghantaran dokumen yang mengandungi maklumat terperingkat (sulit atau terhad) melalui internet hendaklah melalui proses penyulitan terlebih dahulu menggunakan perisian penyulitan yang disyorkan oleh BPTM; d. Pengguna adalah dilarang menyumbangkan perkara-perkara bertentangan dengan Perintah Am Kerajaan kepada mana-mana laman web tanpa kebenaran Ketua Jabatan; e. Pengguna tidak dibenarkan membuat capaian kepada bahan-bahan terlarang seperti laman pornografi, perisian judi, permainan dan lain-lain yang melalaikan atau seumpamanya dengan menggunakan kemudahan pejabat; f. Pada waktu pejabat, Pengguna hanya dibenarkan membuat capaian kepada laman web jaringan sosial yang berkaitan dengan urusan rasmi agensi sahaja;	Semua

g. Capaian laman yang berbentuk hiburan, permainan komputer *online*, radio *online* dan *video streaming* yang membebankan rangkaian Perbendaharaan adalah tidak dibenarkan; h. Pengguna tidak dibenarkan melayari laman-laman yang tidak berkaitan dengan tugas di waktu pejabat; i. Pengguna tidak dibenarkan melanggan kepada mana-mana *mailing list* yang tidak berkaitan dengan tugas; j. Aktiviti *chatting* adalah tidak dibenarkan; k. Aktiviti muat turun (*download*) atau muat naik (*upload*) sebarang perisian cetak rompak adalah dilarang; l. Penggunaan sebarang perisian *Internet Proxy* untuk capaian ke internet adalah tidak dibenarkan. Pentadbir Rangkaian berhak menyekat capaian ke internet bagi PC yang dikesan menggunakan perisian tersebut; m. Pentadbir Sistem ICT adalah diberi kuasa untuk menjana laporan capaian rangkaian dan internet setiap pengguna kepada pihak pengurusan; n. Pentadbir Sistem ICT berhak menyediakan dan memasang perisian penapisan isi kandungan internet; o. Pentadbir Sistem ICT berhak menapis, menghalang dan menegah penggunaan mana-mana laman web yang tidak sesuai; dan p. Kemudahan *Wireless* LAN perlu dipastikan mempunyai kawalan keselamatan.	
7.5 Kawalan Capaian Sistem Pengoperasian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
7.5.1 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan	ICTSO dan

sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian kepada sumber sistem komputer. Kemudahan ini juga perlu bagi: a. Mengenal pasti identiti, terminal atau lokasi bagi setiap Pengguna yang dibenarkan; dan b. Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a. Mengesahkan Pengguna yang dibenarkan; b. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama Pengguna bertaraf *Super User*; dan c. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; b. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap Pengguna dan hanya digunakan oleh Pengguna berkenaan sahaja; c. Mengehadkan dan mengawal penggunaan program; dan d. Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	Pentadbir Sistem ICT
7.5.2 Kad Pintar/*Soft Cert*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan kad pintar Kerajaan Elektronik (Kad EG)/*Soft Cert* hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan;	Semua

b. Kad pintar/*Soft Cert* hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c. Perkongsian kad pintar/*Soft Cert* untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar/*Soft Cert* yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan d. Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pengeluar kad pintar/*Soft Cert.*	
7.6 Kawalan Capaian Sistem dan Aplikasi	
Objektif: Melindungi sistem maklumat dan aplikasi sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.	
7.6.1 Sistem Maklumat dan Aplikasi	
Capaian sistem dan aplikasi di Perbendaharaan adalah terhad kepada Pengguna dengan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi:	
a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan;	Pengguna
b. Setiap aktiviti capaian sistem maklumat dan aplikasi Pengguna hendaklah direkodkan (*log*) bagi mengesan aktiviti-aktiviti yang tidak diingini;	Pentadbir Sistem Aplikasi
c. Memaparkan notis amaran pada skrin komputer Pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan;	Pentadbir Sistem Aplikasi
d. Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan Pengguna akan disekat;	Pentadbir Sistem Aplikasi

e. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan	Pentadbir Rangkaian
f. Untuk mengelakkan capaian terus secara fizikal kepada server yang berada di Pusat Data, capaian sistem maklumat dan aplikasi melalui jarak jauh (*remote*) adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada pegawai berkenaan dan perkhidmatan yang dibenarkan sahaja.	Pentadbir Sistem Aplikasi

7.7 Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif:
Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan bagi komputer mudah alih dan kerja jarak jauh.

7.7.1 Penggunaan Peralatan Mudah Alih

Perkara yang perlu dipatuhi adalah seperti berikut: a. Merekodkan aktiviti keluar masuk peralatan komputer mudah alih gunasama bagi memantau pergerakan peralatan tersebut; dan c. Kabel keselamatan *(cable lock)* hendaklah dipasang pada peralatan mudah alih yang dibekalkan dengan kemudahan tersebut dan disimpan atau dikunci di tempat yang selamat apabila tidak digunakan.	Semua

7.7.2 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.	Semua

Perkara 8 Perolehan, Pembangunan dan Penyelenggaraan Sistem

8.1 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

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

8.1.1 Keselamatan Aplikasi

Perkara yang perlu dipatuhi adalah seperti berikut: a. Pembangunan sistem aplikasi harus mengambil kira keperluan aspek keselamatan yang ditetapkan pada setiap peringkat perolehan, pembangunan dan penyelenggaraan bagi memastikan tidak wujud sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan seperti berikut: i. Sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan; ii. Sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna; dan iii. Sistem output untuk memastikan data yang telah diproses adalah tepat. c. Sebaik-baiknya, semua sistem aplikasi yang dibangunkan sama ada secara dalaman atau *outsource* hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan mematuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan. Ujian tahap keselamatan harus merangkumi Penilaian Keterdedahan *(Vulnerability Assessment)* oleh pihak berkenaan sebelum pengaktifan sistem; dan d. Pemilik Sistem perlu mengenalpasti sama ada maklumat dalam sistem aplikasi tersebut memerlukan penentusahan melalui PKI dan tandatangan digital.	Pemilik Sistem, Pentadbir Sistem Aplikasi, Pentadbir Sistem ICT dan Unit Keselamatan ICT

8.2 Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
8.2.1 Penyulitan	
Pengguna hendaklah membuat penyulitan (*encryption*) ke atas maklumat sensitif atau maklumat terperingkat (sulit atau terhad) pada setiap masa.	Semua
8.2.2 Tandatangan Digital	
Penggunaan tandatangan digital adalah mengikut keperluan khususnya kepada mereka yang menguruskan transaksi maklumat terperingkat (sulit atau terhad) secara elektronik.	Semua
8.2.3 Pengurusan Infrastruktur Kunci Awam (*PKI*)	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua
8.3 Pembangunan Perisian	
Objektif: Memastikan supaya pembangunan sistem diselia dan dipantau untuk memastikan ia mengikut jadual yang telah ditetapkan.	
8.3.1 Pembangunan Sistem Aplikasi	
Perkara yang perlu dipatuhi adalah seperti berikut:	
a. Bahagian-bahagian hendaklah memohon secara rasmi kepada BPTM untuk membangunkan sesuatu sistem aplikasi;	Pemilik Sistem
b. Bahagian perlu memohon kepada JPICT kebenaran untuk membangunkan sistem aplikasi. Permohonan ini hendaklah lengkap meliputi spesifikasi teknikal, anggaran kos yang terlibat, guna tenaga dan juga skop perluasan sistem aplikasi tersebut;	Pemilik Sistem

c. Sesuatu sistem aplikasi perlu mempunyai Pemilik (*owner)* iaitu sesuatu Bahagian atau pengguna utama (yang paling banyak menggunakan sistem atau yang paling banyak memiliki data);	Pemilik Sistem
d. Pengguna yang bertukar bidang tugas atau tidak lagi berkhidmat di Perbendaharaan akan dihapus ID dan capaiannya ke aplikasi dalam masa 30 hari;	Pentadbir Sistem ICT
e. Bahagian yang memohon akan menjadi Pemilik (*owner)* kepada sistem aplikasi tersebut dan hendaklah melantik *champion* bagi melancarkan pelaksanaan sistem aplikasi. *Champion* seboleh-sebolehnya di peringkat TSUB dan mendapat mandat daripada TKSP yang berkaitan;	Pemilik Sistem
f. Pengguna perlu membaca, memahami dan mematuhi prosedur menggunakan sistem melalui dokumen-dokumen yang disediakan;	Pengguna
g. Sesuatu sistem aplikasi yang perlu diintegrasikan dengan sistem aplikasi yang lain hendaklah diterajui oleh Pemilik (*owner)* sistem aplikasi tersebut;	Pemilik Sistem
h. Pemilik (o*wner)* sistem aplikasi perlu membuat pelaporan kepada JPICT secara berkala bagi kemajuan (*progress)* sistem aplikasi tersebut;	Pemilik Sistem
i. Pembangunan sistem aplikasi hendaklah mengambil kira sistem aplikasi sedia ada di agensi berkenaan dan agensi lain bagi mengelakkan pertindihan pembangunan sistem aplikasi yang sama. Sebagai contoh pembangunan sistem yang berkaitan sumber manusia hendaklah dielakkan kerana HRMIS telah sedia untuk diguna pakai;	Pembangun Sistem
j. Sebarang pembangunan sistem aplikasi mestilah mengguna pakai kod-kod yang standard di bawah *Data Dictionary* Sektor Awam (DDSA); dan	Pembangun Sistem
k. Sebarang pembangunan aplikasi yang melibatkan borang yang diwartakan perlulah mendapatkan kelulusan menteri yang berkenaan oleh Pemilik (*owner)* sesuatu sistem aplikasi.	Pemilik Sistem
l. Pembangunan sistem aplikasi adalah digalakkan menggunapakai perisian *Open Source* selaras dengan hasrat	Pemilik Sistem

MAMPU dalam memperluaskan penggunaan produk Open Source di agensi kerajaan. Garis panduan untuk pembangunan sistem aplikasi adalah seperti di **Lampiran 4.**	
8.3.2 Permohonan Perubahan/Keperluan Tambahan Sistem Aplikasi Sedia Ada	
Sesuatu spesifikasi keperluan sistem aplikasi yang telah dipersetujui, tetapi memerlukan perubahan atau tambahan keperluan hendaklah dimohon secara bertulis atau menggunakan borang permohonan yang disediakan.	Pemilik Sistem
8.4 Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
8.4.1 Kawalan Fail Sistem	
Perkara yang perlu dipatuhi adalah seperti berikut:	
a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem Aplikasi atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;	Pentadbir Sistem Aplikasi
b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji;	Pentadbir Sistem Aplikasi
c. Mengaktifkan *audit log* bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan;	Pentadbir Sistem ICT
d. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan	Pentadbir Sistem Aplikasi dan Pentadbir Sistem ICT
e. Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan.	

8.5 Pembangunan dan Proses Sokongan	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
8.5.1 Kawalan Perubahan	
Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.	Pentadbir Sistem Aplikasi
8.6 Pembayaran *Online*	
Objektif: Menerangkan dengan lebih terperinci prosedur yang perlu dipatuhi dalam proses pembayaran *online* di dalam sistem.	
8.6.1 Pembayaran *Online* bagi Sistem	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Pemilik Sistem perlu menentukan kaedah pembayaran (*Financial Process Exchange* (FPX)/kad kredit (Visa dan Mastercard); b. Pemilik Sistem perlu memohon kelulusan Seksyen Khidmat Perunding (SKP), Jabatan Akauntan Negara Malaysia (JANM) untuk pelaksanaan pembayaran secara *online* melalui sistem; c. Pemilik Sistem perlu mendapatkan kelulusan daripada Bahagian Pengurusan Kewangan Strategik (BPKS) untuk resit rasmi yang dijana melalui sistem (selaras dengan Surat Pekeliling Akauntan Negara Malaysia Bilangan 3 Tahun 2007); d. Pemilik Sistem perlu mendapat kelulusan daripada Bahagian Perkhidmatan Operasi Pusat dan Agensi (BPOPA), JANM bagi urusan pembukaan akaun di *acquiring bank*; e. Dokumen perjanjian antara Perbendaharaan Malaysia dan *acquiring bank* mesti dibuat (selaras Pekeliling Perbendaharaan Bilangan 6 Tahun 2007);	Pemilik Sistem

f. Pemilik Sistem perlu membuat peruntukan kewangan yang mencukupi bagi membiayai caj perkhidmatan yang dikenakan oleh bank dalam memproses bayaran secara *online* (Pekeliling Perbendaharaan Bilangan 6 Tahun 2007); g. Pemilik Sistem hendaklah memastikan segala terimaan harian dipindahkan ke Akaun Terimaan Kerajaan (Akaun Bank Pejabat Perakaunan) pada keesokan harinya sebelum jam 4 petang; h. Pemilik Sistem hendaklah memastikan laporan Urusniaga harian dari bank adalah sama dengan sistem; dan i. Sistem yang dibangunkan perlu direkabentuk menggunakan fungsi *Private Key Infrastructure* (PKI).	Pembangun Sistem
8.7 Penamatan Sistem Aplikasi	
Objektif: Menerangkan prosedur yang perlu dilakukan apabila ingin menamatkan penggunaan sesuatu sistem.	
8.7.1 Penamatan Penggunaan Sistem Aplikasi	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Pemilik Sistem perlulah memaklumkan secara bertulis kepada Pengurus ICT sekiranya tidak lagi memerlukan/menggunakan sistem aplikasi; dan b. Sekiranya sesebuah sistem aplikasi tidak digunakan langsung untuk tempoh dua (2) tahun, Pengurus ICT boleh mencadangkan kepada Bahagian agar sistem aplikasi tersebut ditamatkan.	Pemilik Sistem Pengurus ICT
8.8 Portal dan Aplikasi Web	
Objektif: Menerangkan perkara-perkara yang perlu dipatuhi dalam membangunkan portal dan aplikasi web di Perbendaharaan	

8.8.1 Portal dan Aplikasi Web	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Semua maklumat yang hendak dimuatkan ke dalam Portal Perbendaharaan mestilah mendapat kelulusan Ketua Bahagian/Jabatan; b. Maklumat yang terkandung dalam Portal Perbendaharaan adalah di bawah tanggungjawab Bahagian masing-masing; dan c. Laman web/portal syarikat atau individu yang memerlukan pautan ke Portal Perbendaharaan atau sebaliknya mestilah mendapat kebenaran Ketua Jabatan.	Koordinator Web

Perkara 9 Pengurusan Pengendalian Insiden Keselamatan ICT

9.1 Menangani 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

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau disyaki hilang; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri, didedahkan atau disyaki hilang; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. Prosedur pelaporan insiden keselamatan ICT berdasarkan: a. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi”; dan b. Surat Pekeliling Am Bilangan 4 Tahun 2006 bertajuk “Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam”.	Semua

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 Insiden

Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan, prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut: a. Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; b. Menyedia pelan kontingensi dan mengaktifkan Pelan Pemulihan Bencana (DRP); c. Menyimpan jejak audit dan memelihara bahan bukti; dan d. Menyediakan tindakan pemulihan segera.	Unit Keselamatan ICT/CERTMOF

Perkara 10 Pengurusan Kesinambungan Perkhidmatan

10.1 Kesinambungan Perkhidmatan

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

10.1.1 Pelan Kesinambungan Perkhidmatan

Pelan Kesinambungan Perkhidmatan (PKP) 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 JPICT. Perkara-perkara berikut perlu diberi perhatian: a. Pelan Kesinambungan Perkhidmatan Perbendaharaan harus dibentuk dengan menggunakan pendekatan “berpasukan” di mana pasukan tersebut harus diwakili oleh semua Bahagian di Perbendaharaan; b. Penilaian kegagalan keselamatan dan kerugian dalam perkhidmatan akibat bencana harus di analisa; c. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; d. Perancangan kecemasan harus dibina dan dilaksanakan untuk memastikan proses operasi boleh dijalankan semula di dalam tempoh masa yang diperlukan. Perancangan tersebut harus diselenggara dan diamalkan untuk menjadi asas proses pengurusan yang lain; e. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam tempoh yang telah ditetapkan; f. Mendokumentasikan proses dan prosedur yang telah dipersetujui;	BCP

g. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; h. Membuat penduaan; dan i. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	

Perkara 11 Pematuhan

11.1 Pematuhan dan Keperluan Perundangan

Objektif:
Meningkatkan tahap keselamatan ICT bagi mengelak daripada pelanggaran kepada Polisi ICT Perbendaharaan.

11.1.1 Pematuhan Polisi

Setiap Pengguna di Perbendaharaan hendaklah membaca, memahami dan mematuhi Polisi ICT Perbendaharaan serta undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Setiap Pengguna hendaklah menandatangani Surat Akuan Pematuhan Polisi ICT Perbendaharaan seperti di **Lampiran 1.** Semua aset ICT di Perbendaharaan termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti Pengguna untuk mengesan penggunaan selain daripada tujuan yang telah ditetapkan.	Semua

11.1.2 Keperluan Perundangan

Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di Perbendaharaan adalah seperti di **Lampiran 5.**	Semua

11.1.3 Pelanggaran Polisi

Pelanggaran Polisi ICT Perbendaharaan akan dikenakan tindakan undang-undang dan tatatertib di bawah Akta Rahsia Rasmi 1972 dan Perintah-Perintah Am Bab D – Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib). Kemudahan ICT juga akan dilucutkan jika penggunaannya melanggar peraturan/Polisi ICT Perbendaharaan.	Semua

Lampiran 1

SURAT AKUAN PEMATUHAN
POLISI ICT PERBENDAHARAAN

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

Tandatangan : .....
Tarikh : .....

Pengesahan SBTM

.....
( )
b.p. Ketua Setiausaha Perbendaharaan

Tarikh: .....

Lampiran 2

Garis Panduan Mengenai Tatacara Memohon Kelulusan Projek ICT

1. TUJUAN

Dokumen ini adalah bagi mengemas kini dan menggantikan garis panduan tatacara memohon kelulusan projek teknologi maklumat dan komunikasi (ICT) agensi di bawah Kementerian Kewangan yang telah dikeluarkan pada 30 Disember 2009. Ini adalah selaras dengan langkah Jawatankuasa Pemandu ICT Kementerian Kewangan (JPICT MOF) dalam memperkukuhkan lagi tadbir urus Projek ICT bagi agensi-agensi di bawahnya.

2. LATAR BELAKANG

2.1 Jawatankuasa Pemandu ICT (JPICT) Kementerian Kewangan merupakan sebuah jawatankuasa yang ditubuhkan untuk menimbang dan meluluskan permohonan kelulusan teknikal projek ICT daripada agensi-agensi Kementerian Kewangan bagi perolehan sistem, rangkaian, perkakasan dan perisian ICT.

2.2 Kelulusan Ketua Setiausaha Perbendaharaan (KSP) telah diperolehi bagi JPICT Kementerian Kewangan untuk menilai permohonan projek-projek ICT yang menggunakan peruntukan kerajaan persekutuan bagi agensi-agensi seperti berikut:

a) Perbendaharaan Malaysia
b) Jabatan Kastam DiRaja Malaysia – JKDM
c) Jabatan Akauntan Negara Malaysia – JANM
d) Lembaga Hasil Dalam Negeri Malaysia – LHDNM
e) Jabatan Penilaian dan Perkhidmatan Harta – JPPH
f) Lembaga Pembangunan Langkawi – LADA
g) Lembaga Perkhidmatan Kewangan Labuan - LFSA
h) Perbadanan Kemajuan Negeri.

2.3 Projek-projek ICT yang dikemukakan untuk pertimbangan dan kelulusan jawatankuasa ini mestilah telah mempunyai peruntukan.

2.4 Semua permohonan hendaklah mendapat kelulusan JPICT di peringkat agensi terlebih dahulu sebelum dikemukakan kepada JPICT Kementerian Kewangan.

2.5 Permohonan projek ICT yang telah diluluskan melalui jawatankuasa ini seterusnya akan dikemukakan ke Jawatankuasa Teknikal ICT (JTICT) yang bertempat di MAMPU.

3. KEAHLIAN JAWATANKUASA PEMANDU ICT (JPICT)

3.1 Keahlian JPICT adalah seperti berikut:

Pengerusi: TKSP(P)

Timbalan Pengerusi : SBTM

Ahli-ahli:
(a) Ahli Jawatankuasa yang dilantik dari agensi-agensi di Kementerian Kewangan; dan
(b) Wakil dari Bahagian-Bahagian berikut:
   i. Bahagian Pengurusan Perolehan Kerajaan;
   ii. Bahagian Dasar Saraan, Wang Awam dan Khidmat Pengurusan; dan
   iii. Bahagian Pengurusan Kewangan Strategik.

Urus Setia: Bahagian Pengurusan Teknologi Maklumat

4. SKOP PROJEK ICT YANG MEMERLUKAN KELULUSAN JPICT

4.1 Skop projek ICT yang perlu mendapatkan kelulusan Jawatankuasa Pemandu ICT Kementerian Kewangan (JPICT MOF) adalah seperti berikut:

(a) Projek Baru
Projek baru bermaksud projek pengkomputeran yang melibatkan salah satu atau gabungan aktiviti-aktiviti perolehan perkakasan, perisian dan/atau perkhidmatan ICT, untuk membangunkan projek ICT agensi.

i. Perkakasan komputer yang dimaksudkan merangkumi semua jenis alat-alat input/output (contoh: pencetak dan pengimbas), pemprosesan, storan data, peralatan rangkaian dan multimedia (contoh: persidangan video (*video conferencing)*) kecuali alat-alat seperti komponen alat ganti, barang pakai habis (*consumable item*), aksesori dan perabot komputer.

ii. Perisian komputer yang dimaksudkan merangkumi semua jenis perisian sistem dan perisian aplikasi. Perisian sistem merangkumi sistem operasi, pangkalan data dan perisian bagi membangunkan sistem. Perisian aplikasi adalah sistem aplikasi yang dibangunkan ataupun pakej sedia ada (*off-the-shelf*) untuk kegunaan tertentu (contoh: Sistem Perakaunan, Sistem Personel dan Sistem Pengurusan Inventori) dan perisian yang digunakan untuk menyokong kerja-kerja harian seperti penyediaan dokumen.

iii. Perkhidmatan ICT yang dimaksudkan merangkumi semua jenis perkhidmatan teknikal yang diperoleh daripada syarikat perunding swasta, kontraktor dan syarikat-syarikat lain yang berkaitan seperti pembangunan sistem, pemasangan sistem, infrastruktur rangkaian, talian internet, *web hosting*, kemasukan data, pemindahan data, migrasi sistem, pemulihan data, langganan maklumat dalam talian dan seumpamanya.

(b) Peningkatan Sistem

Peningkatan sistem bermaksud mempertingkatkan keupayaan perkakasan, perisian, rangkaian dan/atau perkhidmatan ICT. Contoh peningkatan sistem adalah seperti peningkatan perkakasan dari segi konfigurasi dan kapasiti. Peningkatan perisian merangkumi pengemaskinian fungsi-fungsi di dalam sistem ICT sedia ada kepada tahap yang lebih baik. Contoh peningkatan rangkaian adalah seperti peningkatan saiz jalur lebar (*bandwidth*), peluasan rangkaian dan seumpamanya. Peningkatan perkhidmatan pula merangkumi pertambahan skop perkhidmatan yang sedia ada.

(c) Pertambahan Peralatan

Pertambahan peralatan bermaksud menambahkan bilangan bagi mana-mana perkara di bawah kategori perkakasan, perisian dan/atau rangkaian bagi projek ICT sedia ada.

(d) Perluasan Sistem

Perluasan *(roll-out)* sistem bermaksud memperkembangkan pelaksanaan projek ICT dari lokasi sedia ada ke lokasi-lokasi lain atau dengan menambah bilangan pengguna di lokasi yang sama ataupun kedua-duanya sekali.

4.2 Skop dan had nilai projek ICT yang memerlukan kelulusan JPICT adalah seperti berikut:

(a) Bagi Permohonan Projek ICT yang MELIBATKAN pembangunan Sistem Aplikasi:

i. Bagi projek ICT yang **kurang daripada RM200,000.00** hendaklah mendapat kelulusan daripada JPICT di peringkat agensi sahaja;

ii. SEMUA projek ICT **melebihi RM200,000.00 sehingga RM500,000.00** dan telah diluluskan oleh JPICT Agensi hendaklah mendapat kelulusan teknikal daripada JPICT MOF; dan

iii. Hanya projek ICT yang bernilai **lebih daripada RM500,000.00** dan telah diluluskan oleh JPICT MOF akan dikemukakan untuk kelulusan teknikal JTICT MAMPU.

(b) Bagi Permohonan Projek ICT yang TIDAK MELIBATKAN pembangunan Sistem Aplikasi:

i. Bagi projek ICT yang **kurang daripada RM500,000.00** hendaklah mendapat kelulusan daripada JPICT di peringkat agensi sahaja;

ii. SEMUA projek ICT **melebihi RM500,000.00 hingga RM 3 juta** dan telah diluluskan oleh JPICT Agensi hendaklah mendapat kelulusan teknikal daripada JPICT MOF; dan

iii. Hanya projek ICT yang bernilai **lebih daripada RM 3 juta** dan telah diluluskan oleh JPICT MOF akan dikemukakan untuk kelulusan teknikal JTICT MAMPU.

4.3 Projek-projek ICT yang hendak dikemukakan kepada JPICT MOF perlu mendapat kelulusan daripada JPICT agensi terlebih dahulu.

4.4 Semua perolehan ICT yang telah diluluskan di peringkat JPICT dan memerlukan kelulusan teknikal JTICT di MAMPU hendaklah dikemukakan melalui Urus setia JPICT.

4.5 Semua perolehan ICT sewajarnya berdasarkan kepada Pelan Strategik ICT (ISP). JPICT akan memberi keutamaan kepada projek ICT yang telah dirancang di dalam ISP.

4.6 Untuk projek-projek yang diluluskan oleh JPICT, agensi-agensi yang memohon perlu mengemukakan laporan kemajuan kepada Urus setia JPICT setiap enam (6) bulan daripada tarikh kelulusan sehingga projek selesai.

4.7 Tempoh sah laku kelulusan JPICT adalah selama tiga (3) tahun dari tarikh surat kelulusan. Sekiranya projek yang diluluskan tidak dilaksanakan dalam tempoh tersebut, agensi hendaklah memohon semula kelulusan JPICT sebelum melaksanakan projek ICT tersebut.

4.8 Semua agensi hendaklah mematuhi garis panduan yang dikemukakan di dalam memohon kelulusan teknikal perolehan ICT daripada JPICT.

Sebarang pertanyaan lanjut mengenai permohonan projek ICT boleh menghubungi terus Urus setia JPICT MOF melalui e-mel jpictmof@treasury.gov.my.

Lampiran 3

Carta Organisasi Agensi-Agensi yang Memohon Kelulusan Projek ICT

Lampiran 4

Garis Panduan untuk Pembangunan Sistem Aplikasi dan Pangkalan Data

1. Bahagian (pengguna utama) hendaklah memperuntukkan seorang atau lebih kakitangan sebagai wakil tetap yang dapat meluangkan masa yang cukup sepanjang proses pembangunan dan kerja-kerja berkaitan dengan projek.

2. Bagi aplikasi yang besar (projek pengkomputeran Bahagian), Jawatankuasa Teknikal dan Jawatankuasa Pemandu di peringkat Bahagian perlu diwujudkan.

3. Bagi sistem aplikasi yang melibatkan pelbagai Bahagian, maka setiap Bahagian perlu mempunyai wakil tetap bagi menganggotai Jawatankuasa Teknikal dan Jawatankuasa Pemandu.

4. Cadangan Sistem (*System Proposal*) perlu dibentangkan kepada pengguna untuk ulasan dan persetujuan serta ditandatangani oleh pengguna.

5. Bagi sistem yang melibatkan fungsi dan prosedur tertentu, *subject matter expert* perlu dilibatkan dalam mereka bentuk kawalan yang berkaitan dengan *subject matter* (contoh: Bagi sistem yang melibatkan fungsi dan prosedur kewangan, Akauntan perlu dilibatkan dalam mereka bentuk kawalan yang berkaitan dengan perakaunan).

6. Pengujian dan prosedur penerimaan sistem di setiap peringkat (*unit test, component test* dan *integration test*) perlu dibuat.

7. Pengguna perlu menandatangani Penerimaan Sementara dan Penerimaan Akhir sistem aplikasi.

8. Pelaksanaan kawalan keselamatan ICT dalam aplikasi adalah perlu bagi menghalang capaian yang tidak sah, ubahsuaian, penyebaran maklumat dan kerosakan maklumat.

9. *Source code* dan hak cipta bagi sesuatu aplikasi yang dibangunkan secara dalaman ataupun secara bersama dengan pembekal perlu dinyatakan dalam kontrak sebagai Hak Kerajaan Malaysia.

10. Bagi aplikasi yang dibangunkan oleh pembekal, klausa mengenai pemindahan teknologi *(Transfer of Technology)* hendaklah dinyatakan dalam dokumen kontrak.

11. SUB setiap Bahagian yang terlibat akan mempengerusikan mesyuarat kemajuan projek bagi tujuan pemantauan.

Lampiran 5

Senarai Perundangan dan Peraturan

1. Arahan Keselamatan;
2. Perintah-Perintah Am;
3. Arahan Perbendaharaan;
4. Garis Panduan ICT Perbendaharaan;
5. Prosedur/*Standard Operating Procedure* (SOP) ICT Perbendaharaan;
6. Akta Rahsia Rasmi 1972;
7. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
8. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
9. Akta Tanda Tangan Digital 1997;
10. Akta Jenayah Komputer 1997;
11. Akta Hak Cipta (Pindaan) Tahun 1997;
12. Akta Komunikasi dan Multimedia 1998;
13. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”;
14. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
15. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS);
16. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
17. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”;
18. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
19. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden

Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

20. 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;

21. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam;

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

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

24. Arahan Teknologi Maklumat 2007;

25. Akta Aktiviti Kerajaan Elektronik 2007;

26. *Open Source Software (OSS) Implementation Guidelines August 2008*;

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

28. *The Malaysian Government Interoperability Framework for Open Source Software* (MyGIFOSS);

29. *Malaysian Personal Data Protection Act (MPDPA) 2010;* dan

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

GLOSARI	
Aset	Harta benda kepunyaan atau milikan atau di bawah kawalan Kerajaan yang dibeli atau yang disewa beli dengan wang Kerajaan, yang diterima melalui sumbangan atau hadiah atau diperoleh melalui proses perundangan
Aset ICT	Termasuk tetapi tidak terhad kepada sistem komputer peribadi, terminal, alat-alat periferal komputer, peralatan komunikasi, rangkaian komunikasi, perisian komputer, dokumentasi bantuan, peralatan storan, kemudahan sokongan dan sumber tenaga. Kemudahan terhad kepada kemudahan yang dibeli, disewa, dipajak, dimiliki atau dipinjamkan kepada Perbendaharaan. Ia termasuk semua kemudahan, maklumat dan sistem aplikasi
Bahagian	Bahagian, Seksyen dan Unit di Perbendaharaan
BPTM	Bahagian Pengurusan Teknologi Maklumat termasuk Seksyen Teknologi Maklumat BPP, Unit e-Perolehan dan Unit IT Perbendaharaan Sabah dan Sarawak
BCP	Bahagian Perancangan Korporat
CERTMOF	Pasukan Tindak Balas Insiden Keselamatan ICT Kementerian Kewangan
CIO	Timbalan KSP (Pengurusan) adalah merupakan Ketua Pegawai Maklumat (CIO). Ketua Pegawai Maklumat adalah bertanggungjawab ke atas perancangan, pengurusan, penyelarasan dan pemantauan program ICT di Perbendaharaan
GCERT	Pasukan Tindak balas Insiden Keselamatan ICT Kerajaan *(Government Computer Emergency Response Team)*
Hapus Kira	Satu proses untuk membatalkan rekod aset yang hilang
ICT	Teknologi Maklumat dan Komunikasi
ICTSO	Pegawai Keselamatan ICT yang bertanggungjawab ke atas keselamatan ICT di Perbendaharaan. ICTSO yang bertanggungjawab ke atas agensi masing-masing adalah: a. Timbalan Setiausaha Bahagian Teknologi Maklumat (Operasi), TSBTM(O) Perbendaharaan. b. Ketua Penolong Seksyen Teknologi Maklumat

	(KPS(TM) 2) Bahagian Pinjaman Perumahan. c. Timbalan Pengarah Unit e-Perolehan.
IP	*Internet Protocol*
JPICT	Jawatankuasa Pemandu ICT di Kementerian Kewangan (JPICT MOF)
Kehilangan	Aset yang tiada lagi dalam simpanan disebabkan oleh kecurian, kemalangan, kebakaran, bencana alam, kesusutan, penipuan atau kecuaian pegawai awam
Komputer Server	Komputer yang mempunyai keupayaan tinggi yang memberi perkhidmatan berpusat
Koordinator ICT Bahagian	Penyelaras atau pegawai yang bertanggungjawab ke atas segala urusan ICT di Bahagian
Koordinator Web Bahagian	Pegawai yang dilantik dari setiap bahagian dan bertanggungjawab menyemak, memantau dan mengemaskini maklumat Bahagian masing-masing di Portal Perbendaharaan
KSP	Ketua Setiausaha Perbendaharaan
Mobile Code	Merupakan program, aplikasi atau *content* yang berupaya dipindahkan melalui *embedded email*, dokumen atau *website*. Ia juga boleh dipindahkan melalui rangkaian dan media storan seperti *Universal Serial Bus* (USB) *flash drive*. *Mobile Code* mampu bertindak *(run/execute)* tanpa sebarang proses instalasi dari pengguna komputer tersebut dan seringkali pengguna tidak menyedari bahawa perisian tersebut telah dimuat turun dan telah *running/executed* di dalam komputer mereka. Contoh *mobile code* adalah *scripts* (JavaScript, VBScript), Java applets, ActiveX controls, Flash animations, Shockwave movies (dan Xtras), serta macros yang dibenamkan di dalam Microsoft Office.
Pasukan Portal	Pasukan yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara portal
Pegawai Aset Bahagian	Pegawai penyelaras yang bertanggungjawab ke atas segala aset di Bahagian

Pelupusan	Satu proses untuk mengeluarkan aset daripada milikan, kawalan, simpanan dan rekod mengikut kaedah yang ditetapkan
Pembangun Sistem	Pegawai yang bertanggungjawab membangunkan sistem aplikasi
Pemilik Sistem	Bahagian/Seksyen/Unit yang memiliki data dan merupakan pengguna utama sesuatu sistem
Pengguna	Warga Perbendaharaan yang dibenarkan menggunakan kemudahan ICT Perbendaharaan
Pengurus ICT	Pengurus ICT yang bertanggungjawab ke atas agensi masing-masing adalah: a. Setiausaha Bahagian Pengurusan Teknologi Maklumat (SBTM) Perbendaharaan. b. Ketua Seksyen Teknologi Maklumat (KS(TM)) Bahagian Pinjaman Perumahan. c. Ketua Penolong Pengarah (KPP(TO)) Unit e-Perolehan.
Pengurus Pusat Data/ DRC	Pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara Pusat Data/Pusat Pemulihan Bencana (DRC)
Pentadbir Pangkalan Data	Pegawai yang bertanggungjawab mengurus, mengawal, memantau, menyelenggara operasi dan keselamatan pangkalan data
Pentadbir Rangkaian	Pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara keselamatan rangkaian
Pentadbir Sistem Aplikasi	Pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara sistem aplikasi
Pentadbir Sistem ICT	Pegawai yang bertanggungjawab mengurus, mengawal, memantau, menyelenggara operasi dan keselamatan pelayan serta data yang disimpan
Penyelenggara Bangunan	Pegawai atau pembekal dilantik yang bertanggungjawab untuk menyelenggara bangunan

Penyulitan	Proses untuk mengaburkan maklumat supaya tidak dapat dibaca tanpa pengetahuan khusus *(encryption)*
Peralatan Mudah Alih	Semua peralatan ICT mudah alih (*mobile*) termasuk komputer peribadi (PC), *Notebook, Netbook, Tablet PC* dan seumpamanya
Peralatan Rangkaian	Peralatan dan komponen yang digunakan dalam sistem rangkaian seperti *switch, hub, router* dan sebagainya
Perbendaharaan	Perbendaharaan Malaysia, Bahagian Pinjaman Perumahan (BPP), Unit ePerolehan, Perbendaharaan Malaysia Sabah dan Perbendaharaan Malaysia Sarawak
Perkakasan	Peralatan dan komponen ICT seperti komputer*, notebook*, pencetak dan sebagainya
Pihak Ketiga	Pembekal, pakar runding, pelawat dan pihak-pihak luar lain yang dibenarkan menggunakan kemudahan ICT Perbendaharaan - Pembekal : Seseorang atau kumpulan orang yang dibenarkan membekal sama ada perkhidmatan atau barangan ICT di Perbendaharaan - Pakar Runding : Seseorang atau kumpulan orang yang dipilih untuk memberi perkhidmatan dalam bentuk khidmat nasihat ICT di Perbendaharaan
Soft Cert	Sijil Digital
SUB	Setiausaha Bahagian
TKSP	Timbalan Ketua Setiausaha Perbendaharaan
TSUB	Timbalan Setiausaha Bahagian
Tugas-tugas Dalaman	Tugas-tugas yang menyokong fungsi-fungsi Perbendaharaan
Unit Keselamatan ICT	Unit yang mengurus dan mengendalikan hal-hal keselamatan ICT Perbendaharaan
Warga Perbendaharaan	Seseorang yang dilantik untuk sesuatu jawatan sama ada secara tetap, sambilan, sementara atau kontrak yang berkhidmat di Perbendaharaan

JADUAL PINDAAN POLISI ICT PERBENDAHARAAN

Bil	Perkara	Butiran Pindaan
1	**Penyataan Polisi**	Penambahan Penyataan Polisi, muka surat 1
2	**Skop**	Pengemaskinian skop, muka surat 2
3	**Prinsip-prinsip**	Pengemaskinian prinsip-prinsip, muka surat 4
4	**Penilaian Risiko Keselamatan ICT**	Penambahan Penilaian Risiko Keselamatan ICT, muka surat 10
5	**Perkara 1 – Pembangunan dan Penyelenggaraan Polisi** 1.1.2 Penyebaran Polisi	Penukaran peranan kepada Pengurus ICT, muka surat 6
6	**Perkara 1 – Pembangunan dan Penyelenggaraan Polisi** 1.1.3 Penyelenggaraan Polisi	Penukaran peranan kepada Pengurus ICT, muka surat 8
7	**Perkara 2 – Organisasi ICT** 2.1.4 Pegawai Keselamatan ICT	Menerangkan maklumat ICTSO dengan lebih terperinci, muka surat 10
8	**Perkara 2 – Organisasi ICT** 2.1.5 Jawatankuasa Pemandu ICT Kementerian Kewangan (JPICT MOF)	i. Menyenaraikan keahlian agensi yang perlu mendapat kelulusan projek ICT melalui JPICT MOF. ii. Membuat pindaan agar carta organisasi JPICT MOF diletakkan di lampiran. Pindaan tersebut di muka surat 11
9	**Perkara 2 – Organisasi ICT** 2.1.6 Pasukan Tindakan Insiden Keselamatan ICT Keselamatan Kementerian Kewangan (CERTMOF)	Menyenaraikan nama agensi yang terlibat di dalam CERTMOF, muka surat 13.
10	**Perkara 2 - Organisasi ICT** 2.1.7 Pengurus Pusat Data dan DRC	i. Penambahan DRC ke dalam tajuk dan klausa berkenaan ii. Pembetulan ejaan bagi ‘menganalisis’ kepada ‘menganalisa’. Pindaan tersebut di muka surat 13
11	**Perkara 2 – Organisasi ICT** 2.1.8 Pentadbir Sistem ICT	i. Menerangkan maklumat Pentadbir Sistem ICT dengan lebih terperinci ii. Pembetulan ejaan bagi ‘menganalisis’ kepada ‘menganalisa’ Pindaan tersebut di muka surat 14
12	**Perkara 2 – Organisasi ICT** 2.1.11 Pentadbir Sistem Aplikasi	Mengemas kini perkara 2.1.11 Pentadbir Sistem Aplikasi, muka surat 16
13	**Perkara 2 – Organisasi ICT** 2.1.12 Koordinator ICT Bahagian	Menerangkan maklumat Koordinator ICT dengan lebih terperinci, muka surat 16
14	**Perkara 2 – Organisasi ICT** 2.1.13 Koordinator Web Bahagian	Menerangkan maklumat Koordinator Web dengan lebih terperinci, muka surat 18

15	**Perkara 2 – Organisasi ICT** 2.1.14 Pengguna	i. Mengemas kini peranan pengguna seperti yang tertera di Polisi ICT ii. Memperbaiki perkara 2.1.14 item (b) dari 'Menjalani tapisan keselamatan atau yang setaraf dengannya sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat' kepada 'Lulus tapisan keselamatan atau yang setaraf dengannya'. Pindaan tersebut di muka surat 19
16	**Perkara 2 – Organisasi ICT** 2.2.1 Pembekal, Pakar Runding, Pelawat dan Pihak-Pihak Luar Lain	Mengemas kini peranan di perkara 2.2.1 Pembekal, Pakar Runding, Pelawat dan Pihak-Pihak Luar Lain, muka surat 20
17	**Perkara 3 – Pengurusan Aset** 3.2.1 PC, Komputer Riba, Projektor LCD dan Peralatan Mudah Alih	Mengemas kini peranan di perkara 3.2.1 PC, Komputer Riba, Projektor LCD dan Peralatan Mudah Alih, muka surat 21
18	**Perkara 3 – Pengurusan Aset** 3.2.2 Pencetak	Mengemas kini peranan di perkara 3.2.2 Pencetak, muka surat 21
19	**Perkara 3 – Pengurusan Aset** 3.4.2 Pengendalian Maklumat	Menambah klausa baru 'Melakukan penyulitan *(encryption)* bagi maklumat terperingkat sebelum transmisi; dan' di perkara 3.4.2 item (e), muka surat 23
20	**Perkara 4 – Keselamatan Sumber Manusia** 4.1 Keselamatan Sumber Manusia Dalam Tugas Harian	Mengemas kini perkara 4.1.1 dan tambahan perkara 4.1.2 dan 4.1.3 seperti berikut: 4.2.1 Sebelum Memulakan Perkhidmatan 4.1.2 Dalam Perkhidmatan 4.1.3 Bertukar Atau Tamat Perkhidmatan Pindaan tersebut di muka surat 24-25
21	**Perkara 5 – Keselamatan Fizikal dan Persekitaran** 5.1.1 Kawasan Larangan	i. Mengemas kini klausa di perkara 5.1.1 Kawasan Larangan ii. Penambahan DRC ke dalam klausa berkenaan Pindaan tersebut di muka surat 27
22	**Perkara 5 – Keselamatan Fizikal dan Persekitaran** 5.2.2 Media Storan	i. Mengemas kini perkara 5.2.2 item (a) dari 'yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat' kepada 'yang sesuai dan mempunyai ciri-ciri keselamatan berpadanan dengan

		kandungan maklumat'. ii. Menambah perkara 5.2.2 item (d) – (f) Pindaan tersebut di muka surat 28-29
23	**Perkara 5 – Keselamatan Fizikal dan Persekitaran** 5.2.4 Media Perisian dan Aplikasi	Memperbaiki perkara 5.2.4 item (g) dari 'penyulitan *(encryption)* yang dibenarkan oleh BPTM.' kepada 'penyulitan *(encryption)* yang disyorkan oleh BPTM.', muka surat 29
24	**Perkara 5 – Keselamatan Fizikal dan Persekitaran** 5.2.5 Penyelenggaraan Perkakasan	i. Menambah perkara 5.2.5 item (c) Penyelenggaraan Perkakasan ii. Pengemaskinian talian hotline Pindaan tersebut di muka surat 30-31
25	**Perkara 5 – Keselamatan Fizikal dan Persekitaran** 5.2.6 Peralatan di Luar Premis	Menambah perkara 5.2.6 item (a) Peralatan di Luar Premis, muka surat 31
26	**Perkara 5 – Keselamatan Fizikal dan Persekitaran** 5.2.7 Pelupusan Perkakasan	i. Mengemas kini klausa di perkara 5.2.7 item (a) dari '*degauzing* atau pembakaran' kepada '*degaussing, electronic data erasure* atau pembakaran' ii. Mengemas kini klausa di perkara 5.2.7 item (c) dari 'Maklumat lanjut pelupusan adalah merujuk kepada' kepada 'Pelupusan adalah tertakluk kepada' Pindaan tersebut di muka surat 31
27	**Perkara 6 – Pengurusan Operasi dan Komunikasi** 6.1 Pengurusan Prosedur Operasi	Mengemas kini klausa di perkara 6.1 dari 'Memastikan pengurusan operasi berfungsi dengan betul dan selamat' kepada 'Memastikan operasi ICT berfungsi dengan lancar dan efisien serta selamat', muka surat 36
28	**Perkara 6 – Pengurusan Operasi dan Komunikasi** 6.1.1 Pengendalian Prosedur	Mengemas kini klausa di perkara 6.1.1 item (a) dan (b), muka surat 36
29	**Perkara 6 – Pengurusan Operasi dan Komunikasi** 6.2.1 Perancangan Kapasiti	Menukar peranan bagi perkara 6.2.1 Perancangan Kapasiti, muka surat 37
30	**Perkara 6 – Pengurusan Operasi dan Komunikasi** 6.2.2 Penerimaan Sistem Aplikasi	Menambah klausa di perkara 6.2.2 bagi item (b) dan (c), muka surat 37
31	**Perkara 6 – Pengurusan Operasi dan Komunikasi** 6.2.3 Penerimaan Perkakasan dan Perisian Sistem Baru	Menambah klausa di perkara 6.2.3 bagi item (b) dan (c), muka surat 38

32	**Perkara 6 - Pengurusan Operasi Dan Komunikasi** 6.3.2 Perlindungan Dari *Mobile Code*	Menambah perkara baru 6.3.2 Perlindungan dari Mobile Code, muka surat 39
33	**Perkara 6 – Pengurusan Operasi dan Komunikasi** 6.5.1 Kawalan Infrastruktur Rangkaian	Menambah klausa di perkara 6.5.1 bagi item (g) - (j), muka surat 40
34	**Perkara 6 – Pengurusan Operasi dan Komunikasi** 6.8.1 Pengauditan dan Forensik ICT	Menambah tajuk baru 6.8.1 Pengauditan dan Forensik ICT, muka surat 45
35	**Perkara 6 – Pengurusan Operasi dan Komunikasi** 6.8.2 Jejak Audit	i. Mengemas kini klausa 6.8.2 Jejak Audit ii. Penambahan peranan Pentadbir Sistem Aplikasi bagi perkara berkenaan Pindaan tersebut di muka surat 45-46
36	**Perkara 6 – Pengurusan Operasi dan Komunikasi** 6.8.4 Pemantauan Log	Menambah perkara baru 6.8.4 Pemantauan Log, muka surat 47
37	**Perkara 7 – Kawalan Capaian** 7.1.1 Keperluan Kawalan Capaian	Mengemas kini klausa di perkara 7.1.1 dari 'Capaian kepada proses dan ...' kepada 'Capaian kepada sistem dan ...', muka surat 48
38	**Perkara 7 – Kawalan Capaian** 7.2.1 ID Pengguna	Menukar tajuk bagi 7.2.1 dari 'Akaun Pengguna' kepada 'ID Pengguna', muka surat 48
39	**Perkara 7 – Kawalan Capaian** 7.3.3 Pengurusan Alamat IP	i. Menambah klausa bagi perkara 7.3.3 item (c) ii. Penukaran klausa daripada 'menukar atau meletakkan IP' kepada 'menukar konfigurasi IP' Pindaan tersebut di muka surat 51-52
40	**Perkara 7 – Kawalan Capaian** 7.3.4 Talian Internet Persendirian	Mengemas kini klausa bagi perkara 7.3.4 item (b) dari '... sambungan ke rangkaian Perbendaharaan terlebih dahulu' kepada '... sambungan ke rangkaian Perbendaharaan terlebih dahulu sebelum menggunakan talian internet persendirian', muka surat 52
41	**Perkara 7 – Kawalan Capaian** 7.3.5 Antivirus	Mengemas kini klausa di perkara 7.3.5 item (a) dari '... perkakasan seperti PC yang bersambung ...' kepada '... perkakasan seperti PC dan komputer riba yang bersambung ...', muka surat 52

42	**Perkara 7 – Kawalan Capaian** 7.4.2 Melayari Internet	Mengemas kini klausa di perkara 7.4.2 item (c) dari '...yang mengandungi maklumat melalui...' kepada '...yang mengandungi maklumat terperingkat (sulit atau terhad) melalui ...' Menambah klausa di perkara 7.4.2 item (l), muka surat 54
43	**Perkara 7 – Kawalan Capaian** 7.5 Kawalan Capaian Sistem Pengoperasian	Menambah tajuk baru 7.5 Kawalan Capaian Sistem Pengoperasian selepas Keselamatan Internet, muka surat 55
44	**Perkara 7 – Kawalan Capaian** 7.6.1 Sistem Maklumat dan Aplikasi	Mengubah peranan di perkara 7.6.1 Sistem Maklumat dan Aplikasi, muka surat 57
45	**Perkara 7 – Kawalan Capaian** 7.7.1 Penggunaan Peralatan Mudah Alih	Menambah klausa di perkara 7.7.1 item (a) iaitu 'Merekodkan aktiviti keluar masuk peralatan komputer mudah alih gunasama bagi memantau pergerakan peralatan tersebut; dan', muka surat 58
46	**Perkara 7 - Kawalan Capaian** 7.7.2 Kerja Jarak Jauh	i. Menambah tajuk baru 7.7.2 Kerja Jarak Jauh selepas tajuk Penggunaan Peralatan Mudah Alih ii. 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 Pindaan tersebut di muka surat 58
47	**Perkara 8 – Perolehan, Pembangunan dan Penyelenggaraan Sistem** 8.1.1 Keselamatan Aplikasi	Beberapa perubahan iaitu: i. Perubahan peranan. ii. Mengemas kini klausa item (c) dari '... Penilaian Kerentanan *(Vulnerability Assessment) ...*' kepada '... Penilaian Keterdedahan *(Vulnerability Assessment)* ...' iii. Mengemas kini klausa item (d) dari 'Bahagian perlu mengenalpasti...' kepada 'Pemilik Sistem perlu mengenalpasti...' Pindaan tersebut di muka surat 59
48	**Perkara 8 – Perolehan, Pembangunan dan Penyelenggaraan Sistem** 8.2.1 Penyulitan	Mengemas kini klausa di perkara 8.2.1 dari '...maklumat rahsia rasmi ...' kepada '...maklumat terperingkat (sulit atau terhad)...', muka surat 60

49	**Perkara 8 – Perolehan, Pembangunan dan Penyelenggaraan Sistem** 8.2.2 Tandatangan Digital	Mengemas kini klausa di perkara 8.2.2 dari '...transaksi maklumat secara elektronik.' kepada '...transaksi maklumat terperingkat (sulit atau terhad) secara elektronik.', muka surat 60
50	**Perkara 8 – Perolehan, Pembangunan dan Penyelenggaraan Sistem** 8.3.1 Pembangunan Sistem Aplikasi	Mengemas kini perkara 8.3.1 item (g) dan (k), muka surat 61
51	**Perkara 8 - Perolehan, Pembangunan Dan Penyelenggaraan Sistem** 8.4.1 Kawalan Fail Sistem	Menambah klausa di perkara 8.4.1 bagi item (e), muka surat 62
52	**Lampiran 3**	Menyertakan Carta Organisasi Agensi-Agensi yang Memohon Kelulusan Projek ICT, muka surat 76
53	**Lampiran 4**	Mesyuarat mencadangkan agar Garis Panduan yang dilampirkan akan dikeluarkan setelah Garis Panduan ICT Perbendaharaan diwujudkan. (Garis Panduan ICT Perbendaharaan merangkumi semua garis panduan berkaitan ICT yang baru dan sedia ada), muka surat 77.
54	**Lampiran 5**	Penambahan beberapa item dalam Senarai Perundangan dan Peraturan seperti berikut: i. *Open Source Software (OSS) Implementation Guidelines August 2008* ii. *The Malaysian Government Interoperability Framework for Open Source Software* (MyGIFOSS) iii. *Malaysian Personal Data Protection Act (MPDPA) 2010* Pindaan tersebut di muka surat 78-79
55	**Glosari**	i. Penambahan glosari bagi BPTM ii. Penambahan glosari bagi *Mobile Code* iii. Mengubah deskripsi Pengguna iv. Menambah deskripsi bagi Pentadbir Sistem Aplikasi dan Pentadbir Rangkaian v. *Soft Cert* vi. SUB Pindaan tersebut di muka surat 80-83