SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUAT KUASA
21 Oktober 2022	6.0	Mesyuarat Jawatankuasa ISMS Bil 1/2022	1 November 2022
8 Disember 2021	5.0	Mesyuarat Jawatankuasa Perkhidmatan dan Teknologi Maklumat Bil 6/2021	13 Disember 2021
18 November 2020	4.0	Pengurusan Tertinggi Yang DiPertua MPKj	1 Disember 2020
16 Julai 2020	3.0	Mesyuarat Jawatankuasa Perkhidmatan dan Teknologi Maklumat Bil 4/2020	20 Julai 2020
22 Mei 2018	2.0	Mesyuarat Jawatankuasa ISMS Bil 1/2018	15 Jun 2018
15 Disember 2016	1.4	Mesyuarat Kajian Semula Pengurusan ISMS MPKj Bil 2/2016	16 Disember 2016
24 Oktober 2016	1.3	Mesyuarat Pengurusan Majlis Perbandaran Kajang	25 Oktober 2016
21 April 2014	1.2	Mesyuarat Jawatankuasa Perkhidmatan dan Teknologi Maklumat	30 April 2014
1 Mac 2011	1.1	Mesyuarat Jawatankuasa Perkhidmatan dan Teknologi Maklumat	19 April 2011
4 Februari 2009	1.0	Pengurusan Tertinggi Timbalan Yang DiPertua MPKj	1 Julai 2009

JADUAL PINDAAN DASAR KESELAMATAN ICT MAJLIS PERBANDARANKAJANG

BIL	TARIKH KELULUSAN	TAJUK PINDAAN	PERKARA	PINDAAN
1.	**21 Oktober 2022**	**Bidang 02 Organisasi Keselamatan**	**020103 Pegawai Keselamatan ICT (ICTSO)**	**Pindaan item:** Pindaan Pegawai Teknologi Maklumat MPKj kepada Timbalan Pengarah Teknologi Maklumat MPKj h. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MPKj berdasarkan hasil penemuan dan menyediakan laporan mengenainya
			020106 Pengurus ICT	**Tambahan item:** **020106 Pengurus ICT** Pengurus ICT bagi MPKj adalah Timbalan Pengarah Teknologi Maklumat. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut a. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MPKj;

BIL	TARIKH KELULUSAN	TAJUK PINDAAN	PERKARA	PINDAAN
	21 Oktober 2022	**Bidang 02 Organisasi Keselamatan**		b. Menentukan kawalan akses pengguna terhadap aset ICT MPKj; c. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan d. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MPKj. **<u>Peranan</u>** Pengurus ICT
	21 Oktober 2022	**Bidang 02 Organisasi Keselamatan**	**020104 Pentadbir Sistem Aplikasi** **(PINDAAN PERANAN)**	**<u>Pindaan item:</u>** **020104 Pentadbir Sistem Aplikasi (PINDAAN PERANAN)** Pentadbir Sistem Aplikasi MPKj adalah Pegawai Teknologi Maklumat dan Penolong Pegawai Teknologi Maklumat MPKj b. Memastikan ketepatan dan

BIL	TARIKH KELULUSAN	TAJUK PINDAAN	PERKARA	PINDAAN
				menyekat kebenaran capaian serta-merta apabila tidak lagi diperlukan atau melanggar Dasar Keselamatan ICT MPKj **Peranan** Pegawai Teknologi Maklumat/ Penolong Pegawai Teknologi Maklumat / Juruteknik
	21 Oktober 2022	**Bidang 02 Organisasi Keselamatan**	**020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga**	**Tambahan item:** **Peranan** Penolong Pegawai Teknologi Maklumat, Pentadbir Sistem Aplikasi
2.	**21 Oktober 2022**	**Bidang 05 Keselamatan Fizikal Dan Persekitaran**	**050201 Peralatan ICT**	**Pindaan item:** Peralatan ICT yang hendak dibawa keluar dari premis MPKj, perlulah mendapat kelulusan ICTSO / Penolong Pegawai Teknologi Maklumat / Juruteknik dan direkodkan bagi tujuan pemantauan;
3.	**21 Oktober 2022**	**Bidang 06 Pengurusan Operasi Dan Komunikasi**	**060103 Pengasingan Tugas dan Tanggungjawab**	**Tambahan item:** **Peranan** Pegawai Teknologi Maklumat
			060302 Penerimaan Sistem	**Tambahan item:** **Peranan** Pegawai Teknologi Maklumat

BIL	TARIKH KELULUSAN	TAJUK PINDAAN	PERKARA	PINDAAN
			060501 *Backup*	**Pindaan item:** a. Membuat *backup* ke atas semua data kritikal dalam **Sistem Aplikasi** mengikut keperluan organisasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat;
			060601 Kawalan Infrastruktur Rangkaian	**Pindaan item:** f. Memasang ***Internet Access Management*** pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;
			061002 Jejak Audit	**Tambahan item:** **Peranan** Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat, ICTSO
4.	**21 Oktober 2022**	**Bidang 07** **Kawalan Capaian**	**070101 Keperluan Kawalan Capaian**	**Tambahan item:** **Peranan** Pegawai Teknologi Maklumat
			070202 Hak Capaian	**Tambahan item:** **Peranan** Pegawai Teknologi Maklumat
			070204 *Clear Desk* dan *Clear Screen*	**Pindaan item:** a. Menggunakan kemudahan *Password Screen Saver* **bermula dari 10 minit hingga 15 minit selepas meninggalkan komputer;**

BIL	TARIKH KELULUSAN	TAJUK PINDAAN	PERKARA	PINDAAN
			070501 Capaian Aplikasi dan Maklumat	**Tambahan item:** **Peranan** Pegawai Teknologi Maklumat
			070602 Kerja Jarak Jauh	**Pindaan item:** b. Tertakluk kepada pekeliling semasa **(Lampiran 2 : Senarai Perundangan dan Peraturan)**
5.	**21 Oktober 2022**	**Bidang 08** **Perolehan, Pembangunan Dan Penyelenggaraan Sistem**	**080101 Keperluan Keselamatan Sistem Maklumat**	**Tambahan item:** **Peranan** Pegawai Teknologi Maklumat
			080301 Kawalan Fail Sistem	**Tambahan item:** **Peranan** Pegawai Teknologi Maklumat
			080401 Prosedur Kawalan Perubahan	**Tambahan item:** **Peranan** Pegawai Teknologi Maklumat
			080402 Pembangunan Perisian Secara *Outsource*	**Tambahan item:** **Peranan** Pegawai Teknologi Maklumat
			080501 Kawalan dari Ancaman Teknikal	**Tambahan item:** **Peranan** Pegawai Teknologi Maklumat
6.	**21 Oktober 2022**	**Bidang 09** **Pengurusan Pengendalian Insiden Keselamatan**	**090101 Mekanisme Pelaporan**	**Pindaan item:** Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT

BIL	TARIKH KELULUSAN	TAJUK PINDAAN	PERKARA	PINDAAN
				atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan **NACSA (*National Cyber Security Agency*)** dengan kadar segera

ISI KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT mengandungi peraturan-peraturan yang perlu dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) Majlis Perbandaran Kajang (MPKj). Dasar ini juga menerangkan kepada semua pengguna di MPKj mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT MPKj.

OBJEKTIF

Dasar Keselamatan ICT MPKj diwujudkan untuk memastikan tahap keselamatan ICT MPKj terurus dan dilindungi bagi menjamin kesinambungan urusan MPKj dengan meminimumkan kesan insiden keselamatan ICT.

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

Objektif utama Dasar Keselamatan ICT MPKj ialah:

a. Memastikan kelancaran operasi MPKj dan meminimumkan kerosakan atau kemusnahan;

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

c. Mencegah salah guna atau kecurian aset ICT kerajaan.

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari 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 ICTberkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

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

b. Menjamin setiap maklumat adalah tepat dan sempurna;

c. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

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

Dasar Keselamatan ICT MPKj 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. Datanya 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

Dasar ini meliputi semua sumber atau aset ICT yang digunakan seperti:

1. Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan Majlis Perbandaran Kajang (MPKj). Contoh peralatan adalah seperti komputer, pelayan, *firewall,* pencetak, peralatan media, peralatan komunikasi dan alat-alat prasarana seperti *Uninterruptible Power Supply (UPS)* dan sebagainya.

2. Perisian

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

3. 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.

4. Data dan maklumat

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

5. Manusia

Semua pengguna infrastruktur ICT MPKj yang dibenarkan, termasuk kakitangan, pengguna dan pembekal. Individu yang mempunyai pengetahuan untuk melaksanakan skop kerja harian MPKj bagi mencapai misi dan objektif jabatan. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

6. Media Storan

Semua media storan dan peralatan yang berkaitan seperti storan mudah alih, cakera padat, *thumb drive* dan lain-lain.

7. Media Komunikasi

Semua peralatan berkaitan komunikasi seperti pelayan rangkaian, *gateway, bridge, router*, peralatan PABX, *wireless* LAN, peralatan *video conferencing,* kabel rangkaian, *switches, hub* dan lain-lain.

8. Dokumentasi

Semua dokumen (prosedur dan manual pengguna) yang berkaitan dengan aset ICT, pemasangan dan pengoperasian peralatan dan perisian, sama ada dalam bentuk elektronik atau bukan elektronik.

PRINSIP-PRINSIP

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

1. 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.

2. Hak Akses Minimum

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

3. Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT MPKj.

4. 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 dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

5. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam

keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Oleh yang demikian, aset ICT seperti komputer, pelayan (*server*), *router, firewall*, IPS, Antivirus, pencetak dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*.

6. Pematuhan

Dasar Keselamatan ICT MPKj hendaklah dibaca, difahami oleh semua lapisan kakitangan dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

7. 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 (*backup*) dan pengwujudan pelan pemulihan bencana/kesinambungan perkhidmatan.

8. 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 mekanisme keselamatan ICT di MPKj adalah perlu bagi menjamin keselamatan ICT yang maksimum di MPKj.

PENILAIAN RISIKO KESELAMATAN ICT

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

MPKj 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 MPKj 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. MPKj bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis PanduanPenilaian Risiko Keselamatan Maklumat Sektor Awam.

MPKj perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a. mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

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

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

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

BIDANG 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR	
0101 Dasar Keselamatan ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan MPKj yang berkaitan	
010101 Pelaksanaan Dasar	
Tuan Yang DiPertua adalah bertanggungjawab ke atas pelaksanaan arahan yang dibantu oleh Ketua Bahagian Teknologi Maklumat dan lain-lain pegawai yang dilantik.	Yang DiPertua MPKj
010102 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna ICT MPKj (termasuk kakitangan, pembekal, pakar runding dan lain-lain pihak yang berurusan dengan MPKj).	ICTSO
010103 Penyelenggaraan Dasar	
Dasar Keselamatan ICT MPKj adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan organisasi. Prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT MPKj adalah seperti berikut: a. Mengkaji semula dasar ini sekurang-kurangnya **sekali setahun** ATAU **mengikut keperluan semasa** bagi mengenal pasti dan menentukan perubahan yang diperlukan; b. Memaklumkan perubahan yang telah dipersetujui kepada semua pengguna; dan	ICTSO

010104 Pengecualian Dasar	
Dasar Keselamatan ICT MPKj adalah terpakai kepada semua pengguna ICT MPKj tanpa sebarang pengecualian diberikan.	Pengguna ICT

BIDANG 02 ORGANISASI KESELAMATAN	
0201 Infrastruktur Organisasi Dalaman	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT MPKj	
020101 Yang DiPertua MPKj	
a. Memastikan setiap pengguna memahami peruntukan-peruntukan yang ada di bawah Dasar Keselamatan ICT MPKj; b. Memastikan semua pengguna mematuhi DasarKeselamatan ICT MPKj; c. Memastikan semua keperluan di MPKj seperti sumber kewangan dan kakitangan adalah mencukupi; d. Memastikan semua dasar yang telah ditetapkan dan dipersetujui oleh pengurusan dilaksanakan sepenuhnya di kalangan kakitangan MPKj.	Yang DiPertua MPKj
020102 Ketua Pegawai Maklumat (CIO)	
Ketua Pegawai Maklumat (CIO) bagi MPKj ialah Timbalan Yang DiPertua MPKj. Peranan dan tanggungjawab CIO adalah seperti berikut: a. Menentukan keperluan keselamatan ICT; b. Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT MPKj serta pengurusan risiko dan pengauditan; dan c. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MPKj.	CIO

020103 Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) bagi MPKj ialah Timbalan Pengarah Teknologi Maklumat MPKj. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Menentukan keperluan ICT di MPKj; b. Mengurus keseluruhan Dasar Keselamatan ICT MPKj; c. Menguatkuasakan Dasar Keselamatan ICT MPKj; d. Memberi penerangan dan pendedahan berkaitan Dasar Keselamatan ICT; e. Menjalankan pengurusan risiko; f. Menyelia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; g. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MPKj; h. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MPKj berdasarkan hasil penemuan dan menyediakan laporan mengenainya; i. Memberi amaran terhadap sebarang ancaman berbahaya seperti serangan virus dan memberi khidmat nasihat serta menyediakan langkah- langkah keselamatan; dan j. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah- langkah baik pulih dengan kadar segera.	Pegawai Keselamatan ICT (ICTSO)

020104 Penolong Pegawai Teknologi Maklumat/ Juruteknik	
a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas. (contoh: penukaran dan penghapusan kata laluan sistem yang digunakan oleh kakitangan); b. Memantau aktiviti capaian harian pengguna; c. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT MPKj; d. Memantau aktiviti capaian harian sistem aplikasi pengguna; e. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; f. Menganalisis dan menyimpan rekod jejak audit; g. Menyediakan laporan mengenai aktiviti capaian secara berkala; h. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik. i. Mengenal pasti aktiviti-aktiviti yang tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran, melayari laman-laman web yang tidak dibenarkan dan sebagainya; dan j. Menyediakan laporan mengenai aktiviti capaian secara berkala;	Penolong Pegawai Teknologi Maklumat/ Juruteknik

i. Capaian sistem mengikut permintaan pengguna ii. Capaian internet secara berkala dan mengikut permintaan pengguna.	
020105 Pengguna	
a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPKj; b. Mengetahui dan memahami implikasi keselamatan ICT dari sudut kesan dan tindakannya; c. Melaksanakan arahan-arahan Dasar Keselamatan ICT MPKj dan menjaga kerahsiaan maklumat MPKj; d. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; e. Menghadiri program-program kesedaran mengenai keselamatan ICT; f. Menandatangani surat akuan pematuhan Dasar Keselamatan ICT MPKj; g. Menghalang pendedahan maklumat kepada pihak luar atau pihak yang tidak dibenarkan; h. Menjaga kerahsiaan kata laluan dari semasa ke semasa;dan i. Memberi perhatian kepada sebarang maklumat terperingkat terutama semasa pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.	Pengguna

020106 Pengurus ICT	
Pengurus ICT bagi MPKj adalah Timbalan Pengarah Teknologi Maklumat. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MPKj; b. Menentukan kawalan akses pengguna terhadap aset ICT MPKj; c. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan d. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MPKj.	Pengurus ICT
020107 Pentadbir Sistem Aplikasi	
Pentadbir Sistem Aplikasi MPKj adalah Pegawai Teknologi Maklumat dan Penolong Pegawai Teknologi Maklumat MPKj a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas. (contoh: penukaran dan penghapusan kata laluan sistem yang digunakan oleh kakitangan); b. Memastikan ketepatan dan menyekat kebenaran capaian serta-merta apabila tidak lagi diperlukan atau melanggar Dasar Keselamatan ICT MPKj; c. Memantau aktiviti capaian harian pengguna; d. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat	Pegawai Teknologi Maklumat/ Penolong Pegawai Teknologi Maklumat / Juruteknik

sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT MPKj; e. Memantau aktiviti capaian harian sistem aplikasi pengguna; f. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; g. Menganalisis dan menyimpan rekod jejak audit; h. Menyediakan laporan mengenai aktiviti capaian secara berkala; i. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik. j. Mengenal pasti aktiviti-aktiviti yang tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran, melayari laman-laman web yang tidak dibenarkan dan sebagainya; dan k. Menyediakan laporan mengenai aktiviti capaian secara berkala i. Capaian sistem mengikut permintaan pengguna ii. Capaian internet secara berkala dan mengikut permintaan pengguna.	

0202 Pihak Ketiga	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).	
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPKj; b. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d. Akses kepada aset ICT MPKj perlu berlandaskan kepada perjanjian kontrak;dan e. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MPKj sebagaimana **Lampiran 1**.	CIO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat, Pegawai Keselamatan ICT (ICTSO), Pentadbir Sistem Aplikasi dan Pihak Ketiga

BIDANG 03 PENGURUSAN ASET	
0301 Akauntabiliti Aset	
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MPKj.	
030101 Inventori Aset ICT	
Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik. a. Setiap komputer yang disediakan perlulah dikenal pasti pemilik yang bertanggungjawab menggunakannya. Pegawai yang bertanggungjawab perlu merekodkan butir-butir perkakasan tersebut seperti no siri, pemilik dan jabatan di dalam buku rekod selepas perkakasan tersebut diterima di BTM; b. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MPKj; d. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan e. Setiap pengguna adalah bertanggungjawab ke atas aset ICT di bawah kawalannya.	Penolong Pegawai Teknologi Maklumat, Juruteknik dan Pengguna
0302 Pengelasan dan Pengendalian Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian	

030201 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: i. Rahsia Besar; ii. Rahsia; iii. Sulit; atau iv. Terhad.	Semua
030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan,	Semua

penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	

BIDANG 04 KESELAMATAN SUMBER MANUSIA	
0401 Keselamatan Sumber Manusia Dalam Tugas Harian	
Objektif: Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan MPKj, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga MPKj hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
040101 Sebelum Perkhidmatan	
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan MPKj serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan MPKj serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.	Semua
040102 Dalam Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan pegawai dan kakitangan MPKj serta pihak	Semua

ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MPKj; b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MPKj 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 MPKj serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh MPKj; 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.	
040103 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut:	
a. Memastikan semua aset ICT dikembalikan kepada MPKj mengikut peraturan dan/atau terma perkhidmatanyang ditetapkan; b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh MPKj dan/atau terma perkhidmatan;	Semua Bahagian Teknologi Maklumat

c. Pengarah Jabatan bertanggungjawab untuk memaklumkan pertukaran kakitangan di antara bahagian yang berlaku di dalam jabatan yang sama kepada Bahagian Sumber Manusia; dan	Pengarah Jabatan
d. Bahagian Sumber Manusia bertanggungjawab untuk mengeluarkan surat makluman berkaitan pertukaran dalaman yang berlaku kepada Bahagian Teknologi Maklumat (BTM) dan Bahagian Pengurusan Aset (BPA) berkaitan pertukaran dalaman berikut: • Pertukaran dalaman yang berlaku di antara Jabatan • Pertukaran dalaman yang berlaku di antara bahagian di dalam jabatan yang sama	Bahagian Sumber Manusia

BIDANG 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN	
0501 Keselamatan Kawasan	
Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
050101 Kawalan Kawasan	
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; c. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; d. Memastikan kawasan yang mempunyai aset ICT dilengkapi dengan perlindungan keselamatan yang mencukupi seperti alat pencegah kebakaran dan sebagainya;	ICTSO, Penolong Pegawai Teknologi Maklumat

e. Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; f. Bagi menjamin keselamatan kakitangan dan orang awam semasa situasi wabak pandemik (COVID-19) pemakaian perlu mematuhi pada pekeliling yang terkini.	
050102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Akses masuk ke bilik server hendaklah dihadkan kepada pegawai-pegawai yang diberi kuasa sahaja; b. Setiap pelawat perlu menandatangani buku log keluar masuk bilik server.	Semua
050103 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. a. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Semua

0502 Keselamatan Peralatan	
Objektif: Melindungi peralatan ICT MPKj dari kehilangan, kecurian serta gangguan kepada peralatan tersebut.	
050201 Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan. Sekiranya sebarang penukaran pada komponen asal komputer dikesan, memo peringatan akan dikeluarkan dan diminta memberikan penjelasan; d. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f. Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;	Semua

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

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

i. 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;

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

k. Peralatan ICT yang hendak dibawa keluar dari premis MPKj, perlulah mendapat kelulusan ICTSO/ Penolong Pegawai Teknologi Maklumat/ Juruteknik dan direkodkan bagi tujuan pemantauan;

l. Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;

m. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa;

n. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran ICTSO;

o. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Juruteknik untuk dibaik pulih dan tindakan menyelesaikan masalah kerosakan secara sendiri adalah **SAMA SEKALI** tidak dibenarkan;

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

q. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;

r. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;

s. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat;

t. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO;

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

v. Perkongsian data dan pencetak yang ingin dicapai oleh pengguna lain boleh dicapai menggunakan aplikasi "Log On" yang telah disediakan;

w. Juruteknik yang bertanggungjawab perlu memastikan

aktiviti peminjaman dan pemulangan peralatan ICT direkodkan dan menyemak peralatan yang dipulangkan berada dalam keadaan baik danlengkap;dan x. Pegawai yang bertanggungjawab mestilah memastikan peralatan ICT yang dibawa keluar tidak mengandungi maklumat kerajaan. Ia perlu disalin dan dihapuskan.	
050202 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti cakera padat, *thumb drive* dan media storan mudah alih. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; c. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; d. Semua media storan yang mengandungi data kritikal hendaklah disimpan tempat yang selamat;	Semua

e. Akses dan pergerakan media storan hendaklah direkodkan; f. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; g. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan danbagi mengelakkan kehilangan data; h. Dokumen perlu diletakkan kata laluan supaya hanya orang yang berhak sahaja dapat membukanya; i. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan j. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
050203 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

050204 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MPKj; b. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran ICTSO; c. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua
050205 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b. Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan	Penolong Teknologi Maklumat dan Juruteknik

atau atas keperluan; dan f. Semua penyelenggaraan mestilah mendapat kebenaran daripada ICTSO.	
050206 Peminjaman Peralatan	
Peralatan yang dipinjam hendaklah mendapat kelulusan mengikut peraturan yang telah ditetapkan oleh MPKj bagi membawa keluar perkakasan, perisian atau maklumat tertakluk kepada tujuan yang dibenarkan. Langkah-langkah perlu diambil termasuklah seperti berikut: a. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh MPKj bagi membawa keluar peralatan, perisian atau maklumat tertakluk kepada tujuan yang dibenarkan; b. Melindungi dan mengawal peralatan sepanjang masa; c. Merekodkan aktiviti peminjaman dan pemulangan peralatan; dan d. Menyemak peralatan ketika peminjaman dan pemulangan dilakukan.	Semua
050207 Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari premis MPKj adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan b. Penyimpanan atau penempatan peralatan mestilah	Semua

mengambil kira ciri-ciri keselamatan yang bersesuaian.	
050208 Pelupusan Perkakasan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MPKj dan ditempatkan di MPKj. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MPKj. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c. Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; e. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan	Semua, Pegawai Aset

tersebut;

f. Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT;

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

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

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

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

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

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

v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua

seperti storan mudah alih atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
0503 Keselamatan Persekitaran	
Objektif: Melindungi aset ICT MPKj dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050301 Kawalan Persekitaran	
Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran	Semua

peralatan komputer; g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya sekali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu;dan h. Akses kepada saluran *riser* hendaklah sentiasa berkunci.	
050302 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	ICTSO, Penolong Pegawai Teknologi Maklumat dan Juruteknik
050303 Kabel	
Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah.	ICTSO, Penolong Pegawai Teknologi

Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wiretapping;* dan d. Semua kabel perlu dilabelkan dengan jelas danmestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Maklumat dan Juruteknik
0504 Keselamatan Dokumen	
Objektif: Melindungi maklumat MPKj dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
050401 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; b. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; c. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; d. Menggunakan enkripsi (*encryption*) ke atas dokumen	Semua

rahsia rasmi yang disediakan dan dihantar secara elektronik.	

BIDANG 06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0601 Pengurusan Operasi dan Komunikasi	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
060101 Pengendalian Prosedur	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua
060102 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	Semua

pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
060103 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan c. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

operasi dan rangkaian.	
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
060201 Perkhidmatan Penyampaian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua
0603 Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301 Perancangan Kapasiti	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang.	ICTSO

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.	
060302 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat
0604 Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya.	
060401 Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, serta mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d. Mengemas kini antivirus dengan *pattern* antivirus yang terkini; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini	Semua

seperti kehilangan dan kerosakan maklumat; f. Menghadiri sesi kesedaran mengenai ancamanperisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
060402 Perlindungan dari Mobile Code	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
0605 *Housekeeping*	
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
060501 *Backup*	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat *backup* ke atas semua data kritikal dalam Sistem Aplikasi mengikut keperluan organisasi.Kekerapan *backup* bergantung pada tahap kritikal maklumat;	Semua

b. Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; c. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	
0606 Pengurusan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
060601 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklahdikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Penolong Pegawai Teknologi Maklumat;	ICTSO, Penolong Pegawai Teknologi Maklumat

e. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan MPKj; f. Memasang *Internet Access Management* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; g. Sebarang penyambungan rangkaian yang bukan di bawah kawalan MPKj adalah tidak dibenarkan; h. Semua pengguna hanya dibenarkan menggunakan rangkaian MPKj sahaja dan penggunaan *Uninterruptible Power Supply* (UPS) adalah dilarang sama sekali; i. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan; j. Perkongsian fail hanya dibenarkan kepada pengguna di setiap tingkat sahaja. (Contoh:Pengguna di tingkat 2 hanya boleh berkongsi fail dengan pengguna di tingkat 2 sahaja dan sebaliknya); dan k. Memastikan kemudahan rangkaian WAN dan LAN tidak digunakan untuk kepentingan peribadi atau komersial.	
0607 Pengurusan Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
060701 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih	Semua

dahulu.	
060702 Prosedur Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Semua
060703 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	Semua

dokumentasi sedia ada.	
0608 Pengurusan Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara MPKj dan agensi luar terjamin.	
060801 Pertukaran Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara MPKj dengan agensi luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MPKj dan; d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua
060802 Pengurusan Mel Elektronik (E-mel)	
Penggunaan e-mel di MPKj hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*" dan mana-mana undang-undang bertulis yang	Semua

berkuat kuasa.

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

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

b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh MPKj;

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

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

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

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

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

h. Pengguna dilarang untuk menghantar e-mel yang berunsur fitnah, ugutan dan hasutan yang boleh mengancam ketenteraman awam. i. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; j. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; k. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; l. Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; m. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; n. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing; o. Semua fail yang diterima daripada agensi luar akan ditapis dan diimbas melalui aplikasi Sonicwall Email Security bagi mengelakkan penyebaran spam dan virus; p. Pengguna juga perlu melaporkan dengan kadar segera	

apabila menerima e-mel dan fail kepilan yang tidak diketahui pengirimnya serta meragui asal-usulnya. Pemilik e-mel juga boleh terus menghapuskan e-mel tersebut sekiranya meraguikesahihan e-mel tersebut; dan q. Akaun pengguna e-mel yang tidak lagi berkhidmat di MPKj perlu dipadamkan. Bagi Pegawai Gred A dan B yang baru dilantik, akaun emel baru akan diwujudkan. Akaun Pegawai Gred C diwujudkan atas permintaan pengguna dan kelulusan Pengarah Jabatan.	
0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)	
Objektif: Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
060901 E-Dagang	
Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Maklumat yang terlibat dalam atas talian perlu dilindungi daripada aktiviti penipuan, pertikaiankontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b. Maklumat yang terlibat dalam transaksi atas talian (*online*) perlu dilindungi bagi mengelak penghantaran	Semua

yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c. Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lainyang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	
060902 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: a. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b. Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan c. Memastikan segala maklumat yang hendakdipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua
0610 Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
061001 Pengauditan dan Forensik ICT	
ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT MPKj;	ICTSO

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.	
061002 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*).Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistemsecara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahandalam sesuatu acara.	Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat, ICTSO

Jejak audit hendaklah mengandungi maklumat-maklumat berikut: a. Rekod setiap aktiviti transaksi; b. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan d. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.	
061003 Sistem Log	
Perkara-perkara berikut perlu dilaksanakan: 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 membaikpulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Penolong Pegawai Teknologi Maklumat hendaklah melaporkan kepada ICTSO dan CIO.	Penolong Pegawai Teknologi Maklumat
061004 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Penolong Pegawai Teknologi Maklumat

a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; c. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubah suai dan sebarang capaian yang tidak dibenarkan; d. Aktiviti pentadbiran dan operator sistem perlu direkodkan; e. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan f. Waktu yang berkaitan dengan sistem pemprosesan makluman dalam MPKj atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	

BIDANG 07 KAWALAN CAPAIAN	
0701 Dasar Kawalan Capaian	
Objektif: Mengawal capaian ke atas maklumat	
070101 Keperluan Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d. Kawalan ke atas kemudahan pemprosesan maklumat.	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat
0702 Pengurusan Capaian Pengguna	
Objektif: Mengawal capaian pengguna ke atas aset ICT MPKj	

070201 Akaun Pengguna	
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh MPKj sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan MPKj. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f. Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Bertukar bidang tugas kerja; ii. Bertukar ke agensi lain; iii. Bersara; atau iv. Ditamatkan perkhidmatan.	Semua

070202 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat
070203 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 MPKj seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c. Panjang kata laluan mestilah sekurang-kurangnya dari lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus; d. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;	Semua

f. Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; h. Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; i. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan j. Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
070204 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan kemudahan *Password Screen Saver* bermula dari 10 minit hingga 15 minit selepas meninggalkan komputer;	Semua

b. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	
0703 Kawalan Capaian Rangkaian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
070301 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MPKj, rangkaian agensi lain dan rangkaian awam; b. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO, Penolong Pegawai Teknologi Maklumat
070302 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan Internet di MPKj hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat	ICTSO, Penolong Pegawai Teknologi Maklumat

melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MPKj;

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

c. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. ICTSO berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya. Pengguna perlu mendapatkan kebenaran Ketua Jabatan bagi kebenaran penggunaan Internet;

d. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan/ pegawai yang diberi kuasa;

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

f. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Jabatan sebelum dimuat naik ke Internet;

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

h. Sebarang bahan yang dimuat turun dari Internet

hendaklah digunakan untuk tujuan yang dibenarkan oleh MPKj; i. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; j. Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan k. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian Internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	
0704 Kawalan Capaian Sistem Pengoperasian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistempengoperasian.	
070401 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan.	ICTSO, Penolong Pegawai

Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a. Mengenal pasti identiti 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 dan c. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem.	Teknologi Maklumat
0705 Kawalan Capaian Aplikasi dan Maklumat	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi	
070501 Capaian Aplikasi dan Maklumat	
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara perkara berikut hendaklah dipatuhi: a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

dan keselamatan maklumat yang telah ditentukan; b. Setiap *Login/Logout* ke capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan c. Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; d. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
0706 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh	
070601 Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua
070602 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; dan	Semua

b. Tertakluk kepada pekeliling semasa **(Lampiran 2: Senarai Perundangan dan Peraturan)**	

BIDANG 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi	
Objektif: Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian	
080101 Keperluan Keselamatan Sistem Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan danintegriti data yang dimasukkan,sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; c. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebihdahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telahditetapkan sebelum digunakan.	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

080102 Pengesahan Data *Input* dan *Output*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Data *input* bagi aplikasi perlu disahkan bagimemastikan data yang dimasukkan betul danbersesuaian; dan b. Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Penolong Pegawai Teknologi Maklumat
0802 Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080201 Enkripsi	
Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
080202 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
0803 Keselamatan Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
080301 Kawalan Fail Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Proses pengemaskinian fail sistem hanya boleh dilakukan pegawai yang berkenaan dan mengikut	Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

prosedur yang telah ditetapkan; b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal;dan e. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan	
0804 Keselamatan Dalam Proses Pembangunan dan Sokongan	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
080401 Prosedur Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; c. Mengawal perubahan dan/atau pindaan ke atas pakej	Pegawai Teknologi Maklumat, Penolong PegawaiTeknologi Maklumat

perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d. Akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e. Menghalang sebarang peluang untuk membocorkan maklumat.	
080402 Pembangunan Perisian Secara *Outsource*	
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik MPKj.	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat
0805 Kawalan Kerentanan Teknikal (*Vulnerability*)	
Objektif: Memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
080501 Kawalan dari Ancaman Teknikal	
Kawalan kerentanan teknikal ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memperoleh maklumat kerentanan teknikal berkala ke atas sistem maklumat yang digunakan. b. Memperoleh maklumat kerentanan teknikal ke atas sistem maklumat yang baharu sebelum digunakan dalam persekitaran *production*	Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat,

c. Menilai tahap kerentanan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan d. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	

BIDANG 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN	
0901 Mekanisme Pelaporan Insiden Keselamatan ICT	
Objektif: Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamat ICT	
090101 Mekanisme Pelaporan	
Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan NACSA (*National Cyber Security Agency*) dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberikuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka.	Semua

0902 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada MPKj. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; b. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; d. Menyediakan tindakan pemulihan segera; dan e. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO

BIDANG 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	
1001 Dasar Kesinambungan Perkhidmatan	
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
100101 Pelan Kesinambungan Perkhidmatan	
Pelan Kesinambungan Perkhidmatan (*Business Continuity Management - BCM*) atau Pelan Pemulihan Bencana (*Disaster Recovery Plan* – DRP) 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 Jawatankuasa Perkhidmatan dan Teknologi Maklumat atau jawatankuasa yang setara. Perkara-perkara berikut perlu diberi perhatian: a. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; c. Melaksanakan prosedur-prosedur kecemasan bagimembolehkan pemulihan dapat dilakukan secepatmungkin atau dalam jangka masa yang telah ditetapkan; d. Mendokumentasikan proses dan prosedur yang telah dipersetujui;	ICTSO

e. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;

f. Membuat *backup* dan *restore*; dan

g. Menguji dan mengemas kini pelan sekurang- kurangnya dua tahun sekali atau sekiranya terdapat sebarang perubahan dalam persekitaran atau fungsi perkhidmatan.

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

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

b. Senarai personel MPKj dan vendor berserta nombor boleh dihubungi (telefon dan e-mel). Personel alternatif juga hendaklah dikenalpasti sebagai menggantikan personel yang tidak dapat hadir menangani insiden;

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

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

e. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan.

Salinan pelan ini perlu disimpan di lokasi berasingan atau dalam talian (digital) untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan ini hendaklah diuji sekurang-kurangnya setahun sekali atau apabila terdapat perubahan dalam persekitaran atau fungsi perkhidmatan untuk

memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan ini hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. MPKj hendaklah memastikan salinan pelan ini sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

BIDANG 11 PEMATUHAN	
1101 Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT MPKj.	
110101 Pematuhan Dasar – Dasar Bagi Hak Harta Intelek	
Setiap pengguna di MPKj hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MPKj dan undang- undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di MPKj termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT MPKj selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakansatu penyalahgunaan sumber MPKj. **<u>Dasar bagi Hak Harta Intelek</u>** Akta Hakcipta (Pindaan) 2012 hendaklah sentiasa dipatuhi bagi menghalang aktiviti menciplak hak cipta orang lain. Perkara berikut perlu diambil kira untuk melindungi hartaintelek: i. Penggunaan perisian yang sah; ii. Pembelian dari sumber yang sahih; iii. Sentiasa mengadakan program kesedaran terhadap dasar perlindungan harta intelek; iv. Mengekalkan daftar aset dan mengenalpasti semua keperluan perlindungan terhadap aset; v. Menyimpan lesen perisian; vi. Memastikan bilangan had lesen tidak melebihi had ditetapkan; dan	Semua

vii. Menjalankan pemeriksaan perisian yang sah dan produk berlesen digunakan.	
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
110103 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat.Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua
110104 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di MPKj adalah seperti di Lampiran 2.	Semua
110105 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT MPKj boleh dikenakan tindakan tatatertib.	Semua

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

GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
Hub	Hab (*hub*) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian

	rangkaian tersebut agar sentiasa berasingan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer
Logout	*Log-out* computer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *Trojanhorse, worm, spyware* dan sebagainya.
MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.

Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT MPKj

Nama (Huruf Besar) : ……

No. Kad Pengenalan : ……

Jawatan : ……

Jabatan / Bahagian/Syarikat: ……

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yangterkandung di dalam Dasar Keselamatan ICT MPKj; dan

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

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....

(Nama Pegawai Keselamatan ICT)

b.p Yang DiPertua, Majlis Perbandaran Kajang

Tarikh : .....

LAMPIRAN 2

SENARAI PERUNDANGAN DAN PERATURAN

a. Arahan Keselamatan;

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

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

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

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

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

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

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

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

j. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh23 November2007;

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

l. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) –

Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

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

n. Akta Tandatangan Digital 1997;

o. Akta Rahsia Rasmi 1972;

p. Akta Jenayah Komputer 1997;

q. Akta Hak Cipta (Pindaan) Tahun 1997;

r. Akta Komunikasi dan Multimedia 1998;

s. Perintah-Perintah Am;

t. Arahan Perbendaharaan;

u. Arahan Teknologi Maklumat 2007;

v. Garis Panduan Keselamatan MAMPU 2004;

w. Standard Operating Procedure (SOP) ICT MAMPU;

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

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

z. Arahan Hadir Bekerja S emasa Tempoh Perintah Kawalan Pergerakan Bersyarat di Pentadbiran Setiausaha Kerajaan Negeri Selangor – 2 Mei 2020;

aa. Budaya Kerja Perkhidmatan Awam Semasa Pelaksanaan Perintah Kawalan Pergerakan (PKP) Pentadbiran Kerajaan Negeri Selangor – 9 Jun 2020;

bb. Budaya Kerja Perkhidmatan Awam Semasa Tempoh Perintah Kawalan Pergerakan Pemulihan (PKPP) Pentadbiran Kerajaan Negeri Selangor – 12 Januari 2021;

cc. Arahan Pengoperasian Pejabat Kerajaan di Bawah Perintah-Perintah Kawalan Pergerakan – 12 Januari 2021;

dd. Arahan Pengoperasian Pejabat Kerajaan di Bawah Pentadbiran Kerajaan Negeri Selangor Semasa Perintah Kawalan Pergerakan – 5 Mei 2021

ee. Arahan Pengoperasian Pejabat Kerajaan di Bawah Pentadbiran Kerajaan Negeri Selangor Semasa Perintah Kawalan Pergerakan 3.0

Diperketatkan – 23 Mei 2021;

ff. Garis Panduan Pengoperasian Pejabat Kerajaan Di Bawah Perintah Kawalan Pergerakan 3.0 – 24 Mei 2021;

gg. Arahan Pengoperasian Pejabat Kerajaan Di Bawah Pentadbiran Kerajaan Negeri Selangor Semasa Tempoh Perintah Kawalan Pergerakan (PKP) 3.0 : 15 Hingga 28 Jun 2021 – 16 Jun 2021;

hh. Arahan Pengoperasian Perkhidmatan Kaunter Pejabat Kerajaan Di Bawah Pentadbiran Kerajaan Negeri Selangor Dalam Fasa Pertama Pelan Pemulihan Negara – 29 Jun 2021;

ii. Pelaksanaan Perintah Kawalan Pergerakan Diperketatkan (PKPD)Berkaitan Penularan Wabak Covid-19 Peringkat Pentadbiran Kerajaan Negeri Selangor – 2 Julai 2021;

jj. Arahan Pengoperasian Pejabat Kerajaan di Bawah Pentadbiran Kerajaan Negeri Selangor Mengikut Fasa Pelan Pemulihan Negara (PPN) dan Perintah Kawalan Pergerakan Diperketatkan (PKPD) – 19 Julai 2021;

kk. Arahan Pengoperasian Pejabat Kerajaan Di Bawah Pentadbiran Kerajaan Negeri Selangor Mengikut Fasa Pelan Pemulihan Negara (PPN) – 23 Julai 2021;

ll. Garis Panduan Pengoperasian Pejabat Jabatan Perkhidmatan Awam Dalam Tempoh Perintah Kawalan Pergerakan – 23 Julai 2021;

mm. Arahan Pengoperasian Pejabat Kerajaan di Bawah Pentadbiran Kerajaan Negeri Selangor Mengikut Fasa Pelan Pemulihan Negara – Fasa 2 – 10 September 2021;

nn. Arahan Pengoperasian Pejabat Kerajaan di Bawah Pentadbiran Kerajaan Negeri Selangor Mengikut Fasa Pelan Pemulihan Negara – Fasa 3 – 30 September 2021;

oo. Arahan Pengoperasian Pejabat Kerajaan di Bawah Pentadbiran Kerajaan Negeri Selangor Mengikut Fasa Pelan Pemulihan Negara – Fasa 4 – 21 Oktober 2021