VERSI 1.0

POLISI KESELAMATAN SIBER

MAJLIS PERBANDARAN KAJANG

Disediakan oleh:

BAHAGIAN TEKNOLOGI MAKLUMAT
JABATAN KHIDMAT PENGURUSAN

SEJARAH DOKUMEN

TARIKH PINDAAN	VERSI	KELULUSAN	TARIKH KUATKUASA
15 Mac 2024	1.0	Mesyuarat Jawatankuasa ISMS Bil 1/2024	17 Mei 2024

ISI KANDUNGAN

PENGENALAN

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

OBJEKTIF

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

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

Objektif utama Polisi Keselamatan Siber 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 ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

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

b. Menjamin setiap maklumat adalah tepat dan sempurna;

c. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

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

Polisi Keselamatan Siber 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

Polisi 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, *thumb drive* dan lain-lain.

7. Media Komunikasi

Semua peralatan berkaitan komunikasi seperti pelayan rangkaian, *gateway, bridge, router*, peralatan PABX, *wireless* LAN, WAN, 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 Polisi Keselamatan Siber 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

Polisi Keselamatan Siber 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 bilik server, kabinet berkunci 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 Panduan Penilaian 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

A.5 KAWALAN ORGANISASI	
KENYATAAN	**TANGGUNGJAWAB**
5.1 Polisi Keselamatan Maklumat	
5.1.1 Pelaksanaan Polisi	
Pelaksanaan ini akan dijalankan oleh Tuan Yang Dipertua dan dibantu oleh Jawatankuasa ICT.	Yang Dipertua MPKj
5.1.2 Penyebaran Polisi	
Polisi ini perlu disebarkan kepada semua warga MPKj dan pihak ketiga termasuklah pembekal, pakar runding dan lain-lain.	ICTSO
5.1.3 Penyelenggaraan Polisi	
Polisi Keselamatan Siber 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 Polisi Keselamatan Siber MPKj adalah seperti berikut: a. Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan Jawatankuasa ISMS; b. Memaklumkan cadangan pindaan yang telah dipersetujui kepada Jawatankuasa ISMS bagi tujuan pengesahan; c. Memaklumkan perubahan yang telah dipersetujui kepada semua pengguna dalam Mesyuarat Jawatankuasa ICT; dan d. Mengkaji semula polisi ini sekurang-kurangnya **dua tahun sekali** ATAU **mengikut keperluan semasa** bagi	ICTSO, Jawatankuasa ICT, Jawatankuasa ISMS

mengenal pasti dan menentukan perubahan yang diperlukan.	
5.1.4 Pematuhan dan Pengecualian Dasar	
Polisi Keselamatan Siber MPKj perlu dipatuhi dan terpakai kepada semua warga MPKj dan Pihak Ketiga tanpa sebarang pengecualian diberikan.	Warga MPKj dan Pihak Ketiga
5.2 Peranan dan Tanggungjawab Keselamatan Siber	
5.2.1 Yang Dipertua MPKj	
a. Menentukan halatuju dan strategi pelaksanaan keselamatan siber MPKj b. Memastikan semua keperluan organisasi (contoh: sumber kewangan, sumber manusia dan sumber perlindungan keselamatan) adalah mencukupi. c. Melantik CDO dan ICTSO; d. Menguatkuasakan Polisi Keselamatan Siber MPKj.	Yang Dipertua MPKj
5.2.2 Ketua Pegawai Digital (CDO)	
Ketua Pegawai Digital (CDO) bagi MPKj ialah Timbalan Yang Dipertua MPKj. Peranan dan tanggungjawab CDO adalah seperti berikut: a. Membantu Yang Dipertua dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber sebagaimana yang ditetapkan dalam Polisi Keselamatan Siber MPKj. b. Rujuk surat lantikan CDO para 5. c. Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan dalam polisi ini. d. Memastikan pelan strategik pendigitalan ICT MPKj mengandungi aspek keselamatan siber.	Ketua Pegawai Digital (CDO)

e. Memastikan kawalan keselamatan dalam MPKj diseragam dan diselaraskan dengan sebaiknya. f. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MPKj.	
5.2.3 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 Polisi Keselamatan Siber MPKj; c. Memberi penerangan dan pendedahan berkaitan Polisi Keselamatan Siber; d. Menjalankan pengurusan risiko; e. Menyelia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; f. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber MPKj; g. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MPKj berdasarkan hasil penemuan dan menyediakan laporan mengenainya; h. Memberi amaran terhadap sebarang ancaman berbahaya seperti serangan virus dan memberi khidmat nasihat serta menyediakan langkah-langkah keselamatan; dan i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah- langkah baik pulih	Pegawai Keselamatan ICT (ICTSO)

dengan kadar segera.	
5.2.4 Pegawai Teknologi Maklumat /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. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi Keselamatan Siber MPKj; c. Memantau aktiviti capaian sistem aplikasi pengguna; d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e. Menganalisis dan menyimpan rekod jejak audit; f. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; g. Mengenal pasti aktiviti-aktiviti yang tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran, melayari laman-laman web yang tidak dibenarkan dan sebagainya; h. Melaporkan sebarang insiden keselamatan ICT kepada ICTSO; dan i. Menyediakan laporan mengenai aktiviti capaian secara	Pegawai Teknologi Maklumat /Penolong Pegawai Teknologi Maklumat/ Juruteknik

berkala.	
5.2.5 Pengguna	
a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber MPKj; b. Mengetahui dan memahami implikasi keselamatan ICT dari sudut kesan dan tindakannya; c. Melaksanakan arahan-arahan Polisi Keselamatan Siber 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 Polisi Keselamatan Siber 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
5.2.6 Pengurus Projek ICT	
Pengurus Projek ICT bagi MPKj adalah pegawai yang telah ditugaskan untuk mengendalikan projek ICT Peranan dan tanggungjawab Pengurus Projek ICT adalah seperti berikut: a. Mengkaji semula dan melaksanakan kawalan keselamatan	Pegawai Teknologi Maklumat / Penolong Pegawai Teknologi

ICT selaras dengan keperluan MPKj; b. Memastikan sistem kawalan capaian pengguna ke atas aset -aset ICT MPKj dilaksanakan. c. Memastikan aspek keselamatan maklumat dilaksanakan dalam setiap pengurusan projek. d. Melaksanakan keperluan Polisi Keselamatan Siber (PKS) dalam operasi semasa seperti berikut: i. Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; ii. Pembelian atau peningkatan perisian dan sistem komputer; iii. Perolehan teknologi dan perkhidmatan komunikasi baharu; iv. Pelantikan pembekal, perunding atau rakan usahasama; dan v. Menentukan pembekal, perunding atau rakan usahasama menjalani tapisan keselamatan selaras dengan keperluan tahap perkhidmatan.	Maklumat

5.2.7 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. Mengenal pasti aktiviti- aktiviti tidak normal dan memastikan ketepatan serta menyekat kebenaran capaian serta merta jika terdapat pencerobohan, pengubahsuaian data tanpa kebenaran dan pelanggaran Polisi Keselamatan Siber MPKj; c. Memantau aktiviti capaian sistem aplikasi pengguna; d. Menganalisis dan menyimpan rekod jejak audit; e. Menyediakan laporan mengenai aktiviti capaian secara berkala; f. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; dan g. Melaporkan sebarang insiden keselamatan ICT kepada ICTSO.	Pegawai Teknologi Maklumat/ Penolong Pegawai Teknologi Maklumat

5.3 Pengasingan Tugas

5.3.1 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

5.4 Tanggungjawab Pihak Pengurusan	
5.4.1 Dalam Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan pegawai dan kakitangan MPKj serta pihak 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 warga 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.	Warga MPKj
5.5 Hubungan dengan Pihak Berkuasa	
Mewujudkan dan mengemaskini prosedur/senarai pihak berkuasa perundangan/ pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan termasuklah Polis Diraja Malaysia (PDRM) dan Suruhanjaya Komunikasi dan Multimedia (SKMM). Pihak yang dihubungi semasa	Bahagian Teknologi Maklumat

kecemasan termasuklah tetapi tidak terhad kepada pihak penyedia utiliti, pembekal elektrik, pembekal perkhidmatan dan lain-lain.	
5.6 Hubungan dengan Kumpulan Berkepentingan yang Khusus	
Hubungan dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan seperti Agensi Keselamatan Siber Negara (NACSA), Jabatan Digital Negara(JDN), Pejabat Ketua Keselamatan Kerajaan (CGSO), Cybersecurity Malaysia dan lain-lain.	Pasukan CSIRT dan CERT MPKj
5.7 Ancaman Risikan	
Memberi kesedaran tentang persekitaran MPKj yang terancam supaya tindakan mitigasi yang bersesuaian dapat diambil. Maklumat berkaitan ancaman sedia ada atau yang bakal muncul perlu dikumpul untuk: a) Membantu dalam tindakan pencegahan kepada ancaman yang mendatangkan kemudaratan kepada MPKj ; dan b) Mengurangkan kesan dari ancaman tersebut.	Mesyuarat Jawatankuasa ISMS/Mesyuarat Kajian Semula ISMS
5.8 Keselamatan Maklumat Dalam Pengurusan Projek	
5.8.1 Pengurus Projek ICT	
Pengurus Projek ICT bagi MPKj adalah pegawai yang telah ditugaskan untuk mengendalikan projek ICT Peranan dan tanggungjawab Pengurus Projek ICT adalah seperti berikut: a. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MPKj; b. Memastikan sistem kawalan capaian pengguna ke atas	Pengurus Projek ICT

aset -aset ICT MPKj dilaksanakan. c. Memastikan aspek keselamatan maklumat dilaksanakan dalam setiap pengurusan projek. d. Melaksanakan keperluan Polisi Keselamatan Siber (PKS) dalam operasi semasa seperti berikut: i. Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; ii. Pembelian atau peningkatan perisian dan sistem komputer; iii. Perolehan teknologi dan perkhidmatan komunikasi baharu; iv. Pelantikan pembekal, perunding atau rakan usahasama; dan v. Menentukan pembekal, perunding atau rakan usahasama menjalani tapisan keselamatan selaras dengan keperluan tahap perkhidmatan.	
5.9 Inventori Maklumat dan Aset ICT	
5.9.1 Inventori Aset ICT	
Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik. a. Memastikan semua aset ICT perolehan secara pembelian dikenal pasti dan maklumat aset direkodkan serta dikemaskini dari semasa ke semasa ke dalam sistem pengurusan aset berdasarkan pekeliling yang sedang berkuatkuasa; b. Memastikan semua aset perolehan secara sewaan dikenal pasti dan maklumat aset direkodkan serta dikemaskini dari semasa ke semasa;	Pegawai Aset/ Pembantu Pegawai Aset ICT/Pengguna

c. Memastikan semua aset ICT diuruskan oleh Pegawai Aset/Pembantu Pegawai Aset (ICT) dan dikendalikan oleh Pengguna yang dibenarkan sahaja; d. Memastikan semua warga MPKj mengesahkan penempatan aset ICT yang ditempatkan; e. Peraturan bagi pengendalian aset ICT hendaklah dipatuhi dan dilaksanakan; f. Setiap warga MPKj adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan g. Memastikan semua aset ICT diagihkan kepada warga MPKj mengikut piawaian dan garis panduan yang ditetapkan.	
5.10 Penggunaan Maklumat dan Aset ICT	
5.10.1 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 ada untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. Memberi perhatian kepada maklumat terperingkat	Warga MPKj

terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	
5.11 Pemulangan Aset	
5.11.1 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 perkhidmatan yang ditetapkan; b. Pengarah Jabatan bertanggungjawab untuk memaklumkan pertukaran kakitangan di antara bahagian yang berlaku di dalam jabatan yang sama kepada Bahagian Sumber Manusia; dan c. Bahagian Sumber Manusia bertanggungjawab untuk mengeluarkan surat makluman berkaitan pertukaran dalaman yang berlaku kepada Bahagian Teknologi Maklumat (BTM) dan Unit Pengurusan Aset (UPA) berkaitan pertukaran dalaman berikut: • Pertukaran dalaman yang berlaku di antara Jabatan • Pertukaran dalaman yang berlaku di antara bahagian di dalam jabatan yang sama	Semua Pengarah Jabatan/ Ketua Unit Bahagian Sumber Manusia

5.12 Pengelasan Maklumat	
5.12.1 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: i. Rahsia Besar; ii. Rahsia; iii. Sulit; atau iv. Terhad.	Semua
5.13 Pelabelan Maklumat	
Maklumat hendaklah ditanda dan dikendali berasaskan peringkat keselamatan yang dikenal pasti selaras dengan Arahan Keselamatan -VI Tanda Keselamatan (para 90-99)	Semua

5.14 Pertukaran Maklumat

5.14.1 Pertukaran Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b. Perjanjian 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

5.14.2 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 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	Semua

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 meragui kesahihan 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.	
5.15 Kawalan Akses	
5.15.1 Keperluan Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

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.	
5.15.2 Hak Capaian	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas; dan b. Pentadbir Sistem ICT perlu semak dan kemaskini ke atas hak capaian pengguna.	Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat
5.15.3 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MPKj seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan	Semua

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; Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; f. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; g. Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; h. Kata laluan hendaklah ditukar selepas 180 hari dalam tempoh setahun atau set semula kata laluan pengguna secara manual bagi Sistem Penilaian, Taksiran dan Kutipan; dan i. Mengelakkan penggunaan semula kata laluan yang baru digunakan.	

5.16 Pengurusan Identiti

5.16.1 Akaun Pengguna

Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh 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

5.17 Pengesahan Maklumat

5.17.1 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; 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,	Semua

sesi ditamatkan; i. Kata laluan hendaklah ditukar selepas 180 hari dalam tempoh setahun atau set semula kata laluan pengguna secara manual bagi Sistem Penilaian, Taksiran dan Kutipan; dan j. Mengelakkan penggunaan semula kata laluan yang baru digunakan	
5.17.2 Pengurusan Pengesahan Maklumat Rahsia Pengguna	
Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal dan diselia melalui proses pengurusan yang formal.	Semua
5.17.3 Penggunaan Maklumat Pengesahan Rahsia	
Melaksanakan langkah-langkah perlindungan seperti 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 ICT yang ditetapkan; f. Melaksanakan peraturan berkaitan maklumat rahsia rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan berdasarkan Arahan Keselamatan; g. Menjaga kerahsiaan langkah-langkah keselamatan	Semua

ICT dari diketahui umum; dan h. Mengawal aktiviti penggunaan media sosial seperti dibawah: i. Mengelakkan ketirisan maklumat; ii. Tidak memberi atau mendedahkan sebarang komen atau pernyataan atau isu yang menyentuh perkara-perkara yang boleh menjejaskan imej dan dasar kerajaan; iii. Tidak menyebarkan maklumat yang berbentuk fitnah, hasutan dan lucah atau cuba memprovokasikan sesuatu isu yang menyalahi peraturan dan undang undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan iv. Tidak menggunakan saluran media sosial hingga mengganggu fokus dalam urusan kerja	
5.18 Hak Akses Pengguna	
5.18.1 Akaun Pengguna	
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh MPKj sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;	Semua

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	
5.19 Keselamatan Maklumat Berhubung dengan Pembekal	
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 polisi perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua

5.20 Elemen Keselamatan Dalam Perjanjian Dengan Pembekal	
5.20.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat, Pegawai Keselamatan ICT (ICTSO), Pentadbir Sistem Aplikasi dan 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 Polisi Keselamatan Siber 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 Polisi Keselamatan Siber MPKj sebagaimana **Lampiran 1**.	CIO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat, Pegawai Keselamatan ICT (ICTSO), Pentadbir Sistem Aplikasi dan Pihak Ketiga

5.21 Rantaian Bekalan Teknologi	
5.21.1 Perkhidmatan Penyampaian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c. Pengurusan perubahan polisi perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua
5.21.2 Rantaian Bekalan Teknologi Maklumat Dan Komunikasi	
Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk/perkhidmatan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan c. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa	Semua

dapat dibekalkan dan berfungsi dengan baik.	
5.21.3 Mekanisme Kawalan Peralatan Sewaan/Ujicuba *(Proof Of Concept)*	
Sebarang *proof of concept* (POC) yang dijalankan perlu mendapatkan kelulusan ICTSO dengan mengambilkira perkara-perkara berikut: a. Penerimaan i. Peralatan/perisian yang diterima bebas daripada sebarang perisian hasad (*malware)* dan perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT MPKj; dan ii. Pembekal yang terlibat perlu memastikan semua syarat keselamatan dipatuhi: • Polisi Keselamatan Siber MPKj; • Perakuan Akta Rahsia Rasmi 1972. • Hak Harta Intelek; dan • Perlindungan Peribadi. b. Penyelenggaraan i. Capaian melalui rangkaian luar MPKj adalah tidak dibenarkan; dan ii. Aktiviti penyelenggaraan adalah di bawah pengawasan pegawai MPKj. c. Pemulangan i. Maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (*secured delete*); dan ii. Memastikan semua maklumat tidak tertinggal pada peralatan/perisian; d. Hasil penemuan atau hasil dari *Proof of Concept* (POC)	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

perlu diserahkan dan dibentang kepada pihak MPKj dan tidak dibenarkan untuk disebarkan atau dikongsi dengan mana-mana pihak luar; dan e. Sebarang perubahan yang dilakukan perlu direkod dan dikembalikan kepada kepada asal seperti sebelum *Proof of Concept (POC)*.	
5.22 Memantau dan Menyemak Perkhidmatan Pembekal	
5.22.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber 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 Polisi Keselamatan Siber MPKj sebagaimana **Lampiran 1**.	CDO, ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat, Pengurus Projek ICT, Pentadbir Sistem Aplikasi dan Pihak Ketiga

5.22.2 Memantau Dan Menyemak Semula Perkhidmatan Pembekal	
Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal; dan b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa;	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat, Pengurus Projek ICT, Pentadbir Sistem Aplikasi
5.22.2 Menguruskan Perubahan Kepada Perkhidmatan Pembekal	
Pengurusan perubahan polisi perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	ICTSO
5.23 Keselamatan Maklumat Dalam Penggunaan Perkhidmatan Awan	
5.23.1 Penggunaan Storan Awan (Cloud)	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan tiada sebarang maklumat rahsia rasmi disimpan pada storan awan awam (*public cloud storage*). b. Memastikan setiap dokumen rasmi tidak disimpan di storan awan awam (*public cloud storage*); c. Memastikan pengguna tidak menyimpan dokumen tidak rasmi dan tidak berkaitan seperti yang berbentuk hiburan dan tidak bermanfaat pada storan awan yang disediakan oleh MPKj; d. Semua pengguna perlu memastikan kandungan storan awan yang disediakan oleh MPKj diurus dengan	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

baik dan sentiasa membuat kerja-kerja pengemaskinian data atau housekeeping dari semasa ke semasa; dan e. Pengguna perlu memastikan perkongsian fail dan folder hanya dibuat untuk pengguna yang dibenarkan sahaja dalam tempoh yang dibenarkan	
5.24 Perancangan dan Persediaan Pengurusan Insiden Keselamatan Maklumat	
5.24.1 Tanggungjawab dan Prosedur	
Prosedur pelaporan insiden keselamatan maklumat perlu dilaksanakan berdasarkan Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam.	ICTSO dan CSIRT MPKj / CERT MPKj
5.24.2 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 CSIRT dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti	Semua

kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka.	
5.24.3 Melaporkan Kelemahan Keselamatan Maklumat	
Pelaporan juga perlu dilakukan sekiranya terdapat kelemahan keselamatan di dalam sistem atau perkhidmatan.	Semua
5.25 Penilaian Dan Keputusan Dalam Kejadian Keselamatan Maklumat	
Kejadian keselamatan maklumat perlu dinilai dan diklasifikasikan sebagai insiden keselamatan maklumat.	CSIRT MPKj / CERT MPKj
5.26 Tindak Balas Terhadap Insiden Keselamatan Maklumat	
Insiden keselamatan maklumat perlu diberi tindakbalas sewajarnya mengikut prosedur yang telah didokumenkan.	CSIRT MPKj / CERT MPKj
5.27 Pembelajaran Daripada Insiden Keselamatan Maklumat	
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.	CSIRT MPKj / CERT MPKj
5.28 Pengumpulan Bahan Bukti	
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, penduaan secara berkala dan melindungi integriti semua bahan bukti; b. Menyalin bahan bukti dan merekodkan semua	CSIRT MPKj / CERT MPKj

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.	
5.29 Melaksanakan kesinambungan Keselamatan Maklumat	
5.29.1 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 bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa	ICTSO, Pasukan DRP

yang telah ditetapkan;

d. Mendokumentasikan proses dan prosedur yang telah dipersetujui;

e. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;

f. Membuat penduaan (*backup)* dan pulih (*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 penduaan (*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 dua tahun 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.	
5.30 Persediaan ICT untuk Kesinambungan Keselamatan	
Pelan Pemulihan Bencana (DRP) hendaklah diuji sekurang-kurangnya dua tahun sekali atau apabila terdapat perubahan dalam persekitaran atau fungsi perkhidmatan MPKj untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian ini hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan pegawai yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.	ICTSO, Pasukan DRP

5.31 Undang-Undang, Statutori, Kawal Selia dan Kontrak Perjanjian	
5.31.1 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di MPKj adalah seperti di **Lampiran 2**.	Semua
5.32 Hak Harta Intelek	
5.32.1 Pematuhan Dasar – Dasar Bagi Hak Harta Intelek	
Setiap pengguna di MPKj hendaklah membaca, memahami dan mematuhi Polisi Keselamatan Siber 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 merupakan satu 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	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

keperluan perlindungan terhadap aset; v. Menyimpan lesen perisian; vi. Memastikan bilangan had lesen tidak melebihi had ditetapkan; dan vii. Menjalankan pemeriksaan perisian yang sah dan produk berlesen digunakan.	
5.33 Kawalan Rekod	
5.33.1 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; b. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut Arahan keselamatan; c. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut Arahan Keselamatan; d. Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Semua
5.34 Privasi dan Perlindungan Data Peribadi	
Privasi dan perlindungan maklumat peribadi yang boleh dikenalpasti perlu dilaksanakan mengikut keperluan semasa bagi menjamin tahap keselamatan maklumat berada dalam keadaan terkawal dan selamat pada setiap masa.	Semua

5.35 Semakan Semula Keselamatan Maklumat	
5.35.1 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
5.36 Pematuhan kepada Polisi, Peraturan dan Piawaian Keselamatan Maklumat	
5.36.1 Pematuhan dengan Polisi, Piawaian dan Keperluan Teknikal	
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi polisi, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO

5.37 Mendokumenkan Prosedur Operasi

5.37.1 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua

A.6 KAWALAN MANUSIA	
6.1 Saringan	
6.1.1 Sebelum Perkhidmatan	
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	Semua
6.2 Terma Dan Syarat Perkhidmatan	
6.2.1 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

6.3 Kesedaran, Pendidikan Dan Latihan Keselamatan Maklumat	
6.3.1 Dalam Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan pegawai dan kakitangan MPKj serta pihak 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 warga 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.	Semua
6.4 Proses Tindakan Disiplin	
6.4.1 Dalam Perkhidmatan	
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;	Semua

6.5 Tanggungjawab Selepas Pertukaran Atau Penamatan Perkhidmatan	
6.5.1 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 perkhidmatan yang 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; c. Pengarah Jabatan bertanggungjawab untuk memaklumkan pertukaran kakitangan di antarabahagian yang berlaku di dalam jabatan yang sama kepada Bahagian Sumber Manusia; dan 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	Semua
6.6 Perjanjian Kerahsiaan Maklumat	
6.6.1 Sebelum Perkhidmatan	
Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.	Semua

6.7 Kerja Jarak Jauh	
6.7.1 Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Sebarang aktiviti kerja jarak jauh hendaklah mendapat kebenaran daripada ICTSO dan Pengarah Jabatan. b. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan; dan c. Tertakluk kepada pekeliling semasa (Lampiran 2: Senarai Perundangan dan Peraturan)	ICTSO / Pengarah Jabatan Semua
6.8 Pelaporan Kejadian Keselamatan Maklumat	
Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO,CSIRT MPKj dan CERT MPKj dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka.	Semua

A.7 KAWALAN FIZIKAL

7.1 Perimeter Keselamatan Fizikal

7.1.1 Kawalan Kawasan

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Menyediakan ruang 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; 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.	ICTSO, Penolong Pegawai Teknologi Maklumat

7.2 Laluan Masuk Fizikal	
7.2.1 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Pas pekerja/pelawathendaklah dipakai sepanjang waktu bertugas. b. Semua pas pekerja hendaklah diserahkan semula kepada MPKj apabila warga MPKj berhenti dan bersara. c. Pihak ketiga perlu mengambil pas pelawat di kaunter daftar masuk pelawat MPKj dan dikembalikan semula selepas tamat urusan. d. Kehilangan pas pekerja/pelawat mestilah dilaporkan dengan segera kepada pegawai keselamatan e. Akses masuk ke bilik server hendaklah dihadkan kepada pegawai-pegawai yang diberi kuasa sahaja; f. Setiap pelawat perlu menandatangani buku log keluar masuk bilik server dan perlu diiringi oleh pegawai pengiring.	Semua
7.3 Keselamatan Pejabat, Bilik Dan Kemudahan	
7.3.1 Kawalan Kawasan	
Ini bertujuan untuk menghalang akses, kerosakan dangangguan 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 untukmelindungi aset dan hasil penilaian risiko; b. Menyediakan ruang khas untuk pelawat-pelawat;	Semua

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; 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.	
7.4 Pemantauan Keselamatan Fizikal	
7.4.1 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; 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. c. Kawasan tempat larangan perlu ditutup dan dikunci setiap masa.	Semua

d. Peralatan rakaman/penyimpanan seperti kamera, video, perakam suara dan storan mudah alih adalah tidak dibenarkan dibawa masuk ke dalam kawasan larangan kecuali dengan kebenaran pegawai pengiring.	
7.5 Perlindungan Daripada Ancaman Fizikal Dan Persekitaran	
7.5.1 Kawalan Persekitaran	
Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: a. Merancang dan menyediakan pelan keseluruhan susun atur bilik server; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya sekali dalam setahun. Aktiviti	Semua

dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu;dan h. Akses kepada saluran riser hendaklah sentiasa berkunci.	
7.6 Bekerja Di Kawasan Selamat	
7.6.1 Kawalan Kawasan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; b. Memastikan kawasan yang mempunyai aset ICT dilengkapi dengan perlindungan keselamatan yang mencukupi seperti alat pencegah kebakaran dan sebagainya;	ICTSO, Penolong Pegawai Teknologi Maklumat
7.7 Clear Desk Dan Clear Screen	
7.7.1 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.	

7.8 Penempatan Dan Perlindungan Peralatan

7.8.1 Peralatan ICT

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

imbasan ke atas media storan yang digunakan; g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; i. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); j. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; k. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; l. Peralatan ICT yang hendak dibawa keluar dari premis MPKj, perlulah mendapat kelulusan ICTSO dan direkodkan bagi tujuan pemantauan; m. Peralatan ICT yang hilang hendaklah dilaporkan kepada pihak polis dan memaklumkan ke ICTSO dan Pegawai Aset untuk tindakan selanjutnya; n. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa; o. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran ICTSO;	

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

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

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

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

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

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

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.

7.9 Keselamatan Aset Di Luar Premis	
7.9.1 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 mengambilkira ciri-ciri keselamatan yang bersesuaian.	Semua
7.10 Media Storan	
7.10.1 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti notebook, komputer “desktop” dan lain-lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; c. Semua media storan perlu dikawal bagi mencegah dari	Semua

capaian yang tidak dibenarkan, kecurian dan kemusnahan; d. Semua media storan yang mengandungi data kritikal hendaklah disimpan tempat yang selamat; 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. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan i. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
7.10.2 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 diselenggaraoleh kakitangan atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;	Penolong Teknologi Maklumat dan Juruteknik

d. Menyemak dan menguji semua perkakasan sebelumdan selepas proses penyelenggaraan; e. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f. Semua penyelenggaraan yang melibatkan pihak ketiga mestilah mendapat kebenaran daripada ICTSO.	
7.10.3 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
7.10.4 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	Semua, Pegawai Aset

pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas darikawalan 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 pemeriksa hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

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

f. Pegawai aset jabatan yang dilantik 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; 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.	
7.11 Utiliti Sokongan	
7.11.1 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*	ICTSO, Penolong Pegawai Teknologi Maklumat, Juruteknik dan UPF

(UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan a. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	
7.12 Keselamatan Kabel	
7.12.1 Kabel	
Kabel bekalan kuasa dan telekomunikasi yang mambawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada lintasan gangguan atau kerosakan. 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 b. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	ICTSO, Penolong Pegawai Teknologi Maklumat, Juruteknik dan pihak ketiga
7.13 Penyelenggaraan Peralatan	
7.13.1 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Penolong Teknologi Maklumat dan Juruteknik

a. Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b. Memastikan perkakasan hanya boleh diselenggaraoleh 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 sebelumdan selepas proses penyelenggaraan; e. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f. Semua penyelenggaraan yang melibatkan pihak ketiga mestilah mendapat kebenaran daripada ICTSO.	
7.14 Pelupusan Yang Selamat Atau Penggunaan Semula Peralatan	
7.14.1 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 darikawalan MPKj. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan;	Semua, Pegawai Aset

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 pemeriksa hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

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

f. Pegawai aset jabatan yang dilantik 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 menyimpanperkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya;

ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti speaker dan mana- mana peralatan

yang berkaitan; iii. Memindah keluar dari MPKj mana-manaperalatan 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.	

A.8 KAWALAN TEKNOLOGI

8.1 Aset Mudah Alih

8.1.1 Peralatan ICT

Warga MPKj yang diberikan peralatan ICT hendaklah menjaga dan bertanggungjawab sepenuhnya ke atas peralatan ICT tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f. Pengguna mesti memastikan perisian antivirus di komputer dan komputer riba mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g. Penggunaan kata laluan untuk akses ke sistemkomputer adalah diwajibkan; h. Semua peralatan sokongan ICT hendaklah dilindungi	Semua

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 dan direkodkan bagi tujuan pemantauan;

l. Peralatan ICT yang hilang hendaklah dilaporkan kepada pihak polis dan memaklumkan ke ICTSO dan Pegawai Aset untuk tindakan selanjutnya;

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 tersebutsentiasa 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. Perkongsian data dan pencetak yang ingin dicapai oleh pengguna lain boleh dicapai menggunakan aplikasi "Log On" yang telah disediakan; v. Juruteknik yang bertanggungjawab perlu memastikan aktiviti peminjaman dan pemulangan peralatan ICT direkodkan dan menyemak peralatan yang dipulangkan berada dalam keadaan baik danlengkap;dan w. Pegawai yang bertanggungjawab mestilah memastikan peralatan ICT yang dibawa keluar tidak mengandungi maklumat kerajaan. Ia perlu disalin dan dihapuskan.	

8.2 Hak Capaian Istimewa

8.2.1 Hak Capaian

Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi

	Maklumat
8.2.3 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 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.	ICTSO, Penolong Pegawai Teknologi Maklumat

8.2.4 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a. Mengenal pasti identiti 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.	ICTSO, Penolong Pegawai Teknologi Maklumat
8.3 Sekatan Akses Maklumat	
8.3.1 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 dan keselamatan maklumat yang telah ditentukan; b. Setiap *Login/Logout* ke capaian sistem maklumat dan aplikasi	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

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.	
8.4 Capaian kepada kod sumber	
8.4.1 Prosedur Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; dan b. Akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan;	Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat
8.4.2 Media Perisian dan Aplikasi	
Source code sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

8.5 Pengesahan Kawalan Akses

8.5.1 Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a. Mengenal pasti identiti 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.	ICTSO, Penolong Pegawai Teknologi Maklumat

8.5.2 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	Semua

khusus; d. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f. Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g. 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 180 hari dalam tempoh setahun atau selepas tempoh masa yang bersesuaian; dan j. Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
8.5.3 Dasar 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;	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

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.	
8.6 Pengurusan Kapasiti	
8.6.1 Perancangan Kapasiti	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	ICTSO
8.7 Kawalan terhadap Perisian Hasad (*Malware)*	
8.7.1 Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, 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	ICTSO

bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
8.8 Pengurusan Rentanan Teknikal	
8.8.1 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* c. Menilai tahap kerentanan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan d. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat,

8.9 Pengurusan Konfigurasi

8.9.1 Kawalan Infrastruktur Rangkaian

Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh 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;	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

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); k. Memastikan kemudahan rangkaian WAN dan LAN tidak digunakan untuk kepentingan peribadi atau komersial; dan l. Memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah.	
8.9.2 Peralatan ICT	
Warga MPKj yang diberikan peralatan ICT hendaklah menjaga dan bertanggungjawab sepenuhnya ke atas peralatan ICT tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f. Pengguna mesti memastikan perisian antivirus di komputer dan	Semua

komputer riba mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;

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

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

i. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan.

j. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;

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

l. Peralatan ICT yang hendak dibawa keluar dari premis MPKj, perlulah mendapat kelulusan ICTSO dan direkodkan bagi tujuan pemantauan;

m. Peralatan ICT yang hilang hendaklah dilaporkan kepada pihak polis dan memaklumkan ke ICTSO dan Pegawai Aset untuk tindakan selanjutnya;

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

o. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpakebenaran ICTSO;

p. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Juruteknik untuk dibaik pulih dan tindakan

menyelesaikan masalah kerosakan secara sendiri adalah **SAMA SEKALI** tidak dibenarkan;

q. Sebarang pelekat selain bagi tujuan rasmi tidakdibenarkan. Ini bagi menjamin peralatan tersebutsentiasa berkeadaan baik;

r. Konfigurasi alamat IP tidak dibenarkan diubah daripadaalamat IP yang asal;

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

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

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

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 dipulangkanberada 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.

8.10 Pelupusan Maklumat	
Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat. Maklumat yang disimpan di dalam sistem informasi, peralatan dan mana-mana storan media perlu dihapuskan apabila tidak diperlukan. Kaedah penghapusan secara *secure deletion*. Kawalan prosedur pengendalian maklumat dan prosedur pengendalian media boleh digunakan bagi pemusnahan secara fizikal disamping menghapuskan maklumat yang terkandung di dalamnya.	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat/ Juruteknik
8.11 Melindungi Data (*Data Masking*)	
Data Masking perlu digunakan selaras dengan Akta Perlindungan Data Peribadi 2010 (PDPA 2010) dalam kawalan capaian dan polisi tajuk khusus lain yang berkaitan serta keperluan perkhidmatan dengan mengambil kira pertimbangan undang-undang.	Semua
8.12 Pencegahan Kebocoran Data	
Langkah-langkah perlindungan ketirisan data perlu diguna pakai untuk sistem, rangkaian dan peralatan yang melakukan proses, menyimpan dan menghantar maklumat sensitif.	Semua
8.12.1 Pertukaran Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b. Perjanjian 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	Semua

atau kerosakan semasa pemindahan keluar dari MPKj dan; d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	
8.13 Penduaan (*Backup*) Maklumat	
8.13.1 *Backup*	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat penduaan (*backup)* ke atas semua data kritikal dalam Sistem Aplikasi mengikut keperluan organisasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; 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.	Semua
8.14 Redundansi Pada Kemudahan Pemprosesan Maklumat	
8.14.1 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti notebook, komputer “desktop” dan lain-lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Semua

a. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-cirikeselamatan bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan mediastoran 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; e. Akses dan pergerakan media storan hendaklahdirekodkan; f. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; g. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagimengelakkan kehilangan data; h. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan i. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
8.14.2 *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; 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.	
8.15 Logging	
8.15.1 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. 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.	Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat, ICTSO

8.15.2 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
8.15.3 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; c. Kemudahan merekod dan maklumat log perlu dilindungi daripada 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	Penolong Pegawai Teknologi Maklumat

dengan satu sumber waktu yang dipersetujui.	
8.16 Aktiviti Pemantauan	
8.16.1 Pengauditan dan Forensik ICT	
ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT MPKj; 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.	ICTSO

8.17 Penyeragaman Waktu	
8.17.1 Penyeragaman Jam	
Waktu server dan peralatan ICT yang berpusat dan kritikal perlu diseragamkan dengan satu sumber waktu yang tunggal menggunakan Network Time Protocol (NTP) Server. Masa yang berkaitan dengan sistem pemprosesan maklumat ICT MPKj mestilah diseragamkan mengikut rujukan punca masa yang sama yang digunakan oleh organisasi. Ini untuk memastikan ketepatan masa log yang disimpan serta bertujuan untuk mengawal integriti log tersebut bagi kegunaan masa hadapan.	Penolong Pegawai Teknologi Maklumat/ Juruteknik
8.18 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa	
8.18.1 Hak Capaian	
a. 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
8.19 Pemasangan Perisian Pada Sistem Operasi	
8.19.1 Peralatan ICT	
Warga MPKj yang diberikan peralatan ICT hendaklah menjaga dan bertanggungjawab sepenuhnya ke atas peralatan ICT tersebut. 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	Semua

membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

c. Pengguna dilarang sama sekali menambah, menanggalatau mengganti sebarang perkakasan ICT yang telah ditetapkan;

d. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;

e. Pengguna adalah bertanggungjawab di atas kerosakanatau kehilangan peralatan ICT di bawah kawalannya;

f. Pengguna mesti memastikan perisian antivirus di komputer dan komputer riba mereka sentiasa aktif (*activated*) dandikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;

g. Penggunaan kata laluan untuk akses ke sistemkomputer adalah diwajibkan;

h. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan ataupengubahsuaian 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 dan direkodkan bagi tujuan pemantauan;

l. Peralatan ICT yang hilang hendaklah dilaporkan kepada pihak polis dan memaklumkan ke ICTSO dan Pegawai Aset untuk tindakan selanjutnya;

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 tanpakebenaran 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 tidakdibenarkan. Ini bagi menjamin peralatan tersebutsentiasa berkeadaan baik;

q. Konfigurasi alamat IP tidak dibenarkan diubah daripadaalamat 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. Perkongsian data dan pencetak yang ingin dicapai oleh pengguna lain boleh dicapai menggunakan aplikasi "Log On" yang telah disediakan;

v. Juruteknik yang bertanggungjawab perlu memastikan aktiviti

peminjaman dan pemulangan peralatan ICT direkodkan dan menyemak peralatan yang dipulangkanberada dalam keadaan baik danlengkap;dan w. Pegawai yang bertanggungjawab mestilah memastikan peralatan ICT yang dibawa keluar tidak mengandungi maklumat kerajaan. Ia perlu disalin dan dihapuskan.	
8.19.2 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
8.19.3 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 dapatmelindungi 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;	ICTSO, Penolong Pegawai Teknologi Maklumat

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	
8.20 Keselamatan Rangkaian	
8.20.1 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Penolong Pegawai Teknologi Maklumat; e. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan MPKj;	ICTSO, Penolong Pegawai Teknologi Maklumat

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.	
8.21 Keselamatan Pada Perkhidmatan Rangkaian	
8.21.1 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a. Mengenal pasti identiti atau lokasi bagi setiap pengguna yang dibenarkan; dan b. Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu	ICTSO, Penolong Pegawai Teknologi Maklumat

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.	
8.22 Pengasingan Dalam Rangkaian	
8.22.1 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklahdikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Penolong Pegawai Teknologi Maklumat; e. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan MPKj; f. Memasang *Internet Access Management* pada *Internet*	ICTSO, Penolong Pegawai Teknologi Maklumat

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	
8.23 Penapisan Web (Web Filtering)	
8.23.1 Kawalan Infrastruktur Rangkaian	
Memasang *Internet Access Management* (IAM) pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;	ICTSO, Penolong Pegawai Teknologi Maklumat
8.24 Penggunaan Kriptografi	
8.24.1 Enkripsi	
Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua

8.24.2 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
8.25 Keselamatan Kitar Hayat Pembangunan	
8.25.1 Keperluan Keselamatan Sistem Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan,sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; c. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telahditetapkan sebelum digunakan.	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat
8.26 Keperluan Keselamatan Aplikasi	
8.26.1 Keperluan Keselamatan Sistem Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan	ICTSO, Pegawai Teknologi Maklumat, Penolong

keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan,sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; c. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telahditetapkan sebelum digunakan.	Pegawai Teknologi Maklumat
8.26.2 Pengesahan Data *Input* dan *Output*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b. Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Penolong Pegawai Teknologi Maklumat
8.27 Prinsip Keselamatan Arkitektur Dan Kejuruteraan Sistem	
8.27.1 Keperluan Keselamatan Sistem Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: e. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan	ICTSO, Pegawai Teknologi Maklumat, Penolong

keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; f. Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan,sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; g. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan h. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telahditetapkan sebelum digunakan.	Pegawai Teknologi Maklumat
8.28 Kod Selamat (*Secure Coding*)	
8.28.1 Keperluan Keselamatan Sistem Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan,sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

output untuk memastikan data yang telah diproses adalah tepat; c. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telahditetapkan sebelum digunakan.	
8.29 Pengujian Keselamatan Dalam Pembangunan Dan Penerimaan	
8.29.1 Keperluan Keselamatan Sistem Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan,sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; c. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

d. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telahditetapkan sebelum digunakan.	
8.29.2 Pengesahan Data *Input* dan *Output*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b. Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Penolong Pegawai Teknologi Maklumat
8.30 Pembangunan Oleh Sumber Luar (Outsourced)	
8.30.1 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
8.31 Pengasingan Persekitaran Pembangunan, Pengujian Dan Produksi	
8.31.1 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	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

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 operasi dan rangkaian.	
8.32 Pengurusan Perubahan	
8.32.1 Pengendalian Prosedur	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan- arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua
8.32.2 Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara,	Semua

menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
8.33 Maklumat Untuk Aktiviti Pengujian	
8.33.1 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 a. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua
8.33.2 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;	ICTSO, Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat

b. Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan,sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; c. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telahditetapkan sebelum digunakan.	
8.33.3 Pengesahan Data *Input* dan *Output*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b. Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Penolong Pegawai Teknologi Maklumat
8.34 Perlindungan Keselamatan Maklumat Ketika Pengujian Audit	
8.34.1 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

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.
CDO	*Chief Digital Officer* Ketua Pegawai Digital 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*).

CERT	*Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT MPKj. 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.
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 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 (Perisian Hasad)	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
POLISI KESELAMATAN SIBER
MAJLIS PERBANDARAN KAJANG

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 yang terkandung di dalam Polisi Keselamatan Siber MPKj; dan

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

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....

( )

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) Pekeliling Bilangan 4 Tahun 2022 - Pengurusan Dan Pengendalian Insiden Keselamatan Siber Sektor Awam

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

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

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

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

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

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

– 23 Mei 2021;

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

viii. 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;

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

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

xi. 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;

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

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

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

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

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