DASAR KESELAMATAN ICT

TERBUKA **VERSI 3.6**

REKOD PINDAAN DOKUMEN

BIL.	VERSI DOKUMEN	TARIKH	MUKA SURAT	KETERANGAN PINDAAN
1.	2.0	22/4/2014	16, 17, 34, 35, 40, 43, 48 dan 54	• Kemaskini pada polisi ○ 020106 Pentadbir Pentadbir Rangkaian ○ 020107 Pentadbir Pangkalan Data ○ 020108 Pentadbir Web ○ 060302 Perlindungan Dari Mobile Code ○ 060403 Backup ○ 060801 Perkhidmatan Penyampaian ○ 0601101 Pengauditan dan Forensik ICT ○ 070301 Capaian Rangkaian ○ 080401 Kawalan Perubahan
2.	3.0	8/6/2016	13, 15, 19, 20, 24, 30, 31, 33, 36 dan 40.	• Kemaskini pada polisi ○ 010102: Penyebaran Dasar ○ 020101 Datuk Bandar ○ 020102 Ketua Pegawai Maklumat ○ 020107 Pentadbir Pangkalan Data ○ 020108 Pentadbir Web ○ 020109 Pengguna ○ Objektif bagi Perkara 04 Keselamatan Sumber Manusia ○ 050203 Media Storan ○ 050205 Penyelenggaraan ○ 050301 Kawalan Persekitaran ○ 060102 Kawalan Perubahan ○ 060401 Backup (Polisi Backup bagi versi 2.0 adalah 060403) ○ Pengeluaran bagi polisi 060401 Penduaan dan 060402

				Sistem Log ○ Pengeluaran 060703 *Bring Owned Device* ○ *Lampiran 2* ○ *Lampiran B*
3.	3.1	6/6/2017	16, Lampiran A	• Kemaskini pada polisi ○ 020102 Ketua Pegawai Maklumat ○ Surat Akuan Pematuhan Dasar Keselamatan ICT Majlis Bandaraya Petaling Jaya
4.	3.2	30/5/2019	22, 51 dan 52	• Kemaskini pada polisi ○ 020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga ○ 070201 Akaun Pengguna
5.	3.3	30/7/2020	53 dan 57	• Kemaskini pada polisi ○ 070501 Penetapan keperluan bagi had capaian sistem dan aplikasi; kemaskini daripada 3 kali percubaan kepada 5 kali percubaan ○ 070203 Penetapan had masa pengesahan daripada 2 minit kepada 5 minit.
6.	3.4	20/8/2021	27 dan 47	• Kemaskini pada polisi ○ 040501 Bertukar atau Tamat Perkhidmatan ○ 060902 Pengurusan Mel Elektronik (E-mail)
7	3.5	13.9.2021	Lampiran A Lampiran B	• Kemaskini pada Lampiran A dan B, pada link tidak diletakkan versi.
8	3.6	26.7.2024	25, 36, 40, 41, 45, 50, 51, 54, dan 64	• Penambahan bagi dasar baharu seperti berikut: ○ 030301 Kawalan Penghapusan Maklumat ○ 050401 Kawalan Pemantauan Keselamatan Fizikal

				○ 060201 Kawalan Pengurusan Konfigurasi ○ 060401 Keperluan Risikan Ancaman ○ 060801 Kawalan Penapisan Web ○ 061301 Kawalan Data Masking ○ 061401 Kawalan Pencegahan Kebocoran Data ○ 061601 Pemantauan Berterusan ○ 061701 Kawalan Keselamatan Pengkomputeran Awan ○ 061702 Penstoran Awan (Cloud Storage) ○ 080201 Kawalan Kod Selamat • Penukaran terma CIO kepada CDO

DASAR KESELAMATAN ICT MBPJ

TUJUAN

Tujuan dasar ini adalah untuk memaklumkan peraturan-peraturan yang perlu dipatuhi oleh semua warga Majlis Bandaraya Petaling Jaya (MBPJ) untuk menjaga keselamatan dan aset teknologi maklumat dan komunikasi (ICT). Dengan adanya peraturan ini adalah diharapkan semua pengguna di MBPJ sedar tentang tanggungjawab dan peranan mereka dalam melindungi aset ICT MBPJ. Oleh itu tahap keselamatan ICT dan langkah-langkah mengurangkan risiko ancaman dari dalam dan luar ke atas sistem dan infrastruktur ICT MBPJ dapat dipertingkatkan.

OBJEKTIF

Objektif Dasar Keselamatan ICT adalah seperti berikut:

a) Memastikan pengawalan dan pengurusan keselamatan ke atas perkakasan, perisian, aplikasi dan operasi komputer.
b) Dasar Keselamatan ICT MBPJ diwujudkan untuk menjamin kesinambungan urusan MBPJ dengan memimumkan kesan insiden keselamatan ICT.
c) Mengelakkan berlakunya percanggahan data dan maklumat di MBPJ.
d) Memastikan aset ICT terlindung daripada ancaman pencerobohan/penggodaman, kecurian data, serangan virus dan penafian perkhidmatan.
e) Mencegah kes-kes penyalahgunaan serta kehilangan aset ICT MBPJ

PENYATAAN 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 dimana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Terdapat empat (4) komponen asas keselamatan ICT:

a) Melindungi maklumat rahsia rasmi dan maklumat rasmi Majlis Bandaraya Petaling Jaya

dari capaian tanpa kuasa yang sah.

b) Menjamin setiap maklumat adalah tepat dan sempurna.
c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna.
d) Memastikan akses hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat dari sumber-sumber yang sah.

DKICT MBPJ 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 akses tanpa kebenaran.
b) **Integriti** – Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan.
c) **Tidak boleh disangkal** – Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.
d) **Kesahihan** – Data dan maklumat hendaklah dijamin kesahihannya.
e) **Ketersediaan** – Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

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

a) Perkakasan – Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan agensi. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya.
b) Perisian – Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian,

sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada agensi.

c) Perkhidmatan – Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh :
   i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain.
   ii. Sistem halangan akses seperti sistem kad akses.
   iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

d) Data atau Maklumat – Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif agensi. Contoh : Sistem dokumentasi, prosedur operasi, rekod-rekod agensi, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain.

e) Manusia – Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian agensi bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

Dasar ini adalah terpakai oleh semua pengguna di MBPJ termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT MBPJ.

PRINSIP-PRINSIP

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

a) Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar perlu mengetahui sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

b) Hak akses minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk

membaca dan/atau melibat sahaja. Kelulusan adalah perlu untuk 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.

c) **Akauntabiliti**

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

d) Pengasingan

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

e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, router, firewall dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau audit trail.

f) Pematuhan

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

g) Pemulihan

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

h) Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

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

MBPJ 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 MBPJ termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan yang lain.

MBPJ 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.
MBPJ perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko yang berlaku dan 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.

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

Perkara 01 : PEMBANGUNAN DAN PENYELENGGARAAN DASAR

010101	**Perlaksanaan Dasar**	**Tanggungjawab**
	Pelaksanaan dasar ini akan dijalankan oleh Datuk Bandar MBPJ dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO), Pegawai Keselamatan MBPJ , Pengurus Teknikal dan Pentadbir Sistem dan semua Penolong Pegawai Teknologi Maklumat (PPTM).	Datuk Bandar
010102	**Penyebaran Dasar**	
	Dasar ini perlu disebarkan kepada semua pengguna di MBPJ (termasuk kakitangan, pembekal dan pakar runding dan lain-lain).	ICTSO
010103	**Penyelenggaraan Dasar**	
	Dasar keselamatan ICT Kerajaan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT MBPJ: a) Kenal pasti dan tentukan perubahan yang diperlukan; b) Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Kecil (JKICT) MBPJ atau setara; c) Perubahan yang telah dipersetujui oleh JKICT dimaklumkan kepada semua pengguna; dan d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun oleh ICTSO.	ICTSO
010104	**Pengecualian Dasar**	
	Dasar keselamatan ICT MBPJ adalah terpakai kepada semua pengguna ICT MBPJ dan tiada pengecualian diberikan.	Semua

Perkara 02 : KESELAMATAN ORGANISASI

Infrastruktur Organisasi Keselamatan

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

020101	**Datuk Bandar**	
	Datuk Bandar MBPJ adalah merupakan Pengurusan Tertinggi yang bertanggungjawab melantik Ketua Pegawai Digital (CDO). a) Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi. b) Meluluskan dasar-dasar yang berkaitan dengan keselamatan organisasi.	Datuk Bandar
020102	**Ketua Pegawai Digital (CDO)**	
	Timbalan Datuk Bandar merupakan Ketua Pegawai Digital (CDO). Peranan dan tanggungjawab beliau adalah seperti berikut: a) Membantu Datuk Bandar dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b) Menentukan keperluan keselamatan ICT; c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT serta pengurusan risiko dan pengauditan d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MBPJ.	CDO

020103	**Pegawai Keselamatan ICT (ICTSO)**	
	Pengarah Teknologi Maklumat merupakan Pegawai Keselamatan ICT (ICTSO). Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a) Mengurus keseluruhan program-program keselamatan ICT MBPJ. b) Menguatkuasakan Dasar Keselamatan ICT MBPJ c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MBPJ kepada semua pengguna. d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keperluan ICT MBPJ. e) Menjalankan pengurusan risiko. f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian. h) Melaporkan insiden keselamatan ICT kepada NACSA dan memaklumkannya kepada CDO. i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperlakukan langkah-langkah baik pulih dengan segera. j) Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT MBPJ. k) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	ICTSO

020104	**Pengurus Teknikal**	
	Pegawai Teknologi Maklumat dan Penolong Pegawai Teknologi Maklumat (PPTM) yang dilantik oleh ICTSO adalah merupakan Pengurus Teknikal MBPJ. Peranan dan tanggungjawab Pengurus Teknikal adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MBPJ. b) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MBPJ. c) Menentukan kawalan akses semua pengguna terhadap aset ICT MBPJ. d) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO. e) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MBPJ.	Pengurus Teknikal
020105	**Pentadbir Sistem**	
	Pegawai Teknologi Maklumat dan Penolong Pegawai Teknologi Maklumat (PPTM) yang dilantik oleh ICTSO adalah merupakan Pentadbir Sistem ICT MBPJ. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut: Mengambil tindakan yang bersesuaian denagn segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas. a) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT MBPJ. b) Memantau aktiviti capaian harian pengguna. c) Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta. d) Menyimpan dan menganalisis rekod jejak audit. e) Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	Pentadbir Sistem

020106	**Pentadbir Rangkaian**	
	Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut: a) Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di MBPJ beroperasi sepanjang masa; b) Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; c) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; d) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; e) Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; f) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian MBPJ secara tidak sah seperti melalui peralatan modem dan dial-up; dan g) Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian.	Pentadbir Rangkaian
020107	**Pentadbir Pangkalan Data**	
	Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut: a) Melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data. b) Memastikan pangkalan data boleh digunakan pada setiap masa. c) Melaksanakan pemantauan dan penyenggaraan yang berterusan ke atas pangkalan data. d) Melaksanakan proses *backup* dan *restore* ke atas pangkalan data. e) Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data	Pentadbir Pangkalan Data

	dan proses pengemaskinian data dilaksanakan dengan teratur. f) Melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip DKICT. g) Melaksanakan proses pembersihan data (*housekeeping*) di dalam pangkalan data. h) Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.	
020108	**Pentadbir Web**	
	Peranan dan tanggungjawab Pentadbir Laman Web adalah seperti berikut: a) Memastikan kandungan laman web sentiasa sahih dan terkini. b) Memantau prestasi capaian dan menjalankan penilaian prestasi untuk memastikan akses yang lancar. c) Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman. d) Menghadkan capaian Pentadbir Laman Web bahagian ke web server. e) Mengasingkan kandungan dan aplikasi atas talian untuk capaian secara intranet dan internet ke portal MBPJ. f) Memastikan data-data SULIT tidak boleh disalin atau dicetak oleh orang yang tidak berhak. g) Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi. h) Melaksanakan housekeeping keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di web server. i) Melaksanakan proses *backup* dan *restore* secara berkala. j) Melaporkan sebarang pelanggaran keselamatan laman sesawang kepada ICTSO.	Pentadbir Laman Web

020109	**Pengguna**	
	Peranan dan tanggungjawab pengguna adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MBPJ. b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya. c) Mematuhi tapisan keselamatan. d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat MBPJ. e) Melaksanakan langkah-langkah perlindungan seperti berikut: i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. ii. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa. iii. menentukan maklumat sedia untuk digunakan. f) Menjaga kerahsiaan kata laluan. g) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. h) Memberi perhatian kepada maklumat terperingkat terutama semasa.	Semua

Pihak Ketiga Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga		
020201	**Keperluan Keselamatan Kontrak dengan Pihak Ketiga**	
	a) Dasar Keselamatan ICT hendaklah dibaca, difahami dan dipatuhi. b) Penjagaan kerahsiaan maklumat Kerajaan yang meliputi maklumat terperingkat terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan. c) Penjagaan kerahsiaan kata laluan. d) Maklumat berkaitan hendaklah tepat dan lengkap dari semasa ke semasa. e) Penjagaan kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum. f) Mengetahui dan memahami implikasi keselamatan ICT kesan daripada tindakannya. g) Pihak Ketiga yang menggunakan perkhidmatan ICT dan mempunyai peranan seperti berikut: i. Tapisan keselamatan dilaksanakan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat. ii. Pelaksanaan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat. iii. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT sebagaimana Lampiran 2.	CDO, ICTSO, Pengurus Teknikal, Pentadbir Sistem, Pentadbir Rangkaian, Pentadbir Pangkalan Data, Pihak Ketiga

Perkara 03 : KAWALAN DAN PENGELASAN ASET

Akauntabiliti Aset

Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MBPJ.

030101	**Inventori Aset**	
	Semua aset ICT MBPJ hendaklah direkodkan. Ini termasuklah mengenai pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pengurus Teknikal ICT

Pengelasan dan Pengendalian Maklumat

Objektif: memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

030201	**Pengelasan Maklumat**	
	Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a) Rahsia Besar b) Rahsia c) Sulit d) Terhad e) Terbuka	Semua

030202	**Pengendalian Maklumat**	
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa. c) Menentukan maklumat sedia untuk digunakan. d) Menjaga kerahsiaan kata laluan. e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. f) Memberi perhatian kepada maklumat terperingkat penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan. g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua
	Penghapusan Maklumat Objektif: Mencegah pendedahan maklumat sensitif yang tidak sewajarnya dan mematuhi undang-undang, peraturan dan keperluan perjanjian dalam penghapusan maklumat.	
030301	**Kawalan Penghapusan Maklumat**	
	Maklumat yang disimpan di dalam sistem informasi, peralatan dan mana-mana storan media perlu dihapuskan apabila tidak diperlukan.	Semua

Perkara 04 : KESELAMATAN SUMBER MANUSIA

KESELAMATAN ICT DALAM TUGAS SEHARIAN

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

040101	**Tanggungjawab Keselamatan Semasa Dalam Perkhidmatan**	
	Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, di rekod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.	Semua
040102	**Terma dan Syarat Perkhidmatan**	
	Semua warga MBPJ yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa.	Semua
040103	**Perakuan Akta Rahsia Rasmi**	
	Warga MBPJ yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Semua

Menangani Insiden Keselamatan ICT Objektif : Meminimumkan kesan insiden keselamatan ICT.		
040201	**Pelaporan Insiden**	
	Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera iaitu: 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. e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. Rujukan: Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan ICT”	**Pengurus Teknikal**
Pendidikan Objektif: Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT		
040301	**Program Kesedaran Keselamatan ICT**	
	Setiap pengguna di MBPJ perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT MBPJ.	ICTSO

Tindakan Tatatertib Objektif: Meningkat kesedaran dan pematuhan ke atas Dasar Keselamatan ICT MBPJ.		
040401	**Pelanggaran Dasar**	
	Pelanggaran Dasar Keselamatan ICT MBPJ akan dikenakan tindakan tatatertib.	CDO
Bertukar atau Tamat Perkhidmatan Objektif: Memastikan pertukaran atau tamat perkhidmatan pegawai dan kakitangan Majlis Bandaraya Petaling Jaya, pembekal dan pihak-pihak lain yang berkepentingan diuruskan dengan teratur.		
040501	**Bertukar atau Tamat Perkhidmatan**	
	a) Memastikan semua aset ICT dikembalikan kepada jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan atau meminda semua kebenaran capaian ke atas maklumat, kemudahan proses maklumat dan semua akses berkaitan mengikut peraturan yang ditetapkan oleh MBPJ dan/atau terma perkhidmatan.	Semua

Perkara 05 : KESELAMATAN FIZIKAL

Keselamatan Kawasan

Objektif : Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.

050101	**Perimeter Keselamatan Fizikal**	
	Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah 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) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan. c) Memperkukuhkan dinding dan siling. d) Memasang alat penggera atau kamera CCTV e) Menghadkan jalan keluar masuk. f) Mengadakan kaunter kawalan. g) Menyediakan tempat atau bilik khas untuk pelawat. h) Mewujudkan perkhidmatan kawalan keselamatan	ICTSO, CDO
050102	**Kawalan Masuk Fizikal**	
	a) Setiap pengguna MBPJ hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas. b) Setiap pelawat boleh mendapat Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan. c) Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pengguna berhenti atau bersara. d) Kehilangan pas mestilah dilaporkan dengan segera. e) Hanya pengguna yang diberi kebenaran sahaja boleh	Semua

	mencapai atau menggunakan aset ICT MBPJ.	
050103	**Kawasan Larangan**	
	a) Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di MBPJ adalah bilik Datuk Bandar, Timbalan Datuk Bandar, Timbalan Setiausaha Bandaraya, bilik fail, bilik handheld dan bilik server ICT. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja. Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan bila perlu. b) Pihak ketiga adalah dilarang sama sekali untuk memasuk kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai. c) Semua penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	Pentadbir Sistem
	Keselamatan Peralatan Objektif : Melindung peralatan dan maklumat.	
050201	**Perkakasan**	
	Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu: a) Setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna. b) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. c) Setiap pengguna adalah bertanggungjawab di atas	Semua

	kerosakan atau kehilangan perkakasan ICT di bawah kawalannya. d) Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada Pengurus Teknikal.	
050202	**Dokumen**	
	Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi: a) Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin. b) Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen. c) Menggunakan penyulitan (encryption) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik. d) Memastikan dokumen yang mengandungi bahan atau maklumat sensitif diambil segera dari pencetak.	Semua
050203	**Media Storan**	
	Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat : a) Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat. b) Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja. c) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	Semua

	d) Pergerakan media storan hendaklah direkodkan.	
050204	**Kabel**	
	Kabel komputer hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan. b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan. c) Melindungi laluan pemasangan kabel sepenuhnya.	Semua
050205	**Penyelenggaraan**	
	a) Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti. b) Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan. c) Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja. d) Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan. e) Semua penyelenggaraan mestilah mendapat kebenaran daripada ICTSO. f) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pengurus Teknikal, ICTSO

050206	**Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat**	
	Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan: a) Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan. b) Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan dan mengikut polisi yang ditetapkan oleh Unit Teknologi Maklumat (UTM) Rujukan: Prosedur penggunaan sistem dan perkakasan komputer untuk Majlis Bandaraya Petaling Jaya.	Semua
050207	**Peralatan di luar Premis**	
	Bagi perkakasan yang dibawa keluar dari premis MBPJ, langkah-langkah keselamatan hendaklah diadakan dengan mengambilkira risiko yang wujud di luar kawasan MBPJ: a) Peralatan perlu dilindungi dan dikawal sepanjang masa. b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua
050208	**Pelupusan**	
	Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MBPJ.	Pegawai Aset

050209	**Clear Desk dan Clear Screen**	
	Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakkan, kecurian atau kehilangan. Clear Desk bermaksud tidak meninggalkan bahan-bahan yang sensitive terdedah sama ada atas meja warga atau di paparan skrin apabilawarga tidak berada di tempatnya: a) Gunakan kemudahan password screen saver atau log keluar apabila meninggalkan komputer. b) Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci.	Semua
050210	**Penggunaan Thumb/Pen drive**	
	Penggunaan thumb/pen drive adalah keperluan kepada pengguna untuk menyimpan data/maklumat secara sementara/kekal. Terdapat beberapa perkara yang perlu diberi perhatian mengenai penggunaan thumb/pen drive: a) Pemohon perlu mendapat kebenaran daripada Ketua Jabatan terlebih dahulu. b) Spesifikasi kerja perlu dinyatakan supaya penggunaan thumb/pen drive tidak disalahgunakan. c) Pemohon dan Ketua Jabatan bertanggungjawab sepenuhnya berkenaan penggunaan thumb/pen drive tersebut. d) Semua maklumat yang ada didalam thumb/pen drive berikut yang berkaitan dengan segala maklumat Jabatan jika hilang adalah tanggungjawab sepenuhnya oleh pemohon. e) Penggantian bagi kehilangan thumb/pen drive akibat kecuaian TIDAK akan dilayan	Semua

Keselamatan Persekitaran

Objektif : Melindungi aset ICT MBPJ dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan

050301	**Kawalan Persekitaran**	
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pengarah Teknologi Maklumat. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti. b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan. c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan. d) 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.	Semua

050302	**Bekalan Kuasa**	
	a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT. b) Peralatan sokongan seperti UPS (*Uninterruptable Power System*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan. c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Seksyen Infrastruktur dan Teknikal ICT
	Pemantauan Keselamatan Fizikal Objektif: Mengesan dan menghalang akses fizikal yang tidak sah.	
050401	**Kawalan Pemantauan Keselamatan Fizikal**	
	Premis fizikal perlu dipantau menggunakan sistem pengawasan (contoh: pengawal, penggera pencerobohan, sistem pemantauan video seperti CCTV, sistem aplikasi pengurusan maklumat keselamatan fizikal atau mana-mana yang bersesuaian.) Akses ke lokasi kritikal perlu dipantau secara berterusan bagi mengesan akses yang tidak sah atau tingkah laku yang mencurigakan.	CDO, ICTSO
	Keselamatan Dokumen Objektif: Melindungi maklumat MBPJ dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
050501	**Keselamatan Sistem Dokumentasi**	
	Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan. b) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada. c) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar. d) Pergerakan fail dan dokumen hendaklah direkodkan dan	Semua

	perlulah mengikut prosedur keselamatan. e) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan. f) Pelupusan dokumen hendaklah mengikut Prosedur Keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara. g) Menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang disediakan, disimpan dan dihantar secara elektronik.	

Perkara 06 : PENGURUSAN OPERASI DAN KOMUNIKASI

Pengurusan Prosedur Operasi

Objektif : Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat dari sebarang ancaman atau gangguan.

060101	**Pengendalian Prosedur**	
	a) Semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, 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. c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Seksyen Pentadbiran & QRD
060102	**Kawalan Perubahan**	
	a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada Ketua Pegawai Maklumat. b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan. c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja ataupun tidak.	Semua

060103	**Prosedur Pengurusan Insiden**	
	Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan; prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut: a) Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran. b) Menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan. c) Menyimpan jejak audit dan memelihara bahan bukti. Menyediakan tindakan pemulihan segera.	ICTSO
060104	**Pengasingan Tugas dan Tanggungjawab**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyenggara, dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	CDO

Kawalan Pengurusan Konfigurasi Objektif: Memastikan peralatan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul dengan aturan keselamatan yang diperlukan dan konfigurasi tidak diubah oleh perubahan yang tidak sah dan tidak betul. Perkara yang perlu dipatuhi termasuklah mewujudkan, mendokumenkan, melaksana, memantau dan mengkaji semula konfigurasi keselamatan bagi peralatan, perisian, perkhidmatan dan rangkaian.		
060201	**Kawalan Pengurusan Konfigurasi**	
	Perkara yang perlu dipatuhi termasuklah mewujudkan, mendokumenkan, melaksana, memantau dan mengkaji semula konfigurasi keselamatan bagi peralatan, perisian, perkhidmatan dan rangkaian.	ICTSO, Pengurus Teknikal, Pentadbir Sistem, Pentadbir Rangkaian
Perancangan dan Penerimaan Sistem Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.		
060301	**Perancangan Kapasiti**	
	Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem dan ICTSO
060302	**Penerimaan Sistem**	
	Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui	Pentadbir Sistem dan ICTSO

Risikan Ancaman (*Threat Intelligence*)

Objektif: Memberi kesedaran tentang persekitaran ancaman organisasi supaya tindakan mitigasi yang sewajarnya dapat diambil.

060401	**Keperluan Risikan Ancaman**	
	Maklumat mengenai ancaman sedia ada atau baharu hendaklah dikumpulkan daripada sumber luaran dan dalaman, dan dianalisis untuk: a) Memudahkan tindakan sewajarnya diambil untuk mencegah ancaman daripada menyebabkan kemudaratan kepada organisasi; dan b) Mengurangkan kesan ancaman tersebut. Aktiviti perisikan ancaman hendaklah termasuk: a) Mengenal pasti, memeriksa dan memilih sumber maklumat dalaman dan luaran yang diperlukan dan sesuai untuk melaksanakan tindakan yang diperlukan berdasarkan maklumat perisikan ancaman. b) Memproses dan menganalisis maklumat untuk memahami bagaimana ia berkaitan dan bermakna kepada MBPJ. c) Berkomunikasi dan berkongsi kepada individu yang berkaitan dalam format yang boleh difahami. Perisikan ancaman hendaklah dianalisis dan kemudian digunakan: a) Dengan melaksanakan proses untuk memasukkan maklumat yang dikumpulkan dari sumber perisikan ancaman ke dalam proses pengurusan risiko keselamatan maklumat MBPJ. b) Sebagai input tambahan kepada kawalan pencegahan dan pengesanan teknikal seperti firewall, intrusion detection system, atau penyelesaian anti perisian hasad. c) Sebagai input kepada proses dan teknik Penilaian Tahap Keselamatan.	ICTSO, Pengurus Teknikal, Pentadbir Sistem

Perisian Berbahaya

Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya,

060501	**Perlindungan dari Perisian Berbahaya**	
	a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) mengikut prosedur penggunaan yang betul dan selamat. b) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya. c) Mengemas kini pattern anti virus setiap minggu. d) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat.	Semua
060502	**Perlindungan dari Mobile Code**	
	a) Penggunaan mobile code yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan. b) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, IDS dan IPS mengikut prosedur penggunaan yang betul dan selamat; c) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa; d) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; e) Mengemas kini pattern antivirus dengan yang terkini; f) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; g) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya h) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya.	Semua

	i) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan. j) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
Housekeeping Objektif : Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa		
060601	**Penduaan (Backup)**	
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, backup seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Backup hendaklah direkodkan dan disimpan di off site, di antaranya adalah: a) Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru. b) Membuat backup ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat. c) Menguji sistem backup sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan. d) Backup hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan backup bergantung pada tahap kritikal maklumat. e) Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat.	Semua

Pengurusan Rangkaian

Objektif : Melindungi maklumat dalam rangkaian dan infrastruktur sokongan

060701	**Kawalan Infrastruktur Rangkaian**	
	Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan: 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) Semua peralatan mestilah melalui proses Factory Acceptance Check (FAC) semasa pemasangan dan konfigurasi. e) Firewall hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem. f) Semua trafik keluar dan masuk hendaklah melalui firewall di bawah kawalan MBPJ. g) Semua perisian sniffer atau network analyzer adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO. h) Memasang perisian Intrusion Detection System (IDS) atau Intrusion Preventive System (IPS) bagi mengesan/menghalang sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MBPJ. i) Sebarang penyambungan rangkaian yang bukan dibawah kawalan MBPJ hendaklah mendapat kebenaran ICTSO. j) Semua pengguna hanya dibenarkan menggunakan rangkaian MBPJ sahaja.	Unit Teknologi Maklumat (UTM)

	k) Penggunaan modem atau teknologi lain seperti 3G Broadband perlu mendapatkan kebenaran ICTSO l) Memastikan keperluan perlindungan ICT adalah bersesuaian.	
Penapisan Web (*Web Filtering*) Objektif: Untuk melindungi sistem daripada terjejas oleh perisian hasad dan untuk menghalang akses kepada sumber web yang tidak dibenarkan.		
060801	**Kawalan Penapisan Web**	
	Memasang Web Content Filtering pada Internet Gateway atau kawalan capaian Internet yang bersesuaian untuk menyekat aktiviti/capaian laman web yang dilarang.	ICTSO, Pengurus Teknikal, Pentadbir Rangkaian
Pengurusan Media Objektif: Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal. Media bermaksud sebarang bahan termasuk pita, CD, DVD, filem, disket, thumb drive, laptop, hard disk, surat, dokumen dan manual		
060901	**Penghantaran dan Pemindahan**	
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	Semua
060902	**Prosedur Pengendalian Media**	
	a) Melabelkan semua media mengikut tahap sensitivity sesuatu maklumat. b) Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja. c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan. d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan. e) Menyimpan semua media di tempat yang selamat. f) Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	Semua

060903	**Keselamatan Sistem Dokumentasi**	
	a) Memastikan sistem penyampaian dokumentasi mempunyai ciriciri keselamatan b) Menyediakan dan memantapkan keselamatan sistem dokumentasi c) Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	Semua
	Keselamatan Komunikasi Objektif : Melindungi aset ICT melalui sistem komunikasi yang selamat	
061001	**Internet**	
	a) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan. b) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan. c) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet. d) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak terpelihara. e) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MBPJ. f) 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 Ketua Jabatan terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan **Rujukan:** Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara	Semua

	Penggunaan Internet dan Mel Elektronik di Agensi Kerajaan”	
061002	**Mel Elektronik**	
	a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh MBPJ sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang. b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh MBPJ. c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan. d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul. e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi dua (2) megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan. f) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui. g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel. h) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan. i) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan. j) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat Rujukan Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatcara Penggunaan Internet dan Mel Elektronik di Agensi Kerajaan”	Semua

061003	***Bring Your Owned Device (BYOD)***	
	BYOD adalah peralatan mudah alih persendirian seperti telefon pintar, *tablet* dan *laptop* yang digunakan untuk tujuan rasmi. Maklumat lanjut mengenai *BYOD* boleh merujuk kepada polisi berkaitan *Bring Your Owned Device (BYOD)* seperti di Lampiran B.	Semua
Pengurusan Penyampaian Perkhidmatan Pihak Ketiga Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.		
061101	**Perkhidmatan Penyampaian**	
	Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi,dilaksanakan dan diselenggarakan oleh pihak ketiga; b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua
Pengurusan Pertukaran Maklumat Objektif: Memastikan keselamatan pertukaran maklumat dan perisian Antara MBPJ/agensi dan mana-mana entiti luar terjamin.		
061201	**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 MBPJ dengan pihak luar;	Semua

	c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan,penyalahgunaan atau kerosakan semasa pemindahan keluar dari MBPJ; dan d) Maklumat yang terdapat dalam e-mel perlu dilindungi sebaik-baiknya.	
061202	**Pengurusan Mel Elektronik (E-mail)**	
	Penggunaan e-mel di MBPJ 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"; "Garis Panduan Penggunaan Mel Elektronik MBPJ" dan mana-mana undang bertulis yang berkuat kuasa. Di antara prosedur-prosedur pengurusan e-mel termasuk: a) Akaun atau alamat e-mel yang diperuntukkan oleh MBPJ sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang. b) Permohonan E-mel hendaklah dibuat dengan melengkapkan MForm secara dalam talian kepada Unit Teknologi Maklumat, MBPJ. c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan. d) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan. e) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui. f) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel.	

Data Masking

Objektif: Untuk mengehadkan pendedahan data sensitif termasuk maklumat data peribadi (Personal Identifiable Information (PII)), dan mematuhi keperluan undang-undang, peraturan dan perjanjian.

061301	**Kawalan *Data Masking***	
	Data Masking perlu digunakan selaras dengan polisi tajuk khusus dalam kawalan capaian dan polisi tajuk khusus lain yang berkaitan serta keperluan perkhidmatan dengan mengambil kira pertimbangan undang-undang.	ICTSO, Pengurus Teknikal, Pentadbir Sistem, Pentadbir Pangkalan Data

Pencegahan Kebocoran Data (*Data Leakage Prevention*)

Objektif: Mengesan dan mencegah pendedahan dan pengekstrakan maklumat yang tidak dibenarkan oleh individu atau sistem.

061401	**Kawalan 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

Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak-Pihak Lain Yang Terlibat

Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal, pakar runding dan pihak-pihak lain yang terlibat.

061501	**Perkhidmatan Penyampaian**	
	Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Memasukkan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat. b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat	Semua

	perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa. Pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyenggara dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	

Aktiviti Pemantauan

Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, pengesanan tingkah laku anomali dan potensi kepada insiden keselamatan maklumat.

061601	**Pemantauan Berterusan**	
	Pemantauan kepada rangkaian, sistem dan aplikasi perlu dilaksanakan secara berterusan mengikut tempoh yang bersesuaian. Perkara-perkara yang memerlukan pemantauan termasuklah tetapi tidak terhad kepada: a) Trafik keluar masuk rangkaian, sistem dan aplikasi; b) Capaian kepada sistem, server, perkakasan rangkaian, sistem pemantauan, sistem aplikasi yang kritikal dan lain-lain. c) Tahap pentadbir sistem dan fail konfigurasi rangkaian; d) Log dari peralatan/perisian keselamatan (contoh: Antivirus, IDS, IPS, firewall dan lain-lain). e) Log kejadian berkaitan aktiviti sistem dan rangkaian. f) Penggunaan kod sumber yang disahkan tidak disalah guna. g) Penggunaan sumber (contoh: CPU, hard disks, memory dan bandwith).	ICTSO, Pengurus Teknikal, Pentadbir Sistem ICT, Pentadbir Rangkaian

061602	**Pengauditan dan Forensik ICT**	
	ICTSO mestilah bertanggungjawab merekod dan menganalisa perkara-perkara berikut: a) Sebarang percubaan pencerobohan kepada sistem ICT MBPJ; 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 bandwith rangkaian; g) Aktiviti penyalahgunaan akaun e-mel; h) Aktiviti penukaran alamat IP (IP address) selain daripada yang telah diperuntukkan tanpa kebenaran PSU (KnR); dan i) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian.	ICTSO

061603	**Sistem Log**	
	Fungsi-fungsi sistem log adalah seperti berikut:: a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c) Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	Unit Teknologi Maklumat (UTM)
061604	**Pemantauan Log**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisa dan diambil tindakan sewajarnya; dan f) Masa yang berkaitan dengan sistem pemprosesan maklumat dalam MBPJ atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.	Unit Teknologi Maklumat (UTM)

Perkhidmatan Awan (*Cloud Services*)

Objektif : Memastikan keselamatan dan kawalan maklumat bagi perolehan, penggunaan, pengurusan dan penamatan/pelucutan daripada perkhidmatan awan yang bergantung kepada sumber pengkomputeran seperti pelayan, storan, pangkalan data, rangkaian dan perisian yang boleh dicapai menerusi Internet.

061701	**Kawalan Keselamatan Pengkomputeran Awan**	
	Penggunaan aplikasi dan kemudahan infrastruktur pengkomputeran awan (cloud computing) tidak dibenarkan - sama sekali kecuali pengkomputeran awan yang dibangunkan, dilanggan dan dibenarkan oleh pihak Kerajaan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa. Secara asasnya maksud pengkomputeran awan yang dibangunkan dan dibenarkan oleh pihak Kerajaan adalah perkhidmatan pengkomputeran awan yang dimiliki, diuruskan atau dikendalikan oleh pihak Kerajaan sendiri berdasarkan kepada prinsip, penilaian dan keperluan keselamatan siber secara komprehensif dan strategik melibatkan teknologi, manusia dan proses. Ia bertujuan agar perkhidmatan pengkomputeran awan tersebut memenuhi objektif keselamatan, hala tuju bisnes serta keperluan peraturan dan undang-undang yang berkuat kuasa.	Semua
061702	**Penstoran Awan (*Cloud Storage*)**	
	Maklumat yang terlibat dalam transaksi dalam pengkomputeran awan perlu dilindungi daripada aktiviti penipuan dan pendedahan serta pengubahsuaian yang tidak dibenarkan. Penstoran awan ini tertakluk kepada perkhidmatan awan yang dilanggan dan dibenarkan oleh pihak Kerajaan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Dokumen terperingkat yang disimpan di public cloud storage hendaklah menggunakan kaedah enkripsi terlebih dahulu sebelum dimuat naik; b) Setiap maklumat terperingkat yang disimpan di atas talian perlu mematuhi Arahan Keselamatan; dan	Semua

	c) 3. Bahan rasmi perlu mendapat kelulusan Ketua Jabatan sebelum dimuat naik ke penstoran awan.	

Perkara 07 : KAWALAN CAPAIAN

Dasar Kawalan Capaian

Objektif : Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT MBPJ

070101 Keperluan Dasar

	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada.	Unit Teknologi Maklumat (UTM)

Pengurusan Capaian Pengguna

Objektif : Mengawal capaian pengguna ke atas aset ICT MBPJ

070201 Akaun Pengguna

	Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: a) Permohonan penggunaan sistem mestilah diisi melalui Sistem mForm MBPJ b) Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan. c) Akaun pengguna mestilah unik d) Akaun pengguna yang diwujud pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu. e) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan. f) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang. g) Pentadbir sistem ICT boleh membeku dan menamatkan	Pentadbir ICT, Semua

	akaun pengguna atas sebab-sebab berikut : i. Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam dalam tempoh waktu melebihi 90 hari ii. Bertukar bidang tugas kerja.	
070202	**Jejak Audit**	
	Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi: a) Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan. b) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya. c) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Pentadbir sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan ,pemalsuan dan pengubah suaian yang tidak dibenarkan.	Pentadbir Sistem
070203	**Pengurusan Kata Laluan**	
	Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MBPJ 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 lapan (8) aksara dengan gabungan antara huruf dan nombor (alphanumerik);	Semua

	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 gunasama; f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g) Disarankan membuat pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i) Disarankan had masa pengesahan adalah selama lima (5) minit dan selepas had itu, sesi ditamatkan; j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
070204	**Hak Capaian (Privilege)**	
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas	Pentadbir SIstem
070205	**Sistem Maklumat dan Aplikasi**	
	Capaian sistem dan aplikasi di MBPJ adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi: a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan. b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini. c) Memaparkan notis amaran pada skrin komputer	Unit Teknologi Maklumat (UTM)

	pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan.	
Kawalan Capaian Rangkaian Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.		
070301 Capaian Rangkaian		
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MBPJ, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaiannya; dan c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Rangkaian
070302 Capaian Internet		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan internet di MBPJ hendaklah dipantau secara berterusan oleh BTM bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan malicious code, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MBPJ. b) Kaedah Content Filtering mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan. c) Penggunaan proksi (sekiranya ada) yang telah ditetapkan oleh MBPJ bagi mengawal akses Internet mengikut fungsi kerja dan mematuhi pekeliling semasa yang dikeluarkan. d) Penggunaan teknologi yang bersesuaian untuk mengawal aktiviti video conferencing, video streaming, chat, downloading adalah digalakkan bagi menguruskan	Pentadbir Rangkaian dan Semua

penggunaan jalur lebar (broadband) yang maksimum dan lebih berkesan.

e) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Ketua Jabatan berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya.

f) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh ICTSO/pegawai yang diberi kuasa.

g) Bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan.

h) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Setiausaha Bahagian sebelum dimuat naik ke Internet.

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

j) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MBPJ.

k) 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 CDO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan.

l) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali.

m) 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 dan lagu yang boleh menjejaskan tahap capaian Internet; dan

   ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks, ucapan atau bahanbahan

	yang mengandungi unsur-unsur lucah.	
Kawalan Capaian Sistem Pengoperasian Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian		
070401	**Capaian Sistem Pengoperasian**	
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan. b) Merekodkan capaian yang berjaya dan gagal. c) Membekalkan kemudahan untuk pengesahan; bagi sistem, kata laluan kunci digunakan. Kualiti kata kunci perlu mendapat pengesahan. d) Menghadkan masa penggunaan rangkaian bagi pengguna. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: i. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan. ii. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf super user. iii. Menjana amaran (alert) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. iv. Menyediakan tempoh penggunaan mengikut kesesuaian. Perkara-perkara yang perlu dipatuhi termasuk berikut: • Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; • Mewujudkan satu pengenalan diri (ID) yang unik dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang	Pentadbir Sistem, ICTSO

	bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna. • Menghadkan dan mengawal penggunaan program utiliti yang berkemampuan bagi satu tempoh yang ditetapkan. • Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
Kawalan Capaian Aplikasi dan Maklumat Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi		
070501	**Capaian Aplikasi dan Maklumat**	
	Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di MBPJ adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi: a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian, keselamatan dan sensitiviti maklumat yang telah ditentukan. b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini. c) Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan. d) Menghadkan capaian sistem dan aplikasi kepada lima (5) kali percubaan kecuali kepada sistem legasi seperti Lotus Notes dan Sistem PJIIS. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat. e) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah.	Pentadbir Sistem dan ICTSO

	f) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah dibolehkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
Peralatan Mudah Alih dan Jarak Jauh Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan jarak jauh		
070601	**Peralatan Mudah Alih**	
	Perkara yang perlu dipatuhi adalah seperti berikut: a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua
070602	**Kerja Jarak Jauh**	
	Perkara yang perlu dipatuhi adalah seperti berikut: a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

Perkara 08 : PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Keselamatan Dalam Membangunkan Sistem dan Aplikasi

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

080101	**Keperluan Keselamatan**	
	Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat. 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. Sebaik-baiknya, semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Seksyen Pengurusan Aplikasi, ICTSO

Kod Selamat (*Secure Coding*)

Objektif : Memastikan perisian ditulis dengan selamat dengan mengurangkan potensi kerentanan (vulnerability) keselamatan maklumat di dalam perisian.

080201	**Kawalan Kod Selamat**	
	Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan sistem hendaklah sentiasa dikaji dari semasa ke semasa mengikut keperluan dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat.	Seksyen Pengurusan Aplikasi, ICTSO

Kriptografi		
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat.		
080301	**Penyulitan**	
	Pengguna hendaklah membuat penyulitan ke atas maklumat sensitive atau maklumat rahsia pada setiap masa.	Semua
080302	**Pengurusan Kunci**	
	Pengurusan kunci hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua
Fail Sistem		
Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.		
080401	**Kawalan Fail Sistem**	
	Proses pengemas kini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan. Kod atau aturcara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemas kinian untuk tujuan statistik, pemulihan dan keselamatan.	Seksyen Pengurusan Aplikasi
Pembangunan dan Proses Sokongan		
Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi		
080501	**Kawalan perubahan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum diguna pakai;	Semua

	b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d) Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e) Menghalang sebarang peluang untuk membocorkan maklumat.	
080502	**Pembangunan Perisian Secara Outsource**	
	Pembangunan perisian aplikasi secara outsource perlu dipantau oleh pemilik sistem. Source code adalah menjadi hak milik MBPJ.	Pemilik Sistem dan Pentadbir Sistem
	Kawalan Teknikal Keterdedahan (vulnerability) Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
080601	**Kawalan dari Ancaman Teknikal**	
	Maklumat mengenai ancaman teknikal sistem maklumat yang digunakan perlu diperolehi. Pendedahan organisasi kepada ancaman teknikal perlu dinilai bagi mengenalpasti tahap risiko yang bakal dihadapi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan. b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi. c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem, Pengurus Teknikal

Perkara 09 : PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Dasar Kesinambungan Perkhidmatan

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

090101	**Pelan Kesinambungan Perkhidmatan**	
	Pelan kesinambungan perkhidmatan 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 Jawatan Kuasa Kecil ICT (JKKICT) dan perkara-perkara berikut perlu diberi perhatian: a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan. b) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan. c) Mendokumentasikan proses dan prosedur yang telah dipersetujui. d) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan. e) Membuat penduaan. f) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	Seksyen Infrastruktur dan Teknikal ICT

Perkara 10 : PEMATUHAN

Pematuhan dan Keperluan Perundangan

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

100101	**Pematuhan Dasar**	
	Setiap pengguna di MBPJ hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MBPJ dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di MBPJ termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Semua
100102	**Keperluan Perundangan**	
	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MBPJ: a) Arahan Keselamatan. b) Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”. c) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS). d) Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT). e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “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) Akta Tanda Tangan Digital 1997.	Semua

	h) Akta Jenayah Komputer 1997. i) Akta Hak cipta (Pindaan) 2012. j) Akta Komunikasi dan Multimedia 1998. k) Pekeliling-pekeliling dan Prosedur-prosedur yang dikeluarkan dari masa ke semasa. l) Polisi penggunaan sistem dan perolahan perkakasan dan perisian untuk Majlis Bandaraya Petaling Jaya.	
100103	**Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal**	
	ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
100104	**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
100105	**Pelanggaran Perundangan**	
	Mengambil tindakan undang-undang dan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaian, kelalaian dan perlanggaran keselamatan yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 dan akta lain yang berkaitan.	Semua

LAMPIRAN A

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT MAJLIS BANDARAYA PETALING JAYA

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT MAJLIS BANDARAYA PETALING JAYA

Tuan /Puan,

Dengan hormatnya saya menarik perhatian tuan/puan terhadap perkara di atas.

2.Untuk makluman tuan/puan, Pengurusan MBPJ telah memutuskan supaya Surat Akuan Pematuhan Dasar Keselamatan ICT perlu ditandatangani oleh semua pembekal Unit Teknologi Maklumat dengan merujuk Pekeliling Perkhidmatan Dasar Keselamatan ICT Pejabat Setiausaha Kerajaan Negeri Selangor versi 1.0 (Pekeliling Setiausaha Kerajaan Negeri Selangor Bilangan 4 Tahun 2010) . Sehubungan itu, sukacita sekiranya tuan/puan dapat memberikan kerjasama untuk menandatangani surat akuan pematuhan ini dan kembalikan semula ke Bahagian Teknologi Maklumat. Surat Akuan Pematuhan DKCIT hendaklah diedar kepada semua pasukan kerja yang terlibat dengan projek di MBPJ.

3.Tuan/puan diminta membaca, memahami dan akur akan peruntukan yang terkandung di dalam Dasar Keselamatan ICT Majlis Bandaraya Petaling Jaya.

Sebarang pertanyaan lanjut boleh diajukan kepada :

1. Ts. Samsul Bahari b Nonchi
   No. Telefon : 03-79563544
   samb. 232 Emel :
   samsul@mbpj.gov.my

2. Puan Ummu Fatin Maslan
   No. Telefon : 03-79563544
   samb. 239 Emel :
   ummufatin@mbpj.gov.my

3. En Khairul Nizam b Ab Jabar
   No. Telefon : 03-79563544
   samb. 238 Emel :
   khairulnizam@mbpj.gov.my

Sekian, terima kasih.

Unit Teknologi Maklumat
Majlis Bandaraya Petaling Jaya

Lampiran 1

SURAT AKUAN PEMATUHAN KAKITANGAN

DASAR KESELAMATAN ICT MAJLIS BANDARAYA PETALING JAYA

Nama (Huruf Besar) : _____

No. Kad Pengenalan : _____

Jawatan : _____

Bahagian : _____

Tarikh Lantikan : _____

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca seperti mana dalam capaian URL Majlis iaitu https://www.mbpj.gov.my/ms/dkict memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT Majlis Bandaraya Petaling Jaya.
2. Jika saya ingkar kepada peruntukan-peruntukan yang telah ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : .....

Tarikh : .....

Pengesahan Ketua Pegawai Maklumat

.....
(Ts. Samsul Bahari Bin Nonchi)
b.p. Timbalan Datuk Bandar Petaling Jaya
Majlis Bandaraya Petaling Jaya

Tarikh : .....

Lampiran 2

SURAT AKUAN PEMATUHAN PIHAK KETIGA

DASAR KESELAMATAN ICT MAJLIS BANDARAYA PETALING JAYA

Program / Projek : _____

Nama Syarikat : _____

Tarikh Mula Projek : _____

Tarikh Tamat Projek : _____

Nama (Huruf Besar) : _____

No. Kad Pengenalan : _____

Jawatan : _____

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca seperti mana dalam capaian URL Majlis iaitu https://www.mbpj.gov.my/ms/dkict memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT Majlis Bandaraya Petaling Jaya.
2. Jika saya ingkar kepada peruntukan-peruntukan yang telah ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : .....

Tarikh : .....

Pengesahan Ketua Pegawai Digital

.....
(Ts. Samsul Bahari Bin Nonchi)
b.p. Timbalan Datuk Bandar Petaling Jaya
Majlis Bandaraya Petaling Jaya

Tarikh : .....

LAMPIRAN B

POLISI BERKAITAN *BRING YOUR OWNED DEVICE (BYOD)*
MAJLIS BANDARAYA PETALING JAYA

POLISI *BRING YOUR OWN DEVICE* (BYOD) MAJLIS BANDARAYA PETALING JAYA

ABSTRAK

Polisi BYOD adalah satu garis panduan yang mengandungi tatacara penggunaan secara selamat semua peralatan mudah alih. Garis panduan ini disediakan bagi memastikan langkah-langkah keselamatan perlindungan berkaitan penggunaan BYOD dilaksanakan dan diberi perhatian sewajarnya oleh semua warga kerja MBPJ

ISI KANDUNGAN

POLISI *BRING YOUR OWN DEVICE* (BYOD)

1.1 PENGENALAN

BYOD adalah peralatan mudah alih persendirian seperti telefon pintar, *tablet* dan *laptop* yang digunakan untuk tujuan rasmi. Walaupun fenomena ini berupaya meningkatkan produktiviti, penggunaan peralatan mudah alih di tempat kerja boleh menimbulkan risiko besar kepada keselamatan maklumat jika tidak mempunyai strategi untuk menangani ancaman baru ini.

Bagi kebanyakan organisasi, menyekat penggunaan peralatan mudah alih peribadi adalah pilihan yang realistik. Realiti bisnes masa kini terus menekan dan memaksa pengurusan organisasi untuk membenarkan penggunaan peralatan mudah alih peribadi bagi mencapai aplikasi dan data rasmi organisasi. Namun begitu peralatan mudah alih ini berpotensi sebagai penyumbang kepada risiko keselamatan perlindungan maklumat organisasi sekiranya tidak dikawal dengan baik. Garis panduan peralatan mudah alih ini untuk melindungi aset maklumat Kerajaan, pegawai/kakitangan, harta intelek dan juga reputasi.

Garis panduan ini disediakan untuk menggariskan satu tatacara penggunaan secara selamat semua peralatan mudah alih supaya selaras dengan prinsip Confidentiality, Integrity dan Availability (CIA).

1.2 OBJEKTIF

Garis panduan ini disediakan bagi memastikan langkah-langkah keselamatan perlindungan berkaitan penggunaan BYOD dilaksanakan dan diberi perhatian sewajarnya oleh warga kerja MBPJ. Selaras dengan itu, garis panduan ini bertujuan untuk:

a) Mengelak risiko kebocoran maklumat rasmi.
b) Mengelakkan ancaman risiko keselamatan ke atas infrastruktur ICT.
c) Memastikan produktiviti penjawat awam tidak terjejas dalam menjalankan urusan rasmi jabatan.
d) Meningkatkan integriti data

1.3 RISIKO KESELAMATAN

Risiko keselamatan melibatkan peralatan mudah alih peribadi boleh dibahagikan kepada dua kategori iaitu risiko alat dan risiko aplikasi.

a) Risiko Alat berpunca daripada peralatan mudah alih peribadi berkeupayaan tinggi seperti penyimpanan data samada dalaman atau di *cloud,* penghantaran maklumat keluar daripada organisasi dan kehilangan peralatan. Organisasi biasanya tidak mempunyai kawalan atau mempunyai kawalan yang sangat terhad terhadap peralatan mudah alih ini berbanding PC desktop atau komputer riba yang dibekalkan.

b) Risiko Aplikasi timbul akibat daripada pekerja memasang aplikasi mudah alih pihak ketiga yang berinteraksi dengan data rasmi organisasi yang disimpan di dalam peralatan.

1.4 KATEGORI PERALATAN BYOD YANG DIBENARKAN

Senarai kategori peralatan BYOD yang dibenar untuk digunakan adalah seperti berikut:

Bil.	Kategori BYOD	Sistem Pengoperasian
1.	iPAD	IOS
2.	Tablet Android	Android/ Windows
3.	Telefon Pintar	Android/IOS/ Windows Phone
4.	Notebook	IOS / Windows / Linux

1.5 TATACARA PENGGUNAAN BYOD

Pengguna BYOD perlu mematuhi tatacara penggunaan BYOD seperti berikut:

a) Penggunaan BYOD bagi urusan rasmi seperti memuat turun Slip Gaji telah diluluskan diperingkat Pengurusan Tertinggi. Capaian hanya dibenarkan untuk kakitangan yang masih aktif.

b) Penggunaan BYOD untuk urusan rasmi adalah terhad kepada capaian berikut:
   i. Urusan Emel.
   ii. Maklumat Perhubungan.
   iii. Memuat turun slip Gaji peribadi (Sistem ePayslip)
   iv. Portal intranet dan Kalendar Majlis.
   v. Menguruskan Maklumat Rasmi Tidak Terperingkat.

c) Sebarang bahan rasmi yang dimuat naik/edar/kongsi hendaklah mendapat kebenaran Ketua Jabatan.

d) Menandatangani Surat Akuan Pematuhan DKICT melalui pautan URL https://www.mbpj.gov.my/ms/dkict, supaya mereka memahami dan akur akan peuntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT Majlis Bandaraya Petaling Jaya. (Rujuk Lampiran 1)

1.6 LARANGAN PENGGUNAAN

Pengguna BYOD adalah DILARANG daripada melakukan perkara berikut:

a) Menyambung BYOD ke rangkaian jabatan.
b) Menggunakan BYOD untuk mengakses, menyimpan dan menyebarkan maklumat Rasmi dan Terperingkat kepada pihak yang tidak dibenarkan.
c) Penggunaan BYOD untuk tujuan peribadi yang boleh menggangu produktiviti kerja.
d) Menjadikan BYOD sebagai access point kepada aset ICT jabatan untuk capaian ke Internet tanpa kebenaran.

1.7 KESELAMATAN

Pengguna BYOD perlu memastikan peralatan yang digunakan mempunyai kawalan keselamatan seperti berikut:

a) Menetapkan mekanisme kawalan akses bagi BYOD dan akan mengunci secara automatik apabila tidak digunakan.
b) Melaksanakan penyulitan dan/atau perlindungan ke atas folder yang mempunyai maklumat rasmi Kerajaan yang disimpan di dalam peralatan BYOD.
c) Memuat turun aplikasi daripada sumber yang sah.
d) Memastikan BYOD mempunyai ciri-ciri keselamatan standard seperti berikut
    i. Antivirus
    ii. Patching terkini
    iii. Anti Theft

1.8 RISIKO / LIABILITI / PENAFIAN

Pengguna BYOD adalah tertakluk kepada perkara-perkara seperti berikut:

a) Kakitangan adalah bertanggungjawab menggunakan BYOD secara berhemah sepanjang masa dan mematuhi mana-mana peraturan/dasar yang berkuatkuasa.

b) Kakitangan bertanggungjawab memadamkan segala maklumat yang berkaitan dengan urusan rasmi jabatan sekiranya bertukar/ditamatkan perkhidmatan/bersara ATAU sewaktu dihantar ke pusat servis untuk penyelenggaraan.

c) Kakitangan adalah bertanggungjawab dan boleh dikenakan tindakan tatatertib sekiranya didapati menyalahgunakan BYOD yang menyebabkan kehilangan/ kerosakan/pendedahan maklumat rasmi Kerajaan.

d) Unit Teknologi Maklumat tidak bertanggungjawab atas kehilangan atau kerosakan data BYOD yang digunakan untuk tujuan urusan rasmi jabatan.