MAJLIS PERBANDARAN KLANG

DKICT

DASAR KESELAMATAN ICT
Majlis Perbandaran Klang

Versi 4.2

SEJARAH DOKUMEN		
TARIKH KELULUSAN	**VERSI**	**TARIKH KUATKUASA**
22/09/2008	1.0	06/10/2008
24/08/2010	2.0	08/10/2010
26/04/2012	2.1	02/05/2012
16/09/2014	3.0	01/10/2014
01/11/2016	3.1	14/11/2016
07/12/2018	4.0	07/12/2018
05/04/2021	4.1	05/04/2021
30/10/2023	4.2	1/11/2023

KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT Majlis Perbandaran Klang yang akan disebut sebagai DKICT MPKlang di dalam dokumen ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) Majlis Perbandaran Klang. Dasar ini juga menerangkan kepada semua pengguna di Majlis Perbandaran Klang mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT Majlis Perbandaran Klang.

OBJEKTIF

DKICT MPKlang secara umumnya diwujudkan untuk menjamin kesinambungan urusan Majlis Perbandaran Klang dengan meminimumkan kesan insiden keselamatan ICT.

Objektif utama DKICT MPKlang adalah seperti berikut: -

(a) Memastikan kelancaran operasi Majlis Perbandaran Klang yang menggunakan teknologi ICT dan meminimumkan kerosakan dan kemusnahan
(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem ICT dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan makumat dan komunikasi; dan
(c) Mencegah salahguna atau kecurian Aset ICT Majlis Perbandaran Klang.

PERNYATAAN DASAR

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

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT.

Terdapat empat (4) komponen asas keselamatan ICT iaitu:

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
(b) Menjamin setiap maklumat adalah tepat dan sempurna;
(c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
(d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat daripada sumber yang sah.

Dasar Keselamatan ICT MPKlang merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan.

Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

(a) **Kerahsiaan** – Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
(b) **Integriti** – Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan;
(c) **Tidak Boleh Disangkal** – Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
(d) **Kesahihan** – Data dan maklumat hendaklah dijamin kesahihannya; dan
(e) **Ketersediaan** – Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah:

(a) bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT;
(b) ancaman yang wujud akibat daripada kelemahan tersebut;
(c) risiko yang mungkin timbul; dan
(d) 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**
Aset ICT yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan (contoh seperti komputer, pelayan, peralatan komunikasi dan sebagainya);

(b) **Perisian**
Program perisian atau aplikasi yang menyediakan kemudahan pemerosesan maklumat seperti sistem pengoperasian, sistem pangkalan data, aplikasi pejabat, perisian sistem rangkaian dan sebagainya;

(c) **Premis Komputer dan Komunikasi**
Semua kemudahan serta lokasi yang digunakan untuk menempatkan aset-aset di atas.

(d) **Perkhidmatan**
Perkhidmatan atau sistem yang menyokong aset lain seperti perkhidmatan rangkaian, perkhidmatan keselamatan dan lain-lain lagi;

(e) **Data dan Maklumat**
Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik;

(f) **Manusia**
Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja Majlis Perbandaran Klang yang mana merupakan aset berdasarkan kepada tugas dan fungsi yang dilaksanakan;

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

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT MPKlang dan perlu dipatuhi adalah seperti berikut:-

(a) **Akses Atas Dasar Perlu Mengetahui**

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

(b) **Hak Akses Minimum**

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

(c) **Akauntabiliti**

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT Majlis Perbandaran Klang.

(d) **Pengasingan**

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

(e) **Pengauditan**

Pengauditan adalah 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**

DKICT MPKlang hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk perlanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

(g) **Pemulihan**

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

(h) **Saling bergantung**

Setiap perinsip 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

MPKlang hendaklah 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.

MPKlang 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 system maklumat MPKlang 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 penyelenggaraan, kemudahan utiliti dan sistem-sistem sokongan lain.

MPKlang 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.

MPKlang hendaklah mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

(a) mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
(b) menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan atasan;
(c) mengelak dan/atau mencegah risiko daripada terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
(d) memindahkan risiko kepada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

TERMA DAN DEFINISI

Bahagian ini menerangkan istilah-istilah utama yang digunakan di dalam dokumen ini:

TERMA	DEFINISI
Agensi luar	Individu atau organisasi kerajaan/swasta yang berurusan dengan MPKlang.
Akaun pengguna	Akaun E-mel.
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket,cakera padat, pita magnetik, optical disk, flash disk, CDROM, thumb drive untuk sebarang kemungkinan adanya virus.
Aset ICT	Sumber yang terdiri daripada perkakasan, perisian, premis computer dan komunikasi, perkhidmatan, data/maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Jalur Lebar – Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan
BYOD	BYOD adalah peralatan mudah alih persendirian seperti telefon pintar, tablet dan laptop yang digunakan untuk tujuan rasmi.
CSIRT	Cyber Security Incident Response Team atau Pasukan Tindak Balas Insiden Keselamatan Siber Agensi – Jawatankuasa yang ditubuhkan sebagai *first level support* kepada NACSA dalam membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi.
CDO	*Chief Digital Officer* – Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Cloud Computing	*Cloud computing* adalah satu kaedah penyampaian perkhidmatan Teknologi Maklumat dan Komunikasi (ICT) di mana pelanggan membayar untuk menggunakan, dan bukan semestinya memiliki sumber. Perkhidmatan ini biasanya disediakan oleh pihak ketiga menggunakan teknologi Internet
Content Filtering	Perisian atau perkakasan yang mengesan dan menapis kandungn maklumat daripada penghantar sebelum sampai kepada penerima.
DKICT	Dasar Keselamatan ICT
Dokumen	Semua himpunan atau kumpulan bahan atau dokumen yang disimpan dalam bentuk media cetak, salinan lembut (soft copy), elektronik, dalam talian, kertas lutsinar, risalah atau slaid

Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman.Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/espionage), penipuan (hoaxes).
GCERT	Government Computer Emergency Response Team atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Hard disk	Cakera keras – Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (hub) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	Information and Communication Technology – Teknologi Maklumat dan Komunikasi.
ICTSO	ICT Security Officer – Pegawai Keselamatan ICT
Insiden	Musibah (adverse event) yang berlaku ke atas sistem aplikasi dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari trafik ke trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System(IDS)	Sistem Pengesan Pencerobohan – Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.

Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan – Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code.
JKICT	Jawatankuasa Keselamatan ICT.
JPICT	Jawatankuasa Pemandu ICT.
Kawasan Larangan	Kawasan yang dihadkan kemasukan kepada pegawai-pegawai tertentu sahaja iaitu pegawai yang diberi kuasa.
LAN	Local Area Network – Rangkaian Kawasan Setempat yang menghubungkan komputer.
Load Test	Ujian capaian sistem aplikasi Online bagi menguji tahap ketahanan ke sistem daripada capaian yang banyak.
Logout	Log-out komputer – Keluar daripada sesuatu sistem atau aplikasi komputer.
Maklumat Terperingkat	Dokumen/Maklumat Rasmi yang dikategorikan sebagai Rahsia Besar, Rahsia Sulit dan Terhad.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya.
Malware	Merujuk kepada virus, worms,trojan horses, bots dan lain-lain kod jahat.
Media storan	Perkakasan yang berkaitan dengan penyimpanan data dan maklumat seperti telefon bimbit, kad memori, disket, kartrij,cakera padat, cakera mudah alih, pita, cakera keras dan pemacu pena.
MODEM	MOdulator DEModulator – Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
MPKlang	Majlis Perbandaran Klang – Agensi yang akan mengguna pakai DKICT
Mobile Code	Mobile code merupakan perisian yang boleh dipindahkan antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh Java Applet, ActiveX dan sebagainya pada pelayar internet.
NOC	*Network Operation Center*
NACSA	*National Cyber Security Agency* - Agensi Keselamatan Siber Negara
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.

Penetration Test	Ujian Penembusan – Kaedah menilai tahap keselamatan sistem komputer atau rangkaian dengan melakukan simulasi serangan daripada dalaman dan luaran.
Penggodam	Penceroboh sistem PC dengan melakukan aktiviti seperti pencurian maklumat, mengubahsuai laman web, penyebaran virus, menyesakkan rangkaian, merosakkan PC dan pelbagai lagi aktiviti negatif dalam dunia ICT.
Pengguna	Ia merujuk Warga MPklang di Jabatan/Bahagian termasuk pegawai yang berkhidmat secara kontrak atau pegawai khidmat singkat yang menggunakan aset ICT secara langsung atau tidak langsung.
Peralatan mudah alih	Perkakasan seperti telefon bimbit, komputer peribadi, komputer tablet, projektor, pendrive, external HDD, gajet ICT dan alat-alat rangkaian komunikasi.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej perisian seperti *spreadsheet* dan *word processing* atau sistem yang dibangunkan oleh agensi atau atau pihak luar.
Pihak Ketiga	Ia merujuk pembekal, Pakar Runding dan individu yang dilantik untuk melaksanakan tugas di KPKT dalam jangka masa yang tertentu.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam – Merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
PJTM	Pengarah Jabatan Teknologi Maklumat
PTM	Pegawai Teknologi Maklumat
Pegawai Aset ICT	Pegawai yang diberi kuasa mentadbir untuk mentadbir Aset ICT MPKlang iaitu PPTM.
Pejabat Ketua Pegawai Keselamatan Kerajaan	Badan yang memberi khidmat nasihat keselamatan perlindungan kepada Kerajaan Negeri, Kementerian, Jabatan dan agensi kerajaan dengan tujuan untuk membantu mengekalkan tahap keselamatan fizikal, keselamatan dokumen dan keselamatan personel di semua agensi kerajaan yang ditetapkan oleh kerajaan dari semasa ke semasa bagi melindungi terhadap espionaj dan sabotaj serta daripada kebocoran maklumat tanpa kebenaran daripada semua agensi kerajaan.
Pentadbir Pusat data	Pegawai yang diberi kuasa mentadbir untuk mentadbir Pusat Data MPKlang yang terdiri daripada PTM/PPTM
Pentadbir Rangkaian	Pegawai yang diberi kuasa mentadbir untuk mentadbir Rangkaian MPKlang yang terdiri daripada PTM/PPTM
Pentadbir Sistem ICT	Pegawai yang diberi kuasa mentadbir untuk mentadbir Sistem dan Perisan Aplikasi MPKlang yang terdiri daripada PTM/PPTM

Pentadbir Web	Pegawai yang diberi kuasa mentadbir untuk mentadbir Laman web/Portal MPKlang yang terdiri daripada PTM/PPTM
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan besar kepada Malaysia.
Rahsia Besar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada kepentingan dan martabat Malaysia, atau memberi keuntungan besar kepada sesebuah kuasa asing.
Restoration	Pemulihan ke atas data.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian di lokasi atau kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ian tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer.
Source Code	Kod sumber bagi aplikasi yang dibangunkan.
Stress Test	Ujian ke atas sistem, aplikasi dan perkakasan yang memberi penekanan kepada prestasi, ketersediaan dan kawalan ralat semasa beban puncak.
Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan kerajaan atau orang perseoranganatau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.
Switches	Merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense *Multiple Access*/*Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar,Rahsia atau Sulit tetapi berkehendakan juga diberi satu tahap perlindungan keselamatan.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
UAT	*User Acceptance Test*.
UPS	*Uninterruptible Power Supply* – Bekalan Kuasa elektrik sokongan

Video Conference	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video duahala dan audio secara serentak.
Video Streaming	Sidang Video – Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama diterima oleh penghantar
Virus	Aturcara yang bertujuan merosakkan data atau aplikasi.
Vulnerability	Kelemahan pada sistem dan aplikasi yang membenarkan serangan berlaku dan menjejaskan tahap keselamatan maklumat.
WAN	*Wide Area Network* – Rangkaian yang merangkumi kawasan luas.
Wireless LAN	Jaringan computer yang terhubung tanpa melalui kabel.

PERKARA 01 – PEMBANGUNAN DAN PENYELENGGARAAN DASAR

P01(01) – Dasar Keselamatan ICT	
P01(01) 01 – Perlaksanaan Dasar	**Tindakan**
Perlaksanaan dasar ini akan dijalankan oleh Yang Dipertua MPKlang selaku Pegawai Pengawal dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada:- i) Ketua Pegawai Digital (CDO); ii) Pengarah Teknologi Maklumat (PTM); iii) Pegawai Keselamatan ICT (ICTSO); dan iv) Semua Ketua Jabatan/bahagian. v) Ketua Bahagian Keselamatan ICT dan Pematuhan ICT; vi) Pegawai Maklumat	YDP; CDO
P01(01) 02 –Penyebaran Dasar	**Tindakan**
Dasar ini perlu disebarkan kepada semua pengguna MPKlang meliputi kakitangan, pembekal, pakar runding dan lain-lain berkaitan).	ICTSO
P01(01) 03 – Penyelenggaraan Dasar	**Tindakan**
Dasar Keselamatan ICT MPKlang adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa meliputi kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur berhubung penyelenggaraan dasar keselamatan ICT MPKlang: a) kenal pasti dan tentukan perubahan yang diperlukan; b) kemuka cadangan pindaan secara bertulis kepada Pengarah Teknologi Maklumat (PTM) selaku Pengurus ICT untuk pembentangan dan persetujuan Mesyuarat Pemandu ICT (JPICT) MPKlang; c) perubahan yang telah dipersetujui oleh JPICT dimaklumkan kepada semua pengguna; dan d) Dasar ini hendaklah dikaji semula sekurang-kurangnya **dua tahun sekali** atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	CDO; Pengurus ICT; ICTSO; Ketua Jabatan
P01(01) 04 – Pengecualian Dasar	**Tindakan**
Dasar Keselamatan ICT MPKlang adalah terpakai dan mestilah dipatuhi oleh semua pengguna ICT MPKlang dan tiada pengecualian diberikan	Semua (termasuk kakitangan, pembekal, pakar runding dan lain-lain berkaitan).

PERKARA 02 – ORGANISASI KESELAMATAN

P02(01)INSIDEN – Infrastruktur Organisasi Keselamatan	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.	
P02(01) 01 – Yang Dipertua	**Tindakan**
Peranan dan tanggungjawab Yang Dipertua adalah seperti berikut: (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah DKICT MPKlang; (b) Memastikan semua pengguna mematuhi DKICT MPKlang; (c) Memastikan semua keperluan organisasi seperti sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan (d) memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT MPKlang.	Yang Dipertua
P02(01) 02 – Ketua Pegawai Digital (CDO)	**Tindakan**
Setiausaha Majlis Perbandaran Klang merupakan Ketua Pegawai Digital (CDO) yang dilantik untuk memastikan DKICT MPKlang dilaksanakan secara berterusan. Peranan dan tanggungjawab CDO adalah seperti berikut: (a) Membantu Yang Dipertua dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (b) Bertanggungjawab ke atas perkara-perkara berkaitan dengan keselamatan ICT Majlis; (c) Bertanggungjawab menyelaras pelaksanaan pelan tindakan dan program keselamatan seperti penyediaan DKICT MPKlang, pelan latihan dan program kesedaran pengguna, pengurusan risiko dan pengauditan; (d) Menentukan keperluan Keselamatan ICT; dan (e) Menguatkuasakan pelaksanaan DKICT MPKLANG di semua Jabatan/bahagian Majlis Perbandaran Klang.	CDO
P02(01) 03 – Pengarah Jabatan Teknologi Maklumat (PJTM)	**Tindakan**
Pengarah Jabatan Teknologi maklumat (PJTM) merupakan Pengurus ICT iaitu pegawai yang bertanggungjawab dalam Pengurusan ICT bagi keseluruhan Majlis Perbandaran Klang dan membantu Ketua Pegawai Digital (CDO) dalam memastikan DKICT MPKlang dilaksanakan di semua jabatan/bahagian Majlis Perbandaran Klang. Peranan dan tanggungjawab beliau adalah seperti berikut: (a) Memastikan DKICT MPKlang dilaksanakan di semua Jabatan/Bahagian Majlis Perbandaran Klang; (b) Memastikan semua kakitangan, perunding, kontraktor dan pembekal yang berurusan dengan Majlis Perbandaran Klang mematuhi dasar, piawaian dan garis panduan keselamatan ICT;	Pengurus ICT (PJTM)

(c) Membangun, mengkaji semula dan mengemaskini pelan kontigensi Keselamatan ICT Jabatan (d) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Majlis; (e) Menentukan kawalan akses pengguna terhadap aset ICT Majlis; (f) Memastikan garis panduan, prosedur dan tatacara berkaitan keselamatan ICT diwujudkan untuk memastikan jabatan/bahagan mematuhi keperluan DKICT MPKlang; (g) Mengemukakan kepada ICTSO mengenai maklumat terkini tentang ancaman keselamatan ICT dan menyimpan rekod sebagai rujukan; (h) Melaporkan sebarang perkara atau penemuan ancaman terhadap keselamatan ICT kepada ICTSO; (i) Memastikan DKICT MPKlang dikemaskini sesuai dengan perubahan teknologi, (j) Memastikan Pelan Strategik ICT Majlis Perbandaran klang mengandungi aspek keselamatan ICT; dan (k) Memastikan DKICT MPKlang yang telah dipinda mendapat kelulusan untuk dikuatkuasakan sebelum dilaksanakan di semua jabatan/bahagian Majlis Perbandaran Klang.	
P02(01) 04 – Pegawai Keselamatan ICT (ICTSO)	**Tindakan**
Pengarah Jabatan Teknologi Maklumat merupakan pegawai yang dilantik sebagai Pegawai Keselamatan ICT (ICTSO). Peranan dan tanggungjawab Pegawai Keselamatan ICT (ICTSO) yang dilantik adalah seperti berikut: - (a) Mengurus keseluruhan program-program keselamatan ICT MPKlang; (b) Melaksanakan penguatkuasaan Dasar Keselamatan ICT MPKlang; (c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MPKlang kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MPKlang; (e) Menjalankan pengurusan risiko; (f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MPKlang berdasarkan hasil penemuan dan menyediakan laporan mengenainya; (g) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada Pengurus ICT (h) Menyedia dan menyebarkan amaran yang sesuai terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan dan pemulihan yang bersesuaian; (i) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan Siber Majlis Perbandaran Klang (CSIRT MPKlang) dan memaklumkannya kepada Pengurus ICT (PJTM) dan CDO (j) Melaporkan insiden keselamatan ICT kepada NACSA, sama ada sebagai *input* atau tindakan seterusnya;	ICTSO

(k) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; (l) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Majlis; (m) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; (n) Memastikan pematuhan DKICT MPKlang oleh pihak ketiga seperti perunding, kontraktor dan pembekal yang mencapai dan menggunakan aset ICT Majlis Perbandaran klang untuk tujuan penyelenggaraan, pemasangan, naiktaraf dan sebagainya; (o) Menyediakan laporan secara berkala berkaitan aktiviti pelaksanaan DKICT dan isu-isu berkaitan Keselamatan ICT.		
P02(01) 05 – Ketua Bahagian Keselamatan ICT dan Pematuhan ICT	**Tindakan**	
Ketua Bahagian Keselamatan ICT dan Pematuhan ICT merupakan pegawai yang dilantik sebagai pembantu kepada Pegawai Keselamatan ICT (ICTSO). Peranan dan tanggungjawab Ketua Bahagian Keselamatan ICT dan Pematuhan ICT yang dilantik adalah seperti berikut: - (a) Membantu ICTSO mengurus keseluruhan program-program keselamatan ICT MPKlang; (b) Membantu ICTSO melaksanakan penguatkuasaan Dasar Keselamatan ICT MPKlang; (c) Membantu ICTSO memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MPKlang kepada semua pengguna; (d) Membantu ICTSO mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MPKlang; (e) Membantu ICTSO menjalankan pengurusan risiko; (f) Membantu ICTSO menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MPKlang berdasarkan hasil penemuan dan menyediakan laporan mengenainya; (g) Membantu ICTSO melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada Pengurus ICT (h) Membantu ICTSO menyedia dan menyebarkan amaran yang sesuai terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan dan pemulihan yang bersesuaian; (i) Membantu ICTSO melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT Majlis Perbandaran Klang (CSIRT MPKlang) dan memaklumkannya kepada Pengurus ICT (PJTM) dan CDO (j) Membantu ICTSO melaporkan insiden keselamatan ICT kepada NACSA sama ada sebagai input atau tindakan seterusnya; (k) Membantu ICTSO dalam bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; (l) Membantu ICTSO menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Majlis; (m) Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT (Security Posture Assessment (SPA) serta penilaian risiko keselamatan maklumat;	Ketua Bahagian Keselamatan ICT dan Pematuhan ICT	

(n) Membantu ICTSO menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; (o) Membantu ICTSO memastikan pematuhan DKICT MPKlang oleh pihak ketiga seperti perunding, kontraktor dan pembekal yang mencapai dan menggunakan aset ICT Majlis Perbandaran klang untuk tujuan penyelenggaraan, pemasangan, naiktaraf dan sebagainya; (p) Membantu ICTSO menyediakan laporan secara berkala berkaitan aktiviti pelaksanaan DKICT dan isu-isu berkaitan Keselamatan ICT.	
P02(01) 06 – Pegawai Maklumat	**Tindakan**
Pihak Berkuasa Negeri hendaklah melalui Warta melantik Pegawai Maklumat bagi setiap jabatan. Peranan dan tanggungjawab Pegawai Maklumat yang dilantik adalah seperti berikut: - (a) untuk secara teratur merekodkan semua maklumat di dalam kawalan pihak jabatan dan menjaga rekod tersebut dalam cara yang memudah cara pencarian rekod tersebut dan untuk mempertingkatkan dan melaksanakan amalan terbaik berkaitan dengan penjagaan, penyimpanan dan pelupusan maklumat di dalam jabatan dan pendedahan maklumat kepada orang awam; (b) untuk mengadakan latihan kepada jabatan berkenaan dengan penjagaan, penyimpanan, pengurusan dan memenuhi permohonan maklumat; (c) untuk berkhidmat sebagai perantara bagi jabatan dalam menerima permohonan dan membantu individu untuk mendapatkan maklumat untuk membuat permohonan dan apabila perlu, untuk mengarahkan individu kepada jabatan lain yang mungkin mempunyai maklumat yang diminta; (d) untuk memproses dan mematuhi permintaan untuk maklumat kecuali ia dikecualikan tanpa pengecualian dan untuk kembali kepada pemohon dalam masa yang tetapkan; (e) untuk mengadakan sistem pengesan bagi mengawal selia pemprosesan setiap permohonan untuk maklumat dan membolehkan setiap pemohon untuk bertanya tentang perkembangan permohonannya; dan (f) segala apa yang perlu untuk memudah cara perjalanan maklumat di antara agensi atau entiti dan pemohon yang memohonnya.	Pegawai Maklumat
P02(01) 07 – Pentadbir Sistem ICT	**Tindakan**
Pentadbir Sistem ICT ialah Pegawai Teknologi Maklumat dan Penolong Pegawai Teknologi Maklumat yang dipertanggungjawabkan mentadbir sistem di Majlis Perbandaran Klang dan seterusnya melaksanakan pematuhan DKICT MPKlang. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: - (a) Menyedia dan melaksana garis panduan, prosedur dan tatacara pentadbiran sistem selaras dengan keperluan DKICT MPKlang; (b) Memastikan sistem meliputi sistem aplikasi dan pangkalan data boleh digunakan dan dicapai setiap masa; (c) Melaksanakan instalasi dan penambahbaikan sistem serta perisian yang berkaitan dengan sistem meliputi perisian sistem, pangkalan data dan lain-lain; (d) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;	Pentadbir Sistem ICT

(e) Memantau aktiviti pengguna yang diberi keutamaan capaian yang tinggi dan menentukan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT MPKlang; (f) Memantau aktiviti capaian harian sistemaplikasi pengguna; (g) Memastikan aktiviti pentadbiran sistem meliputi sistem aplikasi dan pangkalan data seperti prestasi capaian, penyelesaian masalah, proses pengemaskinian dan pembersihan data (*housekeeping*)dilaksanakan dengan teratur; (h) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta seterusnya melaporkan kepada ICTSO dan Pengarah Teknologi Maklumat dengan segera; (i) Menganalisa dan menyimpan rekod jejak audit; (j) Menyediakan laporan mengenai aktiviti capaian dan penyelenggaraan sistem secara berkala; (k) Melaksanakan keperluan DKICT MPKlang dalam aktiviti berikut: i) Pembangunan dan pelaksanaan sistem atau aplikasi baru sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru; ii) Pelaksanaan pemantauan dan penyelenggaraan sistem dan pangkalan data; iii) Pelaksanaan Proses *Backup* dan *restoration* sistem dan pangkalan data; dan iv) Pembelian atau peningkatan sistem dan perisian ICT; (l) Memastikan ketepatan dan kesempurnaan kawalan capaian pengguna dan menyekat kebenaran capaian serta-merta apabila tidak lagi diperlukan atau melanggar DKICT MPKlang; (m) Melaksanakan prinsip-prinsip DKICT dan melaksanakan kerahsiaan maklumat Majlis Perbandaran Klang; dan (n) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dan dengan segera.	
P02(01) 08 – Pentadbir Rangkaian	**Tindakan**
Pentadbir Rangkaian ialah Pegawai Teknologi Maklumat dan Penolong Pegawai Teknologi Maklumat yang dipertanggungjawabkan mentadbir Rangkaian ICT Majlis Perbandaran Klang dan seterusnya melaksanakan pematuhan DKICT MPKlang. Pentadbir Rangkaian mempunyai peranan dan tanggungjawab seperti berikut; (a) Menyedia dan melaksana garis panduan, prosedur dan tatacara pentadbiran rangkaian selaras dengan keperluan DKICT MPKlang; (b) Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di Majlis Perbandaran Klang beroperasi sepanjang masa; (c) Memastikan peralatan dan perisian rangkaian diselenggara dengan sempurna; (d) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkian sedia ada; (e) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; (f) Memantau penggunaan rangkaian dan melaporkan kepada ICTSO dan Pengarah Teknologi Maklumat dengan segera sekiranya berlaku penyalahgunaan penggunaan rangkaian;	Pentadbir Rangkaian

(g) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian MPKlang secara tidak sah seperti melalui peralatan *modem* dan *dial-up* tanpa kebenaran; (h) Penggunaan telefon mudah alih bagi tujuan tethering modem adalah DILARANG sama sekali; (i) Menyediakan zon khas untuk tujuan pengujian peralatan dan perisian rangkaian; (j) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; (k) Menyediakan laporan mengenai aktiviti penggunaan dan penyelenggaraan rangkaian secara berkala; (l) Melaksanakan keperluan DKICT MPKlang dalam aktiviti berikut: i) Pembangunan dan pelaksanaan rangkaian LAN atau WAN sama ada dilaksanakan secara dalaman atau luaran yang melibatkan teknologi baru; ii) Perolehan teknologi dan perkhidmatan rangkaian baru; dan iii) Pembelian dan peningkatan perisian komputer; (m) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT MPKlang dan menjaga kerahsiaan maklumat MPKlang; dan Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera.	
P02(01) 09 – Pentadbir Web	**Tindakan**
Pentadbir Web ialah Pegawai Teknologi Maklumat dan Penolong Pegawai Teknologi Maklumat yang dipertanggungjawabkan mentadbir laman web/portal Majlis Perbandaran Klang dan seterusnya melaksanakan pematuhan DKICT MPKlang. Pentadbir Web mempunyai peranan dan tanggungjawab seperti berikut: - (a) Menyedia dan melaksana garis panduan, prosedur dan tatacara pentadbiran Web selaras dengan keperluan DKICT MPKlang; (b) Memastikan kandungan laman web sentiasa sahih dan terkini; (c) Memantau prestasi capaian dan menjalankan penilaian prestasi untuk memastikan akses yang lancar; (d) Mengasingkan kandungan dan aplikasi atas talian untuk capaian secara intranet dan internet ke portal Majlis Perbandaran Klang; (e) Memastikan data-data SULIT tidak boleh disalin atau dicetak oleh pihak yang tidak berhak; (f) Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; (g) Melaporkan sebarang pelanggaran keselamatan laman web/portal kepada ICTSO dan Pengarah Teknologi Maklumat dengan segera; (h) Menyediakan laporan aktiviti pengemaskinian dan penyelenggaraan laman web/portal secara berkala; (i) Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman; (j) Menghadkan capaian pentadbir web jabatan/bahagian ke web server;	Pentadbir Web

(k) Melaksanakan housekeeping keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di web server;
(l) Melaksanakan keperluan DKICT MPKlang dalam aktiviti berikut:
  i) Pembangunan dan pelaksanaan laman web sama ada dilaksanakan secara dalaman atau luaran yang melibatkan teknologi baru;
  ii) Penyelenggaraan dan pengemaskinian laman web;
  iii) Pelaksanaan proses backup dan restoration secara berkala;
  iv) Perolehan teknologi dan perkhidmatan web baru; dan
  v) Pembelian dan peningkatan perisian/aplikasi web;
(m) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT MPKlang dan menjaga kerahsiaan maklumat MPKlang; dan
(n) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera.

P02(01) 10 – Pentadbir Pusat Data	**Tindakan**

Pentadbir Pusat Data ialah Pegawai Teknologi Maklumat dan Penolong Pegawai Teknologi Maklumat yang dipertanggungjawabkan mentadbir Pusat Data Majlis Perbandaran Klang dan seterusnya melaksanakan pematuhan DKICT MPKlang.
 	
Pentadbir Pusat Data mempunyai peranan dan tanggungjawab seperti berikut: -
(a) Menyedia dan melaksana garis panduan, prosedur dan tatacara pentadbiran Pusat Data selaras dengan keperluan DKICT MPKlang;
(b) Memastikan Pusat Data Majlis Perbandaran Klang beroperasi sepanjang masa;
(c) Memastikan keselamatan fizikal dan persekitaran Pusat Data Majlis Perbandran Klang dan mengambil langkah-langkah untuk mengurangkan risiko ancaman keselamatan ICT bagi melindungi perkhidmatan di Pusat Data;
(d) Bertanggungjawab memantau setiap perkakasan dan perisian ICT yang ditempatkan di Pusat Data di dalam keadaan yang baik;
(e) Memastikan semua Aset di dalam Pusat Data diselenggara mengikut jadual yang ditetapkan;
(f) Memantau dan mengawal akses fizikal (keluar dan masuk) ke Pusat Data;
(g) Mengawal dan memantau capaian secara atas talian ke server-server dan peralatan ICT di Pusat Data seperti penyediaan *Console Room*, buku log dan sebagainya;
(h) Menyediakan dan melaksanakan pelan kesinambungan perkhidmatan;
(i) Mengesan dan mengambil tindakan pembaikan segera ke atas Perkhidmatan Pusat Data;
(j) Memantau aktiviti capaian perkhidmatan di Pusat Data dan melaporkan kepada ICTSO dan Pengarah Teknologi Maklumat dengan segera sekiranya berlaku sebarang insiden pelanggaran dasar keselamatan Pusat Data;
(k) Menyediakan laporan mengenai aktiviti operasi Pusat Data dan penyelenggaraan secara berkala;
(l) Melaksanakan keperluan DKICT MPKlang dalam aktiviti berikut:
  i) Pembangunan dan pelaksanaan operasi Pusat Data sama ada dilaksanakan secara dalaman atau luaran yang melibatkan teknologi baru;
  ii) Penyelenggaraan dan pengemaskinian Perkhidmatan di Pusat Data;
  iii) Perolehan teknologi dan perkhidmatan komunikasi baru; dan
  iv) Pembelian dan peningkatan perisian pengoperasian Pusat Data;
	Pentadbir Pusat Data

	(m) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT MPKlang dan menjaga kerahsiaan maklumat MPKlang; dan (n) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera. (o) Setiap Pusat Data/Bilik Server hendaklah disediakan dengan sistem Security Access Door atau sentiasa berkunci bagi memantau dan mengawal pengguna yang keluar masuk ke bilik server; (p) Hanya pengguna yang dibenarkan sahaja boleh memasuki bilik server; (q) Setiap server mestilah dilabelkan bagi memudahkan setiap pentadbir menjalankan tugas masing -masing; (r) Pastikan bilik server sentiasa bersih, kemas, tidak menempatkan perkakasan yang tidak diperlukan dan server tidak terdedah kepada habuk; (s) Pastikan pengkabelan disusun dengan kemas dan teratur serta dilabelkan dengan betul; (t) Penghawa dingin mestilah berfungsi dengan baik di mana suhunya dan kelembapan di paras yang sesuai; (u) Semua peralatan keselamatan, UPS penghawa dingin mestilah diselenggarakan secara berkala; (v) Diagram kedudukan server hendaklah disediakan dan dipamerkan di dalam Pusat Data/Bilik Server; dan (w) Semua pergerakan keluar dan masuk perkakasan di Pusat Data perlu direkodkan dan mendapat kebenaran dengan menggunakan borang permohonan yang disediakan.		
	P02(01) 11 - Pentadbir Media Sosial MPK		
	Pentadbir Media Sosial MPK adalah bertangggungjawab mentadbir media sosial MPK dan seterusnya melaksanakan pematuhan DKICT MPKlang. Peranan dan tanggungjawab Pentadbir Media Sosial MPK adalah seperti berikut: (a) maklumkan kepada semua ahli kumpulan, sebab utama kumpulan aplikasi pesanan diwujudkan dan memikirkan sama ada peraturan asas diperlukan; (b) prihatin terhadap peraturan atau syarat-syarat yang digariskan oleh penyedia platform; (c) menegur posting atau komen untuk memastikan perbincangan berada di landasan yang betul; (d) sentiasa semak posting atau komen (dengan seorang moderator, jika boleh); (e) mempertimbangkan untuk mengeluarkan atau menyekat mereka yang terus membuat posting atau komen jelik; dan (f) melaporkan sebarang pelanggaran polisi penggunaan yang sedang berkuatkuasa.		
	P02(01) 12 – Pengguna	**Tindakan**	
	Pengguna merupakan pihak yang menggunakan aset ICT Majlis Perbandaran Klang iaitu Warga kerja Majlis Perbandaran Klang dan pihak ketiga yang terdiri daripada pembekal, perunding dan lain-lain berkaitan. Pengguna mempunyai peranan dan tanggungjawab seperti berikut: -	Pengguna	

(a) Warga Kerja Majlis Perbandaran Klang dan pihak ketiga dikehendaki membaca, memahami dan mematuhi Dasar Keselamatan ICT MPKlang; (b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan maklumat rasmi terperingkat; (d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT MPKlang dan menjaga kerahsiaan maklumat MPKlang; (e) Menghadiri program-program kesedaran dan pembudayaan keselamatan ICT; (f) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MPKlang sebagaimana **Lampiran 1**. (g) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; (h) 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; iv) Menjaga kerahsiaan kata laluan; v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan; vi) Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemerosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan; dan vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	
P02(01) 13 – Jawatankuasa Keselamatan ICT (JKICT)	**Tindakan**
Jawatankuasa Keselamatan ICT (JKICT) adalah Jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT MPKlang. Di MPKlang, Keahlian Jawatankuasa JKICT adalah sama dengan: i) Jawatankuasa Pemandu ICT (JPICT) ii) Jawatankuasa Pemandu Sistem Pengurusan Keselamatan Maklumat (Information Security Management System – ISMS) **Pengerusi:** Yang Dipertua MPKlang/CDO **Ahli:** (1) Semua Ketua Jabatan; (2) Pegawai Keselamatan (Urusetia Keselamatan); (3) Pengarah Kesihatan (urusetia OSHA); (4) Pengarah Teknologi Maklumat (Urusetia Keselamatan ICT); (5) Pegawai Keselamatan ICT (ICTSO); dan **Urus Setia:** Jabatan Teknologi Maklumat	JKICT/JPICT/ Mesyuarat Pengurusan

Sekiranya Mesyuarat JKICT tidak bersidang, fungsi JKICT boleh dijadikan agenda tetap di dalam Mesyuarat Jawatankuasa Pemandu ICT (JPICT) dan mesyuarat Pengurusan Majlis Perbandaran Klang. **Bidang kuasa:** a) Menentukan arah tuju keselamatan ICT Majlis Perbandaran Klang; b) Menilai, Memperaku/meluluskan Dokumen DKICT MPKlang; c) Memantau tahap pematuhan keselamatan ICT; d) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam MPKlang yang mematuhi keperluan DKICT MPKlang; e) Memantau tahap pematuhan keselamatan ICT; f) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam MPKlang yang mematuhi keperluan DKICT MPKlang; g) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; h) Memastikan DKICT MPKlang selaras dengan dasar-dasar ICT kerajaan semasa; i) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; j) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden. k) Membincang tindakan yang melibatkan pelanggaran DKICT MPKlang; l) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden; m) Memastikan pengauditan sistem ICT Majlis Perbandaran Klang dilaksanakan; n) Menyemak semula sistem ICT supaya sentiasa mematuhi keperluan DKICT MPKlang; dan o) Bekerjasama dengan CSIRT MPKlang untuk mendapatkan maklum balas dan maklumat insiden untuk tindakan pengemaskinian DKICT MPKlang.	
P02(01) 14 – Pasukan Tindak Balas Insiden Keselamatan Siber Majlis Perbandaran Klang (CSIRT MPKLANG)	**Tindakan**
Jawatankuasa Tindak Balas Insiden Keselamatan Siber (CSIRT MPKlang) adalah Jawatankuasa yang bertanggungjawab dalam menangani insiden keselamatan ICT di Majlis Perbandaran Klang. Keanggotaan CSIRT MPKlang adalah seperti berikut: - **Pengarah:** Pengarah Teknologi Maklumat **Pengurus**: Pegawai Teknologi Maklumat (ICTSO) **Ahli :** (1) Semua Ketua Bahagian Teknologi Maklumat; (2) Penolong Pegawai Teknologi Maklumat berkaitan; (3) Semua Wakil jabatan/bahagian yang telah dilantik; **Urusetia** : Jabatan Teknologi Maklumat Majlis Perbandaran Klang.	CSIRT MPKlang

Peranan dan Tanggungjawab CSIRT MPKlang adalah seperti berikut: i) Menerima aduan keselamatan ICT dan menilai tahap dan jenis insiden; ii) Merekod dan menjalankan siasatan awal insiden yang diterima; iii) Menangani tindakbalas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; iv) Menghubungi dan melaporkan kepada ICTSO dan NACSA sama ada sebagai input untuk pemakluman atau untuk tindakan seterusnya; v) Merujuk jabatan-jabatan berkaitan untuk mengambil tindakan pemulihan dan pengukuhan;	
P02(01) 15 Jawatankuasa Pelaksana ISMS	**Tindakan**
Penyelaras berperanan merancang dan menyelaras Pensijilan ISMS seperti: a) merancang dan menyelaras struktur organisasi ISMS b) merancang dan menyelaras kursus kesedaran ISMS c) merancang skop ISMS d) melaksanakan analisis jurang e) membantu Pasukan Pelaksana menyediakan penyataan dasar ISMS, Statement of Applicability (SoA), penilaian risiko, risk treatment plan, kaedah pengukuran kawalan dan prosedur-prosedur ISMS; f) menyelaras permohonan pensijilan g) mengemukakan isu dan masalah ISMS sekiranya ada; dan h) membantu mengukur keberkesanan kawalan dan pelaksanaan ISMS Pasukan Kerja berperanan melaksana ISMS seperti: a) mengurus struktur organisasi ISMS, b) menghadiri kursus kesedaran ISMS dan kursus pelaksanaan standard MS ISO/IEC 27001:2013 ISMS, c) menyediakan skop ISMS, d) melaksanakan analisis jurang, e) menyedia dan melaksanakan dasar ISMS, jadual pelaksanaan, Statement of Applicability (SoA), penilaian risiko, risk treatment plan dan prosedur-prosedur, f) melaksanakan prosedur dan kawalan dalam MS ISO/IEC 27001:2013 ISMS g) membangun dan mengurus dokumen ISMS, h) membuat permohonan pensijilan, i) Mengenalpasti isu dan masalah ISMS sekiranya ada, j) melaksanakan tindakan pembetulan / penambahbaikan dan pencegahan, k) mengenal pasti kaedah dan melaksana pengukuran keberkesanan kawalan ISMS, l) memantau dan menyemak semula ISMS, dan m) melaksanakan peranan sebagai auditee ISMS Majlis Perbandaran Klang perkhidmatan operasi Pusat Data.	Pasukan Pelaksana ISMS

P02(02) Pihak Ketiga	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).	
P02(02) 01 – Keperluan Keselamatan Kontrak dengan Pihak Ketiga	**Tindakan**
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPKlang; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; (d) Akses kepada aset ICT MPKlang perlu berlandaskan kepada perjanjian kontrak; (e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. Dasar Keselamatan ICT MPKlang; ii. Tapisan Keselamatan; iii. *Non-Discloure Agreement* (NDA); iv. Akta Kawasan Larangan dan Tempat Larangan 1959; v. Perakuan Akta Rahsia Rasmi 1972; vi. Arahan Teknologi Maklumat 2007; vii. Hak Harta Intelek; dan viii. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MPKlang sebagaimana di **Lampiran 1**.	CDO; Pengurus ICT; ICTSO; Pentadbir Sistem; Pihak Ketiga

PERKARA 03 – PENGURUSAN ASET

P03(01) Akauntabiliti Aset ICT	
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MPKlang.	
P03(01) 01 – Inventori Aset ICT	**Tindakan**
Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemaskini; (b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;	Pegawai Aset Jabatan/ Bahagian dan Pengguna

(c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MPKlang; (d) Peraturan bagi pengendalian aset ICT hendaklah dikenalpasti, didokumen dan dilaksanakan; dan (e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya. (f) Sebarang perlanggaran dan penyalahgunaan aset hendaklah dilaporkan kepada pegawai Aset/ICTSO	
P03(02) Pengelasan dan Pengendalian Aset ICT	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
P03(02) 01 – Pengelasan Maklumat	**Tindakan**
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad.	Semua
P03(02) 02 – Pengendalian Maklumat	**Tindakan**
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;	Semua

(b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) Menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. (h) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian/sistem. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (i) Mengadakan program dan prosedur jaminan kualiti ke atas perisian/system yang dibangunkan; dan	

(j) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus. (k) Mengawal penghantaran makumat melalui pos, faks, e-mel dan media baharu seperti Facebook, WhatsApp, Twitter, YouTube dan Instagram; dan (l) Mengawal penghantaran maklumat melalui percakapan termasuk melalui telefon bimbit, mel suara, mesin menjawab telefon dan VoIP.	

PERKARA 04 – KESELAMATAN SUMBER MANUSIA

P04(01) Keselamatan Sumber Manusia Dalam Tugas Harian	
Objektif: Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan MPKlang, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga MPKlang hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.	
P04(01) 01 – Sebelum Perkhidmatan	**Tindakan**
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan MPKlang serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan MPKlang serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan; dan (d) Memenuhi keperluan prosedur keselamatan (NDA) bagi pembekal, pakar runding dan pihak-pihak lain yang berkepentingan selaras dengan keperluan perkhidmatan.	Semua
P04(01) 02 – Dalam Perkhidmatan	**Tindakan**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan pegawai dan kakitangan MPKlang serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MPKlang; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MPKlang secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan MPKlang serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh MPKlang; dan	Semua

(d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Latihan, Jabatan Khidmat Pengurusan atau Jabatan Teknologi Maklumat MPKlang.	

P04(01) 03 – Bertukar Alamat atau Tamat Perkhidmatan	**Tindakan**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada MPKlang mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh MPKlang dan/atau terma perkhidmatan.	Semua

P04(02) Program Pembudayaan Keselamatan ICT

Objektif:
Memastikan sumber-seumber manusia yang terlibat termasuk pegawai, kakitangan MPKlang dan pihak-pihak yang berkepentingan memperolehi latihan yang mencukupi dan melibatkan mereka dalam program kesedaran dan pembudayaan ICT.

P04(02) 01 – Kursus Keselamatan ICT	**Tindakan**
Kursus dan latihan kakitangan hendaklah disediakan dan memastikan kakitangan menerima latihan keselamatan ICT yang mencukupi secara berterusan untuk dilaksanakan di dalam tugas harian mereka.	Semua

P04(02) 02 - Program Kesedaran Dan Pembudayaan	**Tindakan**
Program kesedaran dan pembudayaan keselamatan ICT seperti taklimat dan seminar mengenai pentingnya keselamatan ICT dititikberatkan serta kesan-kesannya sekiranya diabaikan hendaklah diadakan secara kerap dan menyeluruh di kalangan kakitangan. Program menangani insiden keselamatan ICT juga penting untuk memastikan kakitangan dapat bertindak segera dan sewajarnya sekiranya ia berlaku.	Semua

PERKARA 05 – KESELAMATAN FIZIKAL DAN PERSEKITARAN

P05(01) Keselamatan Kawasan

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

P05(01) 01 – Kawalan Kawasan	Tindakan
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (c) Memasang alat penggera atau kamera; (d) Mengehadkan jalan keluar masuk; (e) Mengadakan kaunter kawalan; (f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; (g) Mewujudkan perkhidmatan kawalan keselamatan; (h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (i) Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (j) Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; (k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Pegawai Keselamatan MPKlang, Ketua Jabatan, CDO, ICTSO

P05(01) 02 – Kawalan Masuk Fizikal	Tindakan
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: - (a) Setiap pengguna MPKlang hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan balik kepada MPKlang apabila pengguna berhenti atau bersara; (c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan dikembalikan semula selepas tamat urusan/lawatan; Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pengguna berhenti atau bersara; (d) Setiap pelawat hendaklah mendaftar di Kaunter Keselamatan di Lobi Pejabat Majlis Perbandaran Klang terlebih dahulu; dan (e) Kehilangan pas mestilah dilaporkan dengan segera;	Semua dan Pelawat

P05(01) 03 – Kawasan Larangan	Tindakan
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di kawasan tersebut. Kawasan larangan di MPKlang adalah : (a) Bilik Yang Dipertua; (b) Bilik Setiausaha, (c) Semua Bilik Ketua Jabatan; (d) Pusat Data (e) Semua Bilik Server; (f) Semua Bilik Rangkaian; (g) Semua Bilik Keselamatan; (h) Semua Bilik Kebal (i) Semua Bilik Fail; (j) Semua Stor; (k) Bilik NOC (l) Bilik Operasi; dan (m) Mana-mana kawasan yang diishtiharkan sebagai kawasan larangan; Kawalan keselamatan bagi melindungi kawasan ini daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam adalah seperti berikut : (a) Akses kepada bilik-bilik tersebut hanyalah kepada pegawai yang diberi kuasa sahaja; (b) Pihak ketiga adalah dilarang sama sekali untuk memasuki 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 dan mestilah mendapat kebenaran daripada Ketua Jabatan; (c) Butiran pihak ketiga atau pelawat yang keluar masuk ke kawasan larangan hendaklah direkodkan; (d) Pemantauan hendaklah dibuat menggunakan kaedah atau peralatan yang sesuai (CCTV, Log Akses dan lain-lain); (e) Peralatan keselamatan hendaklah diperiksa dan diselenggara secara berkala; (f) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; (g) Memperkukuhkan dinding dan siling untuk menghalang pencerobohan dan risiko kesemamatan; (h) Menghadkan jalan keluar masuk; (i) Mengadakan kaunter kawalan; (j) Menyediakan tempat atau bilik khas untuk pelawat; dan (k) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan dan laluan awam;	Semua
P05(01) 04 – Keselamatan Pusat Data	**Tindakan**
Semua server hendaklah diletakkan di dalam Pusat Data bagi memastikan ia sentiasa selamat daripada pencerobohan atau sebarang ancama dan membolehkan ia dicapai sepanjang masa.	

Langkah-langkah kawalan Pusat Data bagi melindungi server adalah seperti berikut : (a) Pemantauan dan pengawalan keluar masuk pengguna ke Pusat Data melalui sistem *Security Access Door*; (b) Hanya pengguna yang mempunyai kad access door sahaja yang dibenarkan memasuki Pusat Data; (c) Memastikan Pusat Data sentiasa bersih dan Server-server tidak terdedah kepada habuk; (d) Menyediakan Uninterruptible Power Suply (UPS) sebagai sokongan bekalan elektrik; (e) Menyediakan kemudahan Pendingin Hawa Khas yang tidak bersambung dengan pendingin Hawa Bangunan. (f) Pendingin hawa mestilah berfungsi dengan baik. (g) Menyediakan kemudahan perlindungan suhu bagi memastikan suhu adalah bersesuaian dengan Pusat Data; dan (h) Semua peralatan dan sistem keselamatan seperti *Security Access door*, *Firewall*, UPS dan Pendingin Hawa mestilah diselenggarakan secara berkala.	Pentadbir Pusat Data; ICTSO; Pengurus ICT (PJTM);
P05(02) Keselamatan Peralatan	
Objektif: Melindungi peralatan ICT MPKlang dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
P05(02) 01 – Peralatan ICT	**Tindakan**
Perkara-perkara yang mesti dipatuhi bagi memastikan keselamatan peralatan ICT terjamin adalah seperti berikut: (a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (b) Pengguna bertanggungjawab sepenuhnya ke atas peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang peralatan ICT yang telah ditetapkan; (d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; (e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemaskini di samping melakukan imbasan ke atas media storan yang digunakan; (g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; (i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS);	Semua

(j) UPS yang berkuasa tinggi perlu diletakkan di bilik yang berasingan, bersuhu rendah dan dilengkapi dengan pengudaraan yang sesuai; (k) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; (l) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; (m) Peralatan ICT yang hendak dibawa keluar dari premis MPKlang, perlulah mendapat Pengesahan Ketua Jabatan dan kelulusan Pengurus ICT dan hendaklah direkodkan bagi tujuan pemantauan; (n) Keselamatan dan sebarang kehilangan peralatan adalah di bawah tanggungjawab individu yang membawa keluar peralatan tersebut; (o) Peralatan ICT yang hilang hendaklah dilaporkan kepada Pengurus ICT dan Pegawai Aset dengan segera; (p) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa; (q) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pengurus ICT; (r) Sebarang kerosakan peralatan ICT hendaklah dilaporkan ke Jabatan Teknologi Maklumat (JTM) pembaikan; (s) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (t) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; (u) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT; (v) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (w) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; (x) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan (y) Memastikan plag dicabut daripada suis utama (*main switch*) sebelum meninggalkan pejabat bagi mengelakkan kerosakan perkakasan jika berlaku kejadian seperti petir, kilat dan sebagainya;	
P05(02) 02 – Media Storan	**Tindakan**
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; (b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja	Semua

(c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; (e) Akses dan pergerakan media storan hendaklah direkodkan; (f) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; (g) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; (h) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan (i) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
P05(02) 03 – Media Tandatangan Digital	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan (c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Semua
P05(02) 04 – Media Perisian dan Aplikasi	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MPKlang; (b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; (c) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada *CD-rom, disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan (d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua
P05(02) 05 – Penyelenggaraan Peralatan ICT	**Tindakan**
Peralatan ICT hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; (b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan	Pegawai Aset ICT, Jabatan Teknologi Maklumat

(d) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (e) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (f) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (g) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	
P05(02) 06 – Peralatan ICT di Luar Premis	**Tindakan**
Peralatan yang dibawa keluar dari premis MPKlang adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (c) Keselamatan dan sebarang kehilangan peralatan adalah di bawah tanggungjawab individu yang membawa keluar peralatan tersebut;	Semua
P05(02) 07 – Pelupusan Peralatan ICT	**Tindakan**
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MPKlang dan ditempatkan di MPKlang. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MPKlang. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; (b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; (c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; (d) Pegawai Aset ICT hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (f) Pegawai Aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori Aset ICT; (g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan (h) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:	Semua, Pegawai Aset ICT Jabatan Teknologi Maklumat

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MPKlang; iii. Memindah keluar dari MPKlang mana-mana peralatan ICT yang hendak dilupuskan; dan iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan adalah di bawah tanggungjawab MPKlang.	
P05(02) 08 – Pinjaman Peralatan ICT	**Tindakan**
Peralatan ICT termasuklah projektor, komputer riba, PC, pencetak, dan aksesori yang berkaitan seperti kabel komputer dan sebagainya, adalah di bawah tanggungan JTM. Oleh itu setiapperalatan yang dipinjam atau dibawa keluar atau masuk dikehendaki mengikut prosedur berikut: (a) Memohon kepada JTM untuk membuat peminjaman peralatan yang diperlukan; (b) Pengguna dikehendaki menggunakan Borang Kebenaran Membawa Keluar Peralatan ICT Jabatan yang disediakan oleh JTM; (c) Peminjam dikehendaki menandatangani Kad Daftar Pergerakan Harta Modal dan Inventori sebelum peralatan dibawa keluar; (d) Peralatan yang dipinjam perlulah dikembalikan setelah sselesai menggunakannya untuk semakan dan simpanan; (e) Peminjam adalah bertanggungjawab untuk memastikan ke semua peralatan dikembalikan dengan sempurna, lengkap dan selamat; dan (f) Sebarang kerosakan dan kegagalan peralatan untuk berfungsi dengan baik hendaklah dilaporkan kepada Helpdesk ICT dengan segera.	Semua
P05(03) Keselamatan Persekitaran	
Objektif: Melindungi aset ICT MPKlang dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
P05(03) 01 – Kawalan Persekitaran	**Tindakan**
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO). Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi:	Semua

(a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti 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; (b) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; (c) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; (d) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; (e) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; (f) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan (g) Akses kepada saluran *riser* hendaklah sentiasa dikunci; dan (h) Memastikan Pegawai yang bertanggungjawab menyimpan kunci dapat dihubungi bila manakeadaan memerlukan berbuat demikian.	
P05(03) 02 – Bekalan Kuasa	**Tindakan**
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; (b) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) hendaklah digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan (c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Semua
P05(03) 03 – Kabel	**Tindakan**
Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	JTM dan ICTSO

P05(03) 04 – Prosedur Kecemasan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MPKlang; dan (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan MPKlang.	Semua

P05(04) Keselamatan Dokumen

Objektif:
Melindungi maklumat MPKlang dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.

P05(04) 01 – Dokumen	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan (e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik. (f) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; dan (g) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada;	Semua

PERKARA 06 – PENGURUSAN OPERASI DAN KOMUNIKASI

P06(01) Pengurusan Prosedur Operasi	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
P06(01) 01 – Pengendalian Prosedur Operasi	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur pengurusan operasi yang diwujud, dikenalpasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua
P06(01) 02 – Kawalan Perubahan	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod mengunakan borang kawalan perubahan dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua
P06(01) 03 – Pengasingan Tugas dan Tanggungjawab	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan	Pengurus ICT; ICTSO

(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.	
P06(01) 04 – Prosedur Pengurusan Insiden	**Tindakan**
Pasukan CSIRT MPKlang diketuai oleh Pengurus ICT (PJTM) bertindak menangani insiden Keselamatan Siber yang berlaku di MPK mengikut prosedur Pengurusan Insiden seperti berikut : (a) menerima aduan keselamatan ICT daripada pengguna, laporan yang dikesan melalui peralatan/perisian keselamatan atau laporan dari sumber luar; (b) Maklumat insiden didaftarkan untuk tindakan lanjut; (c) Menjalankan siasatan awal bagi mengenalpasti insiden tersebut; (d) Laporan insiden dimaklumkan kepada NACSA; (e) Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan hendaklah dipanjangkan kepada penguatkuasa agensi undang-undang; (f) Pasukan CSIRT MKlang mengambil tindakan menangani insiden secara capaian jarak jauh (*remote*) atau *on-site*; (g) Sekiranya laporan tersebut memerlukan bantuan NACSA, permohonan akan dihantar bagi mendapatkan maklumbalas NACSA; (h) Bagi laporan yang memerlukan bantuan dari CSIRT agensi lain, permohonan akan dihantar melalui NACSA bagi mendapatkan khidmat nasihat melalui saluran yang betul; (i) Laporan akan disediakan oleh ICTSO dan ICTSO perlu mendapatkan pengesahan daripada Pengurus ICT/CDO sekiranya Pelan Kesinambungan Perkhidmatan (BCP) perlu diaktifkan atau sebaliknya; dan (j) Laporan Insiden yang tidak memerlukan BCP akan terus diambil tindakan bagi tujuan pemulihan;	Pengurus ICT (PJTM) dan ICTSO
P06(02) 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.	
P06(02) 01 – Perkhidmatan Penyampaian	**Tindakan**
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

P06(03) Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
P06(03) 01 – Perancangan Keupayaan	**Tindakan**
Keupayaan/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 keupayaan/kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem ICT dan ICTSO
P06(03) 02 – Penerimaan Sistem	**Tindakan**
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Kriteria ini hendaklah merangkumi perkara berikut: - (a) Memenuhi kehendak dan keperluan pengguna; (b) Menggunakan perisian pembangunan yang sah; (c) Menggunakan teknologi terkini; (d) Memenuhi ciri-ciri keselamatan bagi mengelakkan risiko pencerobohan dan sebagainya (e) Memenuhi keperluan-keperluan teknologi semasa dan akan datang (contoh: berkeupayaan menggunakan pelbagai *platform*, *IPV6 ready*)	Pentadbir Sistem ICT dan ICTSO
P06(04) Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya.	
P06(04) 01 – Perlindungan daripada Perisian Berbahaya	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; (c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; (d) Sentiasa Mengemaskini anti virus dan perisian keselamatan dengan *pattern* terkini;	Semua

(e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan (i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
P06(04) 02 – Perlindungan dari *Mobile Code*	**Tindakan**
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pentadbir Sistem ICT
P06(05) *Housekeeping*	
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
P06(05) 01 – *Backup*	**Tindakan**
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; (c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; (d) *Backup* hendaklah dilaksanakan secara berjadual secara harian, mingguan, bulanan dan tahunan mengikut jadual yang ditetapkan; dan (e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	Pentadbir Sistem ICT; Pentadbir Pusat Data;
P06(06) Pengurusan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
P06(06) 01 – Kawalan Infrastruktur Rangkaian	**Tindakan**
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;	JTM

(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 serta dikonfigurasi dan diselia oleh Pengurus ICT; (f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan rangkaian MPKlang; (g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; (h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MPKlang; (i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; (j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan MPKlang adalah tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian MPKlang sahaja dan penggunaan modem adalah dilarang samasekali; dan Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan	
P06(07) Pengurusan Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
P06(07) 01 – Penghantaran dan Pemindahan	**Tindakan**
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pengarah Teknologi Maklumat/pemilik terlebih dahulu.	Semua
P06(07) 02 – Prosedur Pengendalian Media	**Tindakan**
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Menyimpan semua media di tempat yang selamat; dan (f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat	Semua

P06(07) 03 – Keselamatan Sistem Dokumentasi	Tindakan
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan (c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Semua

P06(08) Pengurusan Pertukaran Maklumat

Objektif:
Memastikan keselamatan pertukaran maklumat dan perisian antara MPKlang dan agensi luar terjamin.

P06(08) 01 – Pertukaran maklumat	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; (b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara MPKlang dengan pihak luar; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MPKlang; dan (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua

P06(08) 02 – Pengurusan Mel Elektronik (E-Mel)	Tindakan
Penggunaan Mel Elektronik (E-mel) di MPKlang 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*", Manual MPK Tahun 2013 *"Manual Pengurusan Aplikasi E-Mel Rasmi"* yang dikeluarkan pada 01 Januari 2013 dan mana-mana undang-undang bertulis yang berkuat kuasa. Antara perkara-perkara yang perlu dipatuhi dalam pengendalian E-mel adalah seperti berikut: (a) Permohonan E-mel hendaklah melalui ketua jabatan masing-masing dengan melengkapkan Borang Pengurusan E-mel Rasmi Majlis Perbandaran Klang yang boleh diperolehi dari JTM atau Portal Staf MPKlang; (b) Hanya kakitangan dan Ahli Majlis sahaja boleh dipertimbangkan untuk mendapat kemudahan E-mel rasmi jabatan dan kelayakan diberi kepada kumpulan gred yang telah ditentukan; (c) Penggunaan alamat E-mel rasmi MPKlang bagi pendaftaran dalam mana-mana web/kumpulan/forum yang tidak berkaitan dengan urusan kerja rasmi adalah **DILARANG SAMA SEKALI**;	Semua

(d) Penghantaran E-mel rasmi hendaklah menggunakan akaun E-mel yang telah diperuntukkan oleh MPKlang sahaja dan pastikan alamat E-mel penerima adalah betul; (e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah **DILARANG;** (f) Pengguna hendaklah memastikan setiap E-mel yang disediakan mematuhi format yang telah ditentukan sebelum dihantar kepada penerima; (g) Pengguna hendaklah memastikan subjek dan kandungan E-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; (h) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10MB) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; (i) Pengguna hendaklah mengelak dari membuka E-mel daripada penghantar yang tidak diketahui atau diragui; (j) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum transaksi maklumat melalui E-mel; (k) Pengguna hendaklah memastikan alamat E-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; (l) Pengguna hendaklah memastikan dan menentukan tarikh dan masa sistem komputer adalah tepat; (m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbo*x* masing-masing; (n) Setiap E-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; (o) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; (p) Mengambil tindakan dan memberi maklum balas terhadap E-mel dengan cepat dan mengambil tindakan segera; dan (q) Bahagian Sumber Manusia Jabatan Khidmat Pengurusan hendaklah memaklumkan sebarang status pengguna (bertukar jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke Majlis Perbandaran Klang) bagi tujuan pengemaskinian E-mel terlibat. Perlanggaran pada mana-mana peraturan boleh menyebabkan penggantungan akaun pengguna atau mana-mana tatatertib yang bersesuaian.	Semua
P06(09) Perkhidmatan Elektronik	
Objektif: Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
P06(09) 01 – E-Perkhidmatan	**Tindakan**
Bagi menggalakkan pertumbuhan e-perkhidmatan serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet.	Semua

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat yang terlibat dalam e-perkhidmatan perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; (b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	
P06(09) 02 – Maklumat Umum	**Tindakan**
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: (a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; (b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan (c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua
P06(10) Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
P06(10) 01 – Pengauditan dan Semakan ICT	**Tindakan**
ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT MPKlang; (b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery*, *phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; (g) Aktiviti penyalahgunaan akaun e-mel; dan (h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian ICT dan kelulusan Pengarah Teknologi Maklumat selaku Pengurus ICT.	ICTSO

P06(10) 02 – Jejak Audit	Tindakan
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi; (b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Pengendalian Jejak audit hendaklah memastikan perkara-perkara berikut:- ▪ Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. ▪ Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. ▪ Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem ICT
P06(10) 03 – Sistem Log	**Tindakan**
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan Pengurus ICT.	Pentadbir Sistem ICT
P06(10) 04 – Pemantauan Log	**Tindakan**
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;	Pentadbir Sistem ICT, Pentadbir Rangkaian ICT, ICTSO

(e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MPKlang atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	

PERKARA 07 – KAWALAN CAPAIAN

P07(01) Dasar Kawalan Capaian	
Objektif: Mengawal capaian ke atas maklumat yang menggunakan aset ICT MPKlang.	
P07(01) 01 – Keperluan Kawalan Capaian	**Tindakan**
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan (d) Kawalan ke atas kemudahan pemprosesan maklumat.	JTM, ICTSO
P07(02) Pengurusan Capaian Pengguna	
Objektif : Mengawal capaian pengguna ke atas aset ICT MPKlang.	
P07(02) 01 – Akaun Pengguna	**Tindakan**
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenai pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem ICT dikehendaki mematuhi langkah-langkah berikut: (a) Akaun yang diperuntukkan oleh MPKlang sahaja boleh digunakan; (b) Akaun pengguna (*user ID*) mestilah unik dan hendaklah mencerminkan identiti pengguna; (c) Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; (d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan MPKlang. Akaun boleh ditarik balik jika kaedah penggunaannya melanggar peraturan; (e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah **DILARANG**; dan	Semua, Pentadbir Sistem ICT

(f) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Pengguna yang bercuti panjang atau berkursus luar pejabat dalam tempoh waktu melebihi 30 hari (sebulan); ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	
P07(02) 02 – Hak Capaian	**Tindakan**
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
P07(02) 03 – Kajian Semula Hak Akses Pengguna (*Review of User Access Rights*)	**Tindakan**
(a) Pemilik aset hendaklah menyemak hak akses pengguna sekurang-kurangnya 1 TAHUN sekali. (b) Hak akses warga MPKLANG dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam MPKLANG	Pemilik Sistem, Pentadbir Sistem ICT
P07(02) 04 – Pengurusan Kata Laluan	**Tindakan**
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 MPKlang 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 Sembilan (9) aksara dan maksimum dua belas (12) aksara dengan gabungan aksara, angka dan aksara khusus; (d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun; (e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (f) Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; (g) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula; (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (i) Tentukan had masa pengesahan selama dua (2) minit atau mengikut kesesuaian sistem dan selepas had itu, sesi ditamatkan; (j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian;	Semua, Pentadbir Sistem ICT

(k) Mengelakkan penggunaan semula kata laluan yang baru digunakan. (l) Kata laluan paparan kunci (lock screen) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (m) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum TIGA (3) KALI sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga ID capaian diaktifkan semula; dan (n) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	

P07(02) 05 – *Clear Desk* dan *Clear Screen*	**Tindakan**
Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat dalam apa jua bentuk media disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	Semua
P07(03) Kawalan Capaian Rangkaian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
P07(03) 01 – Capaian Rangkaian	**Tindakan**
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MPKlang, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Semua, Pentadbir Rangkaian ICT, ICTSO
P07(03) 02 – Capaian Internet	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet di MPKlang hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian ICT bagi memastikan penggunaannya untuk tujuan capaian	Semua, Pentadbir Rangkaian ICT, ICTSO

yang dibenarkan sahaja untuk melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MPKlang; (b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; (c) Penggunaan teknologi yang bersesuaian seperti *packet shaper* untuk mengawal aktiviti *video conferencing*, *video streaming*, *chat*, *downloading* dan lain-lain aktiviti berkaitan adalah perlu bagi menguruskan penggunaan jalur lebar (*broadband*) yang maksimum dan lebih berkesan; (d) Penggunaan Internet hanyalah untuk **KEGUNAAN RASMI SAHAJA**. Walaupun kemudahan Internet dibuka kepada semua kakitangan, Ketua Jabatan berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya dengan memajukan kepada Pengurus ICT untuk tindakan; (e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengarah/ pegawai yang diberi kuasa; (f) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; (g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet; (h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; (i) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MPKlang; (j) 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; (k) Penggunaan modem untuk tujuan sambungan ke Internet **TIDAK DIBENARKAN SAMA SEKALI** melainkan dengan kelulusan dan pengesahan; dan (l) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	
P07(03) 02 – *Bring Your Own Device (BYOD)*	**Tindakan**
BYOD merupakan peralatan mudah alih persendirian seperti telefon pintar, tablet dan laptop yang digunakan oleh pengguna yang melaksanakan tugas rasmi melalui sambungan rangkaian Jabatan. Pengguna yang menggunakan kemudahan wifi jabatan atau data line persendirian untuk akses kepada Internet tertakluk kepada DKICT. Sebagai garis panduan, pengguna bertanggungjawab memastikan langkah-langkah keselamatan perlindungan berkaitan penggunaan BYOD seperti berikut: (a) mengelakkan risiko kebocoran maklumat rasmi; (b) mengelakkan ancaman risiko keselamatan ICT; (c) memastikan produktiviti pengguna tidak terjejas dalam menjalankan urusan rasmi jabatan; dan (d) meningkatkan integriti data.	Semua, Pentadbir Rangkaian ICT, ICTSO

Bagi mengawal dan memantau pelaksanaan BYOD, mekanisme kawalan diwujudkan seperti berikut: (a) mendaftarkan penggunaan peralatan mudah alih yang digunakan melalui *active directory*; (b) mengaktifkan fungsi keselamatan kata laluan bagi mengelakkan akses yang tidak dibenarkan; dan (c) melaporkan kehilangan peralatan mudah alih kepada ICTSO. (d) pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD. Pengguna BYOD adalah dilarang daripada melakukan perkara-perkara berikut: (a) Menggunakan peranti untuk mengakses, menyimpan dan menyebarkan maklumat rasmi kepada pihak yang tidak dibenarkan; (b) Menggunakan peranti untuk tujuan peribadi yang boleh mengganggu produktiviti (c) kerja; (d) Menjadikan peranti sebagai medium sandaran (backup) daripada komputer bagi menyimpan maklumat rasmi MPKLANG; (e) Membuat rakaman, mengedar, menyalin audio dan video rasmi untuk tujuan (f) peribadi; (g) Menjadikan peranti sebagai access point kepada aset ICT jabatan untuk capaian ke Internet yang menyebabkan pelanggaran kepada keselamatan ICT; dan (h) Mengabaikan keselamatan peranti dengan sengaja seperti peralatan mudah alih tidak disimpan di tempat yang selamat apabila tidak digunakan.	

P07(04) Kawalan Capaian Sistem Pengoperasian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
P07(04) 01 – Capaian Sistem Pengoperasian	**Tindakan**
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; dan (c) Menghadkan masa penggunaan rangkaian bagi pengguna. Kaedah-kaedah yang digunakan hendaklah berupaya menyokong perkara-perkara berikut: (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; (b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* dan (c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. (d) Menyediakan tempoh penggunaan mengikut kesesuaian	Semua, Pentadbir Rangkaian ICT, ICTSO

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Menghadkan dan mengawal penggunaan program utiliti bagi satu tempoh yang ditetapkan; dan (d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
P07(04) 02 – Kad Pintar	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan kad pintar (sekiranya ada) hendaklah digunakan bagi capaian sistem yang dikhususkan; (b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; (c) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan hendaklah disekat; dan (d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Jabatan Teknologi Maklumat, MPKlang.	Semua

P07(05) Kawalan Capaian Aplikasi dan Maklumat

Objektif:
Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi

P07(05) 01 – Capaian Aplikasi dan Maklumat	**Tindakan**
Bertujuan melindungi aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian aplikasi dan maklumat di MPKlang adalah terhad kepada pengguna yang dibenarkan dan tujuan yang ditentukan berdasarkan kategori pengguna. Bagi memastikan kawalan capaian aplikasi dan maklumat adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: (a) Pengguna hanya boleh mengakses aplikasi dan maklumat yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; (b) Setiap aktiviti capaian aplikasi dan maklumat oleh pengguna hendaklah direkodkan (sistem log) bagi mengesan aktiviti yang tidak diingini; (c) Menghadkan capaian aplikasi dan maklumat kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; (d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan (e) Capaian aplikasi dan maklumat melalui jarak jauh adalah terhad kepada perkhidmatan yang dibenarkan sahaja	Pentadbir Sistem ICT, ICTSO

P07(06) Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.	
P07(06) 01 – Peralatan Mudah Alih	**Tindakan**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua
P07(06) 02 – Kerja Jarak Jauh (*Remote Access*)	**Tindakan**
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
P07(06) 02 - Perkhidmatan Pengkomputeran Awan Awam (*Public Cloud Computing Service*)	
Perkhidmatan Pengkomputeran Awan Awam menawarkan beberapa kelebihan seperti penjimatan kos, berprestasi tinggi serta membolehkan penyediaan perkhidmatan yang cepat. Sungguhpun begitu tanpa kawalan, penggunaan perkhidmatan ini boleh meningkatkan risiko kehilangan dan kecurian data, capaian tidak sah, penyalahgunaan data peribadi dan organisasi memandangkan aset serta kemudahan pengkomputeran tersebut berada di luar kawalan organisasi. Polisi ini terpakai kepada semua Warga MPKLANG yang menerima dan/atau mengendalikan Maklumat Terperingkat menggunakan mana-mana model perkhidmatan pengkomputeran awan awam yang dinyatakan di seperti berikut: (a) **Perisian Sebagai Perkhidmatan *(Software-as-a-Service (SaaS)*)** Perkhidmatan ini menyediakan keupayaan untuk menggunakan perisian di awan dan pengguna boleh mengakses melalui Internet. Contoh perkhidmatan ini adalah seperti email percuma (Gmail, Yahoo Mail, Hotmail dan Microsoft Outlook); perkhidmatan simpanan awan (Google Drive, Dropbox, One Drive Cloud, iCloud Drive dan Pocket Data); media sosial (Facebook, Twitter, Instagram, YouTube, TikTok dan Reddit); dan Microsoft Office 365. (b) **Infrastruktur sebagai Perkhidmatan *(Infrastructure-as-as-Service (IaaS)*)** Persekitaran asas yang menyediakan sumber pengkomputeran awan seperti *virtual machine, virtual network* dan sebagainya. Di antara contoh perkhidmatan ini adalah seperti DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod dan Microsoft Azure. (c) **Platform sebagai Perkhidmatan *(Platform-as-a-Service (PaaS)*)** Persekitaran pembangunan dan penggunaan perkhidmatan aplikasi yang disediakan untuk pembangun sistem. Contohnya seperti Microsoft Azure dari	Semua

Microsoft, Elastic Compute Cloud (EC2) dari Amazon, Google Application Engine dan e-Learning Platform.

Maklumat

Semua maklumat rasmi milik MPKLANG adalah meliputi pengajaran, pembelajaran, penyelidikan, sumber manusia dan kewangan. Ia juga merangkumi maklumat milik pihak ketiga yang MPKLANG terima/kendali semasa berurusan dengan pihak ketiga seperti agensi-agensi kerajaan lain yang berkaitan.

Maklumat yang dimaksudkan termasuk dalam semua bentuk seperti data mentah, data dari pangkalan data, kod sumber, dokumen, foto, audio, video dan dalam format salinan *(softcopy/hardcopy)*. Maklumat yang dimaksudkan di atas, selepas ini dirujuk sebagai "Maklumat".

Maklumat Terperingkat

Maklumat terperingkat adalah dokumen rasmi yang mengandungi maklumat yang mesti diberi perlindungan keselamatan dan yang bertanda dengan sesuatu peringkat keselamatan sama ada 'Rahsia Besar', 'Rahsia', 'Sulit' atau 'Terhad'. Manakala dokumen tidak terperingkat adalah dokumen rasmi yang mengandungi maklumat rasmi tetapi tidak bertanda dengan peringkat keselamatan.

Berikut adalah peraturan-peraturan yang perlu dipatuhi:

(a) Maklumat Terperingkat adalah dilarang ditempatkan di *public cloud*;
(b) Sekiranya terdapat keperluan menggunakan *public cloud* bagi menempatkan Maklumat Terperingkat, kelulusan BERTULIS dari CDO hendaklah diperolehi terlebih dahulu;
(c) Hanya *public cloud* yang dilanggan dan diterimapakai di peringkat MPKLANG (termasuk tetapi tidak terhad kepada aplikasi Google, Microsoft Office 365, Adobe dan Zoom) dibenarkan untuk diguna bagi tujuan rasmi. Sungguhpun begitu penempatan Maklumat Terperingkat adalah masih tertakluk kepada para (a) dan (b);
(d) Sekiranya terdapat keperluan untuk menggunakan public cloud selain dari yang dinyatakan di para (c), pemilihan Penyedia public cloud hendaklah diluluskan oleh Jawatankuasa Pemandu ICT MPKLANG terlebih dahulu sebelum perkhidmatan tersebut diterimapakai;
(e) *Public cloud* percuma seperti Facebook, Twitter, Instagram, YouTube dan Flickr adalah dibenarkan untuk tujuan rasmi. Sungguhpun begitu penyebaran, perkongsian dan penyimpanan Maklumat Terperingkat di *public cloud* tersebut melalui akaun korporat, masih tertakluk kepada para (a) dan (b).
(f) Penyebaran, perkongsian dan penyimpanan Maklumat Terperingkat MPKLANG di akaun persendirian Facebook, Twitter, Instagram, YouTube, Flickr,LinkedIn, Scribd, SlideShare dan seumpamanya adalah DILARANG;
(g) Sebarang penggunaan *public cloud* hendaklah mematuhi segala peruntukan undang-undang, peraturan, pekeliling, polisi dan arahan-arahan yang dikeluarkan dari semasa ke semasa yang dikuatkuasakan oleh Kerajaan Malaysia dan MPKLANG; dan

(h) Warga MPKLANG hendaklah pada setiap masa menjaga dan mengekalkan integriti serta kerahsiaan segala maklumat selari dengan nilai-nilai teras MPKLANG.	

PERKARA 08 – PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

P08(01) Keselamatan Dalam Membangunkan Sistem dan Aplikasi	
Objektif: Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
P08(01) 01 – Keperluan Keselamatan Sistem Maklumat	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (b) Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan sistem output untuk memastikan data yang telah diproses adalah tepat; (c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan (d) Memastikan semua sistem yang dibangunkan sama ada secara *inhouse* atau *outsource* hendaklah diuji terlebih dahulu dengan *Stress Test*, *Load Test* dan *Penetration Test* bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan. (e) Memastikan Semua sistem yang dibangunkan sama ada secara *inhouse* atau *outsource* menjalani Ujian Penerimaan Pengguna (*User Acceptence Test*); dan (f) Memastikan dokumentasi sistem disediakan bagi semua sistem yang dibangunkan sama ada secara secara *inhouse* atau *outsource*.	Pemilik Sistem, Pentadbir Sistem ICT, ICTSO
P08(01) 02 – Pengesahan Data *Input* dan *Output*	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan (b) Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem, Pentadbir Sistem ICT, ICTSO
P08(01) 03 – Kawalan Prosesan	**Tindakan**
Kawalan Proses dikehendaki diwujudkan di dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan akibat daripada kesilapan pemprosesan atau perlakuan yang disengajakan. Kawalan proses yang diwujudkan hendaklah berkeupayaan menyokong perkara-perkara berikut: (a) Mengesan pengguna yang melakukan pengubahsuaian; (b) Mengesan proses-proses yang telah diubahsuai;	Pentadbir Sistem ICT

(c) Mengenalpasti jenis pengubahsuaian sama ada kesilapan pemprosesan atau perlakuan disengajakan; dan (d) Menjana laporan pengemaskinian/pengubahsuan maklumat.	

P08(02) Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
P08(02) 01 – Penyulitan/Enkripsi	**Tindakan**
Pengguna hendaklah membuat penyulitan/enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
P08(02) 02 – Tandatangan Digital	**Tindakan**
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
P08(02) 03 – Pengurusan Infrastruktur Kunci Awam (PKI)	**Tindakan**
Pengurusan Kunci Awam hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua
P08(03) Keselamatan Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
P08(03) 01 – Kawalan Fail Sistem	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai mengikut prosedur yang telah ditetapkan; (b) Kod atau aturcara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; (c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal, (e) Data ujian perlu dipadamkan dan dikembalikan semula selepas digunakan;dan (f) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem, Pentadbir Sistem ICT
P08(04) Keselamatan Dalam Proses Pembangunan dan Sokongan Sistem	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	

P08(04) 01 – Prosedur Kawalan Perubahan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pihak ketiga (pembekal, perunding, agensi yang dilantik); (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.	Pemilik Sistem; Pentadbir Sistem ICT

P08(04) 02 – Pembangunan Perisian Secara *Outsource*	Tindakan
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh Pemilik Sistem dan Pentadbir Sistem ICT. Kod sumber (*source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik MPKlang.	Pemilik Sistem, Pengurus ICT; Pentadbir Sistem ICT;

P08(05) Kawalan Teknikal Keterdedahan (*Vulnerability*)

Objektif:
Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.

P08(05) 01 – Kawalan dari Ancaman Teknikal	Tindakan
Kawalan maklumat teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan sebagai langkah keselamatan dari ancaman teknikal. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	ICTSO; Pentadbir Sistem ICT

P08(06) Pembangunan Aplikasi Mudah Alih

Objektif :

Menerangkan perkara yang perlu dipatuhi dalam membangunkan aplikasi mudah alih.

P08(06) 01 Prosedur Integrasi Pembangunan Aplikasi Mudah Alih	Tindakan
Pembangunan aplikasi mudah alih yang melibatkan integrasi dengan sistem induk hendaklah menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang tidak memberi risiko ancaman keselamatan.	Pentadbir Sistem ICT

PERKARA 09 – PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

P09(01) Mekanisme Pelaporan Insiden Keselamatan ICT	
Objektif: Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.	
P09(01) 01 – Mekanisme Pelaporan	**Tindakan**
Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan CSIRT MPKlang dengan kadar segera dan semua maklumat adalah SULIT. Insiden keselamatan ICT seperti berikut: (a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Prosedur pelaporan insiden keselamatan ICT berdasarkan: (a) Pekeliling Am Bilangan 4 Tahun 2022 Pengurusan Dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022 Tindakan dalam Prosedur pelaporan Insiden Keselamatan ICT mengambil kira empat perkara di bawah : **i) Pelaporan** (a) Semua insiden keselamatan ICT yang berlaku hendaklah dilaporkan kepada ICTSO dan Jawatankuasa CSIRT MPKlang untuk pengendalian dan statistik insiden keselamatan ICT; dan (b) Semua maklumat insiden adalah SULIT dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. **ii) Tanggungjawab Jawatankuasa CSIRT MPKlang** (a) Jawatankuasa CSIRT MPKlang akan bertindak menghubungi dan melaporkan insiden yang berlaku kepada NACSA sama ada sebagai input atau tindakan seterusnya; dan (b) Merujuk jabatan-jabatan berkaitan untuk mengambil tindakan pemulihan dan pengukuhan.	ICTSO; Pengurus ICT CSIRT MPKlang; Pengguna

iii) Tanggungjawab Pengguna (a) Semua kakitangan, pembekal, pakar runding dan pihak-pihak lain yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, sebaliknya terus melaporkan dengan segara sebarang kejadian insiden keselamatan ICT; dan (b) Pastikan tindakan mengikut prosedur untuk mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan menceroboh. **iv) Tindakan Dalam Keadaan Berisiko Tinggi** (a) Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. (b) Tindakan segera perlu di ambil bagi mengelakkan kejadian insiden merebak.	

P09(02) Pengurusan Maklumat Insiden Keselamatan ICT

Objektif:
Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

P09(02) 01 – Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	**Tindakan**
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada MPKlang. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; (d) Menyediakan tindakan pemulihan segera; dan (e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO; Pengurus ICT; CSIRT MPKlang

PERKARA 10 – PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

P10(01) Dasar Kesinambungan Perkhidmatan

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

P10(01) 01 – Pelan Kesinambungan Perkhidmatan	**Tindakan**
Pelan Kesinambungan Perkhidmatan (*Business Continuity Management -BCM*) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Tujuan utama Pelan Kesinambungan disediakan adalah untuk memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT MPKlang dan perkara-perkara berikut perlu diberi perhatian: (a) Mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; (c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (d) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (f) Membuat *backup*; dan (g) Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali. Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai personel MPKlang dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden; (c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan (e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh. BCM yang telah dibangunkan hendaklah melalui proses berikut: - (a) Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama; (b) Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun (secara berkala) atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan; (c) Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan;	CDO; Pengurus ICT

(d) Pengujian hendaklah direkodkan sebagai rujukan untuk memastikan hasil pengujian dapat dinilai dengan lebih tepat untuk penambahbaikan dan pengukuhan yang lebih berkesan; (e) Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, dan menjalankan tanggungjawab dan peranan mereka apabila pelan dilaksanakan; dan (f) Salinan pelan BCM hendaklah sentiasa dikemaskini dan dilindungi seperti di lokasi utama.	ICTSO; Pengurus ICT
P10(01) 02 – *Redundancy*	
Semua sistem aplikasi dan perkakasan yang kritikal hendaklah mempunyai kemudahan redundancy dan diuji (*failover test*) keberkesanannya mengikut keperluan.	Pengurus ICT, Pentadbir Sistem

PERKARA 11 – PEMATUHAN

P11(01) Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT MPKlang.	
P11(01) 01 – Pematuhan Dasar	**Tindakan**
Pematuhan Dasar merangkumi perkara berikut :- (a) Setiap pengguna di MPKlang hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MPKlang dan undang-undang atau peraturan-peraturan lain yang berkaitan yang sedang berkuat kuasa. (b) Semua aset ICT di MPKlang termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. (c) Sebarang penggunaan aset ICT MPKlang selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber MPKlang.	Semua
P11(01) 02 – Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	**Tindakan**
Untuk memenuhi perkara di atas, perkara berikut hendaklah dilaksanakan :- (a) ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. (b) Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT. (c) Sebarang penilaian pematuhan teknikal seperti aktiviti *Security Posture Assessment* (SPA) mestilah dijalankan oleh individu yang kompeten dan dibenarkan.	ICTSO
P11(01) 03 – Pematuhan Keperluan Audit	**Tindakan**

Pematuhan kepada keperluan audit adalah perlu bagi memaksimumkan keberkesanan dalam proses audit sistem maklumat. Perkara yang perlu dilaksanakan adalah seperti berikut: - (a) Pengauditan perlu dilaksanakan secara berkala terhadap pengoperasian sistem maklumat bagi meminimumkan ancaman dan meningkatkan ketersediaan sistem; (b) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan; dan (c) Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua
P11(01) 04 – Pematuhan Perundangan	**Tindakan**
Sumber kuasa perundangan dan peraturan-peraturan di MPKlang terbahagi kepada dua iaitu daripada peringkat persekutuan/negeri dan peringkat Dalaman MPKlang. Senarai adalah seperti di bawah:	Semua

(a) Keperluan perundangan atau peraturan-peraturan lain berkaitan di Peringkat persekutuan/Negeri yang perlu dipatuhi oleh semua pengguna di MPKlang adalah seperti berikut:
(1) Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
(2) Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
(3) *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002;
(4) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
(5) Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
(6) Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network)* di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
(7) Garis Panduan IT Outsourcing Agensi-agensi Sektor Awam Tahun 2006 yang dikeluarkan oleh Jabatan Perdana Menteri;
(8) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
(9) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
(10) Akta Rahsia Rasmi 1972;
(11) Akta Tandatangan Digital 1997;
(12) Akta Hak Cipta (Pindaan) Tahun 1997;
(13) Akta Komunikasi dan Multimedia 1998;
(14) Akta Jenayah Komputer 1997;

(15) Akta Aktiviti Kerajaan Elektronik 2007; (16) Arahan Teknologi Maklumat 2007; (17) Arahan Keselamatan; (18) Perintah-Perintah Am; (19) Arahan Perbendaharaan; (20) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009; (21) Surat Arahan Ketua Pengarah MAMPU – Penggunaan Media Jaringan Sosial di Sektor Awam yang bertarikh 19 November 2009 (22) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010; (23) Surat Arahan Ketua Pengarah MAMPU – Panduan Pelaksanaan Pengurusan Projek ICT Sektor Awam yang bertarikh 5 Mac 2010 (24) Surat Arahan Ketua Pengarah MAMPU – Pemantapan Penggunaan Dan Pengurusan E-Mel Di Agensi-Agensi Kerajaan yang bertarikh 1 Julai 2010 (25) Surat Arahan Ketua Pengarah MAMPU – Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam yang bertarikh 24 November 2010 (26) Surat Arahan Ketua Pengarah MAMPU – Panduan Keperluan Dan Persediaan (27) Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam yang bertarikh 24 November 2010 (28) Surat Arahan Ketua Pengarah MAMPU – Panduan Penggunaan MyRAM yang bertarikh 23 Februari 2012 (29) Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSA) Versi 1.0 bertarikh April 2016. (30) Surat Ketua Pengarah Keselamatan Negara, Majlis Keselamatan Negara bertarikh 28 Januari 2019 (MPK(S).10.700-8/12/3 (20) – Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Emergency Response Team (GCERT) oleh Agensi Keselamatan Negara (NACSA). (31) Pekeliling Am Bilangan 4 Tahun 2022 Pengurusan Dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022. (b) Keperluan perundangan atau peraturan-peraturan lain berkaitan di Peringkat dalaman MPKlang yang perlu dipatuhi oleh semua pengguna di MPKlang adalah seperti berikut: (1) Surat Aku Janji; (2) Manual Prosedur; (3) Garis Panduan Keselamatan MPK (4) Manual MPK Tahun 2013 : Manual/proses kerja berkaitan ICT	
P11(01) 05 – Pelanggaran Dasar	**Tindakan**
Pelanggaran dasar ini boleh diambil tindakan undang-undang dan tatatertib di bawah Akta Rahsia Rasmi 1972 dan Perintah-Perintah Am Bab “D” - Peraturan-Peraturan Pegawai Awam (Kelakuan Dan Tatatertib).	Semua

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT MAJLIS PERBANDARAN KLANG
(DKICT MPKLANG)

Nama (Huruf Besar) : …….
No. Kad Pengenalan : …….
Jawatan : …….
Jabatan / Bahagian : …….

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam dasar keselamatan ICT MPKlang; dan

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

…….
Tandatangan

Tarikh :

ICTSO

…….

Tarikh :

Pengurus ICT

…….

Tarikh :

Pegawai Pengawal / CDO

…….

LAMPIRAN 2

JABATAN TEKNOLOGI MAKLUMAT
ARAS M, BANGUNAN SULTAN ALAM SHAH,
JALAN PERBANDARAN,
41675 KLANG, SELANGOR DARUL EHSAN.
www.mpklang.gov.my
Talian Perkhidmatan ICT :33755555 samb. 1110

MPK.PK (A15) L15

No. Daftar

Tarikh Berkuatkuasa:28 Ogos 2013

Borang Perjanjian Tanpa Pendedahan (NDA)

Borang **Perjanjian Tanpa Pendedahan** (*Non-Disclosure Agreement*) ini berkuatkuasa pada tarikh _____ , diantara pihak,**Majlis Perbandaran Klang** dengan _____

Perjanjian ini adalah untuk mengadakan peruntukan bagi perlindungan kerahsiaan dan pengendalian maklumat sulit ketika pihak tuan/puan menjalankan kerja/projek: _____ di **Majlis Perbandaran Klang**.

BAHAWASANYA saya _____
No Pekerja/No KP:_____bagi pihak yang tersebut di atas bersedia untuk menerima Maklumat Sulit menurut terma Perjanjian ini untuk tujuan kerja/projek:

Tiada Pendedahan: Penerima Maklumat bersetuju untuk menggunakan usaha terbaik untuk mencegah dan melindungi Maklumat Sulit itu, atau mana-mana bahagiannya, daripada pendedahan kepada mana-mana orang selain daripada pekerja syarikat yang terbabit yang mempunyai keperluan untuk pendedahan berkaitan dengan penggunaan yang dibenarkan kepada Penerima Maklumat Sulit.

Perlindungan Kerahsiaan: Penerima bersetuju untuk mengambil semua langkah yang semunasabahnya untuk melindungi kerahsiaan Maklumat Sulit, dan untuk mencegah Maklumat Sulit daripada jatuh ke dalam domain awam atau ke dalam milikan orang-orang yang tidak dibenarkan.

Pemilikan Maklumat Sulit: Penerima bersetuju bahawa semua Maklumat Sulit hendaklah kekal sebagai harta ***Discloser*** dan tidak boleh menggunakan Maklumat Sulit untuk sebarang tujuan tanpa kewajipan untuk penerima. Penerima tiada hak membuat apa-apa pemindahan hak maklumat sulit bagi mana-mana patern atau harta intelektual lain yang melindungi atau berkaitan maklumat sulit tersebut.

Tempoh dan Penamatan: Obligasi Perjanjian ini hendaklah berterusan sehingga Maklumat Sulit yang didedahkan kepada penerima tidak lagi sulit.

Berkuat kuasa: Perjanjian ini hendaklah terus berkuatkuasa dan berkesan sepanjang tempoh di mana penerima terlibat secara aktif atau tidak aktif dalam pelaksanaan kerja/projek.

Tindakan: sebarang pelanggaran mana-mana peruntukan Perjanjian ini maka tindakan akan diambil berdasarkan kepada Akta Rahsia Rasmi 1972, Akta Tandatangan Digital 1997 dan Akta Hak Cipta (Pindaan) Tahun 1997.

SEKIRANYA didapati pihak syarikat melanggar mana-mana terma perjanjian di atas, maka pihak syarikat bersedia menerima sebarang tindakan yang akan di ambil oleh pihak Majlis.

PADA MENYAKSIKAN HAL, pihak-pihak telah memeterai perjanjian ini berkuatkuasa bermula dari tarikh seperti di atas.

Pendedahan Maklumat:	Penerima Maklumat:
.....	.....
(Tandatangan / cop rasmi)	(Tandatangan / cop rasmi)
Nama Penuh:	Nama Penuh:
No K/P:	No K/P:

Saksi:

.....
(Tandatangan / cop rasmi)

Nama Penuh:

No K/P: