MAJLIS PERBANDARAN HULU SELANGOR
JALAN BUKIT KERAJAAN
44000 KUALA KUBU BHARU

DASAR KESELAMATAN ICT (DKICT)
MAJLIS PERBANDARAN HULU SELANGOR

KOD	:	**MPHS-ISMS-P1-01**
NO. TERBITAN	:	**4.1**
TARIKH	:	**20 MAC 2023**

ISO/IEC 27001:2013

DASAR KESELAMATAN ICT
MAJLIS PERBANDARAN HULU SELANGOR

MPHS-ISMS-P1-01

KANDUNGAN

KANDUNGAN

KANDUNGAN

KANDUNGAN

KANDUNGAN

KANDUNGAN

KANDUNGAN

PENGENALAN

Majlis Perbandaran Hulu Selangor (MPHS) berperanan untuk menyediakan perkhidmatan bagi perancangan, pembangunan dan pengurusan sumber manusia sektor awam yang cemerlang berteraskan profesionalisme, integriti dan teknologi. Dokumen ini menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dan melindungi aset Teknologi Maklumat dan Komunikasi (Information and Communication Technology – ICT) MPHS. Dokumen ini diguna pakai oleh semua kakitangan, pengguna dan pembekal yang menyediakan perkhidmatan, mencapai dan menggunakan aset dan sistem aplikasi ICT di MPHS.

Dasar Keselamatan ICT MPHS (DKICT MPHS) merangkumi Dasar Keselamatan ICT Majlis Perbandaran Hulu Selangor dan semua jabatan di bawahnya. Dasar ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) Majlis Perbandaran Hulu Selangor (MPHS). Dasar ini juga menerangkan kepada semua pengguna di MPHS mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT MPHS.

OBJEKTIF

Dasar Keselamatan ICT MPHS (DKICT MPHS) diwujudkan untuk memastikan tahap keselamatan ICT MPHS terurus dan dilindungi bagi menjamin kesinambungan urusan pengoperasian dan pengurusan ICT MPHS dengan meminimumkan kesan insiden keselamatan ICT.

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

Objektif utama Dasar Keselamatan ICT MPHS adalah seperti berikut:

a) Memastikan kelancaran operasi jabatan yang berlandaskan ICT dengan mencegah serta meminimumkan kerosakan atau kemusnahan aset ICT jabatan;

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

c) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;

d) Meningkatkan tahap kesedaran keselamatan ICT kepada para kakitangan, pengguna dan pembekal;

e) Mencegah penyalahgunaan atau kecurian aset ICT MPHS; dan

f) Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal

PENYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. 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 dari pespektif ICT pula bermaksud keadaan dimana 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 MPHS 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 hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat dari sumber-sumber yang sah.

Dasar Keselamatan ICT MPHS 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 yang berikut:

a) Kerahsiaan - maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan akses tanpa kebenaran;

b) Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini.

Datanya boleh diubah dengan cara yang dibenarkan;

c) Tidak boleh disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

d) Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan;

e) Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

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

a) **Perkakasan**

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan MPHS. Contoh peralatan dan peranti perisian seperti komputer, pelayan, firewall, pencetak, peralatan media, peralatan komunikasi dan alat-alat prasarana seperti Uninterruptible Power Supply (UPS) dan sebagainya.

b) **Perisian**

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

c) **Perkhidmatan**

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

d) **Data dan maklumat**

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif MPHS. Contohnya sistem dokumentasi, prosedur operasi, rekod-

rekod, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain.

e) **Manusia**

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

f) **Media Storan**

Semua media storan dan peralatan yang berkaitan seperti storan mudah alih, cakera padat dan pemacu USB.

g) **Media Komunikasi**

Semua peralatan berkaitan komunikasi seperti pelayan rangkaian, gateway, router, peralatan PABX, wireless LAN, talian internet, kabel rangkaian, switches, hub dan lain-lain.

h) **Dokumentasi**

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

PRINSIP-PRINSIP

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

a) **Akses atas dasar perlu mengetahui**

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan (Semakan dan Pindaan 2017) perenggan 18, muka surat 14;

b) **Hak akses minimum**

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

c) **Kebertanggungjawaban/Akauntabiliti**

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT MPHS.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;

iii) Menentukan maklumat sedia untuk digunakan;

iv) Menjaga kerahsiaan kata laluan;

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

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

v) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

d) **Pengasingan**

Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan (unauthorized access) serta melindungi aset ICT MPHS daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan tugas juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

e) **Pengauditan**

Pengauditan adalah tindakan untuk mengenalpasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan aset ICT. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

Dengan itu, aset ICT seperti komputer, pelayan, router, firewall dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit (audit trail).

f) **Pematuhan**

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

g) **Pemulihan**

Pemulihan sistem perlu untuk memastikan kebolehsediaan dan kebolehcapaian bagi meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan dan ketidakbolehcapaian. Pemulihan boleh dilakukan melalui proses penduaan (backup) dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan (BRP).

h) **Saling Bergantungan**

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

PENILAIAN RISIKO KESELAMATAN ICT

MPHS perlu mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan vulnerability yang semakin meningkat hari ini. Justeru itu MPHS perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

MPHS hendaklah melaksanakan penilaian risiko Keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat MPHS 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, kemudahan utiliti dan sistem-sistem sokongan yang lain. MPHS 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 dan garis panduan keselamatan daripada pihak MAMPU yang dikeluarkan dari semasa ke semasa.

MPHS perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko yang berlaku dan memilih tindakan berikut :

a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

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

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

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

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

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

BIDANG 02 ORGANISASI KESELAMATAN	
0201 Infrastruktur Organisasi Dalaman	
Objektif: Menerangkan peranan dan tanggungjawab semua pihak yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT MPHS	
020101 Tuan Yang Dipertua MPHS (YDP MPHS)	
Peranan dan tanggungjawab YDP MPHS adalah seperti berikut: a) Memastikan setiap pengguna memahami peruntukan-peruntukan yang ada di bawah Dasar Keselamatan ICT MPHS. b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT MPHS, c) Memastikan semua keperluan jabatan seperti sumber kewangan, sumber kakitangan dan perlindungan keselamatan adalah mencukupi, dan d) Memastikan semua dasar yang telah ditetapkan dan dipersetujui oleh pengurusan dilaksanakan sepenuhnya di kalangan kakitangan MPHS.	YDP MPHS
020102 Ketua Pegawai Digital (CDO)	
Ketua Pegawai Digital (CDO) bagi MPHS adalah disandang oleh Tuan Setiausaha MPHS. Peranan dan tanggungjawab CDO adalah seperti berikut: a) Menentukan keperluan keselamatan ICT;	CDO

b) Bertanggungjawab menyelaras dan mengurus pelan tindakan dan program keselamatan seperti penyediaan DKICT MPHS, pelan latihan dan kesedaran pengguna, pengurusan risiko dan pengauditan; c) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MPHS. d) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT MPHS di semua Jabatan/Bahagian/Unit di MPHS.	
020103 Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) bagi MPHS adalah disandang oleh Ketua Bahagian Teknologi Maklumat MPHS. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a) Menentukan keperluan ICT di MPHS; b) Mengurus keseluruhan program keselamatan ICT MPHS; c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MPHS; d) Menguatkuasakan Dasar Keselamatan ICT MPHS; e) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MPHS. f) Menjalankan pengurusan risiko; g) Menjalankan audit, mengkaji semula, merumus tindak balas	ICTSO

pengurusan ICT MPHS berdasarkan hasil penemuan dan menyediakan laporan mengenainya;

h) Memberi dan menyebarkan amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;

i) Mencadangkan langkah-langkah pengukuhan bagi mematuhi dasar-dasar berkaitan keselamatan ICT MPHS;

j) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (GCERT) Selangor dan seterusnya membantu dalam penyiasatan atau pemulihan;

k) Memastikan pematuhan DKICT MPHS oleh pihak luaran seperti perunding, kontraktor dan pembekal yang mencapai dan menggunakan aset ICT MPHS untuk tujuan penyelenggaraan, pemasangan, naik taraf dan sebagainya;

l) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan ICT; dan

m) Memastikan DKICT MPHS dikemaskini sesuai dengan perubahan teknologi, arahan jabatan dan ancaman-ancaman dari semasa ke semasa;

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

020105 Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPHS; b) Mengetahui dan memahami implikasi keselamatan ICT dari sudut kesan dan tindakannya; c) Melaksanakan arahan-arahan Dasar Keselamatan ICT MPHS dan menjaga kerahsiaan maklumat MPHS; d) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; e) Menghadiri program-program kesedaran mengenai keselamatan ICT; f) Menandatangani surat akuan pematuhan Dasar Keselamatan ICT MPHS; g) Menghalang pendedahan maklumat kepada pihak luar atau pihak yang tidak dibenarkan; h) Menjaga kerahsiaan kata laluan dari semasa ke semasa;dan i) Memberi perhatian kepada sebarang maklumat terperingkat terutama semasa pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan	Penguna

0202 Pihak Ketiga	
Objektif : Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain)	
020201 Keperluan Keselamatan Kontrak Dengan Pihak Ketiga	
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPHS; 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 MPHS perlu berlandaskan kepada perjanjian kontrak;dan e) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MPHS sebagaimana **Lampiran 1**.	CDO, Pegawai Teknologi Maklumat / Pegawai Keselamatan ICT (ICTSO), Pentadbir Sistem dan Pihak Ketiga
020202 Kawalan Akses Aset ICT	
Pelantikan pihak ketiga untuk memberi perkhidmatan memerlukan pihak tersebut mengakses aset ICT MPHS seperti internet MPHS, kad akses, sistem/aplikasi dan sebagainya. Pengurus projek	Pengurus Projek, ICTSO

bertanggungjawab untuk menguruskan proses pemberian, penggantungan atau penamatan akses pihak ketiga tersebut sepanjang tempoh kontrak atau perkhidmatan.	

BIDANG 03 PENGURUSAN ASET	
0301 Akauntabiliti Aset	
Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset MPHS.	
KENYATAAN	**TINDAKAN**
030101 Inventori Aset ICT	
Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik. Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi: a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa di kemaskini; b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c) Memastikan semua pengguna mengesahkan aset ICT yang ditempatkan di MPHS; d) Semua peraturan pengendalian aset hendaklah dikenal pasti,	Penolong Pegawai Teknologi Maklumat, Juruteknik dan Pengguna

didokumen dan dilaksanakan; e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan f) Sebarang pelanggaran hendaklah dilaporkan kepada Pegawai Aset/ICTSO.	
0302 Pengelasan dan Pengendalian Maklumat	
Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian	
030201 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; atau d) Terhad. Maklumat yang telah dikelaskan mestilah dilabel mengikut kelas yang telah ditetapkan.	Semua
030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah	Semua

hendaklah mengambil kira langkah-langkah keselamatan berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g) Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum; h)	
030203 Penyebaran Maklumat	
Setiap maklumat yang hendak dikeluarkan kepada pihak media atau orang awam (Contoh: kenyataan, ucapan, laporan teknikal) perlu disemak oleh Bahagian Korporat serta diluluskan oleh pihak Pengurusan Tertinggi.	Semua
030204 Penyimpanan Maklumat	
Setiap maklumat yang dikelaskan Rahsia Besar, Rahsia, Sulit dan Terhad dalam medium bercetak atau *softcopy* mesti disimpan di lokasi	Semua

yang ditetapkan.	
030205 Penggunaan Semula Maklumat	
Penggunaan semula maklumat yang dikelaskan Rahsia Besar, Rahsia, Sulit dan Terhad dalam medium bercetak atau *softcopy* perlu dikawal.	Semua

BIDANG 04
KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif :

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

040101 Sebelum Perkhidmatan

Memastikan pegawai dan kakitangan MPHS, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT. Perkara yang mesti dipatuhi termasuk yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan MPHS serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan MPHS serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua

040102 Dalam Perkhidmatan	
Perkara yang perlu dipatuhi termasuk yang berikut: a) Memastikan pegawai dan kakitangan MPHS serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan ditetapkan MPHS; b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MPHS 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 MPHS, serta pihak ketiga yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan yang ditetapkan MPHS; dan d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	Semua
040103 Kesedaran, Pendidikan & Latihan Berkaitan Keselamatan ICT	
Setiap pengguna di MPHS perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga adalah penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT MPHS.	Ketua Jabatan/ Bahagian/ Unit

040104 Bertukar Atau Tamat Perkhidmatan	
Memastikan pertukaran atau tamat perkhidmatan pegawai dan kakitangan MPHS, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan diuruskan dengan teratur. Perkara yang perlu dipatuhi termasuk: a) Memastikan semua aset ICT dikembalikan kepada jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan atau meminda semua kebenaran capaian ke atas maklumat, kemudahan proses maklumat dan semua akses berkaitan mengikut peraturan yang ditetapkan oleh MPHS dan/atau terma perkhidmatan. c) Pengarah Jabatan bertanggungjawab untuk memaklumkan pertukaran kakitangan di antara bahagian yang berlaku di dalam jabatan yang sama kepada Bahagian Sumber Manusia; dan d) Jabatan Khidmat Pengurusan bertanggungjawab untuk mengeluarkan surat makluman berkaitan pertukaran dalaman yang berlaku kepada Bahagian Teknologi Maklumat (BTM) dan Unit Aset dan Stor berkaitan pertukaran dalaman berikut : i) Pertukaran dalaman yang berlaku di antara Jabatan. ii) Pertukaran dalaman yang berlaku di antara bahagian di dalam jabatan yang sama	Semua, Bahagian Teknologi Maklumat
040105 Tindakan Tatatertib	
Ketidakakuran kepada DKICT MPHS, polisi dan prosedur berkaitan keselamatan ICT boleh membawa kepada tindakan tatatertib sekiranya perlu.	Ketua Jabatan/ Bahagian/ Unit

BIDANG 05
KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 Keselamatan Kawasan

Objektif:

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

050101 Kawalan Kawasan

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; d) Memastikan kawasan yang mempunyai aset ICT dilengkapi dengan perlindungan keselamatan yang mencukupi seperti alat pencegah kebakaran dan kamera litar tertutup (CCTV); e) Mereka bentuk dan melaksanakan perlindungan fizikal dari	CDO, KJ, ICTSO

kebakaran, banjir, letupan, kacau-bilau dan bencana; f) Bagi menjamin keselamatan kakitangan dan orang awam semasa situasi wabak pandemik (COVID-19) pemakaian perlu mematuhi pada pekeliling seperti di bawah: i) Pelaksanaan Perintah Kawalan Pergerakan Berkaitan Penularan Wabak Covid-19 Peringkat Pentadbiran Kerajaan Negeri Selangor bertarikh 17 Mac 2020. ii) Operasi Pejabat Kerajaan Semasa Perintah Kawalan Pergerakan Bersyarat (PKPB) bertarikh 2 Mei 2020. iii) Budaya Kerja Perkhidmatan Awam Semasa Tempoh Perintah Kawalan Pergerakan Pemulihan (PKPP) Pentadbiran Kerajaan Negeri Selangor bertarikh 9 Jun 2020.	
050102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut:- a) Setiap pengguna MPHS hendaklah memakai atau mengenakan pas pekerja sepanjang waktu bertugas; b) Semua pas pekerja hendaklah diserahkan balik kepada MPHS apabila pengguna berhenti atau bersara; c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama MPHS. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan d) Kehilangan pas mestilah dilaporkan dengan segera. e) Akses masuk ke bilik server hendaklah dihadkan kepada pegawai-pegawai yang diberi kuasa sahaja;	Semua

f) Setiap pelawat perlu menandatangani buku log keluar masuk bilik server.	
050103 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan; kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	YDP MPHS, CDO, KJ
0502 Keselamatan Peralatan	
Objektif: Melindungi peralatan ICT MPHS dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
050201 Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b) Penggunaan kata laluan untuk akses ke sistem komputer	Semua pengguna

adalah diwajibkan;

c) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

d) Pengguna dilarang sama sekali menambah, menanggalkan atau mengganti sebarang perkakasan ICT yang telah ditetapkan;

e) Pengguna dilarang meminjamkan peralatan ICT yang diberikan kepada pihak lain tanpa kebenaran.

f) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;

g) Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;

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

i) Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;

j) Peralatan-peralatan kritikal perlu disokong oleh UPS;

k) Semua peralatan 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 bilik atau rak 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 MPHS, perlulah mendapat kelulusan ICTSO atau Penolong Pegawai Teknologi Maklumat dan direkodkan bagi tujuan pemantauan;

n) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;

o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset;

p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Bahagian Teknologi Maklumat untuk dibaik pulih;

q) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*Administrator Password*) yang telah ditetapkan oleh Pentadbir Sistem ICT;

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

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

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

u)	Memastikan plag dicabut daripada suis utama (*Main Switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya; dan	
v)	Juruteknik yang bertanggungjawab perlu memastikan aktiviti peminjaman dan pemulangan peralatan ICT direkodkan dan menyemak peralatan yang dipulangkan berada dalam keadaan baik dan lengkap;	
050202	**Media Storan**	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti cakera padat, thumb drive, *external hard disk* dan media-media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut:		Semua
a)	Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;	
b)	Semua media storan data yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat;	
c)	Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu;	
d)	Perkakasan *backup* hendaklah diletakkan di tempat yang	

terkawal; e) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; f) Akses dan pergerakan kepada media storan yang mempunyai data kritikal perlu direkodkan; g) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; h) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan i) Dokumen perlu diletakkan kata laluan supaya hanya orang yang berhak sahaja dapat membukanya.	
050203 Media Tandatangan Digital	
Sebarang media yang digunakan untuk ditandatangan digital hendaklah mematuhi langkah-langkah berikut: a) Pengguna hendaklah bertanggungjawab sepenuhnya bagi perlindungan 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 selanjutnya.	Semua

050204 Media Perisian Dan Aplikasi	
Sebarang media yang digunakan sebagai media perisian dan aplikasi hendaklah mematuhi langkah-langkah berikut: a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan jabatan MPHS; b) Sistem aplikasi dalaman tidak dibenarkan diagih / didemontrasikan kepada pihak lain kecuali dengan kebenaran ICTSO; 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
050205 Pelupusan Perkakasan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MPHS dan ditempatkan di MPHS. Langkah-langkah berikut perlu diambil dalam memastikan peralatan ICT dilupuskan dengan teratur: a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan. b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah	Pegawai Aset ICT, Pegawai Aset

membuat penduaan;

c) Pegawai Aset ICT akan mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

d) Peralatan ICT yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

e) Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam rekod Aset;

f) Pelupusan peralatan ICT boleh dilakukan secara berpusat/tidak berpusat mengikut tatacara pelupusan semasa yang berkuat kuasa;

g) Peralatan-peralatan ICT yang akan dilupuskan hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;

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

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

ii) Menyimpan dan memindahkan perkakasan luaran komputer seperti speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian MPHS; dan

iii) Memindah keluar dari MPHS mana-mana peralatan ICT yang hendak dilupuskan; iv) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab MPHS; dan v) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti storan muda alih atau *thumb drive* dan *hard disk* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
050206 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: a) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; b) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan;	Penolong Pegawai Teknologi Maklumat dan Juruteknik

e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada ICTSO.	
050207 Peralatan Di Luar Premis	
Perkakasan yang dibawa keluar dari premis MPHS adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Mendapatkan kelulusan ICTSO bagi membawa keluar peralatan atau maklumat tertakluk kepada tujuan yang dibenarkan; b) Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan bagi tujuan pemantauan; c) Peralatan perlu dilindungi dan dikawal sepanjang masa; d) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan e) Sebarang kehilangan peralatan adalah di bawah tanggungjawab individu yang membawa keluar peralatan tersebut.	Semua

050208 Peminjaman Peralatan	
Peralatan yang dipinjam hendaklah mendapat kelulusan mengikut peraturan yang telah ditetapkan oleh MPKj bagi membawa keluar perkakasan, perisian atau maklumat tertakluk kepada tujuan yang dibenarkan. Langkah-langkah perlu diambil termasuklah seperti berikut: a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh MPHS bagi membawa keluar peralatan, perisian atau maklumat tertakluk kepada tujuan yang dibenarkan; b) Melindungi dan mengawal peralatan sepanjang masa; c) Merekodkan aktiviti peminjaman dan pemulangan peralatan; dan d) Menyemak peralatan ketika peminjaman dan pemulangan dilakukan.	Semua
050209 Pengendalian Peralatan Peribadi (BYOD)	
Kakitangan atau pihak ketiga yang menggunakan peralatan ICT peribadi milik seperti komputer riba, tablet atau storan mudah alih untuk mengakses perkakasan, maklumat, sistem, rangkaian atau infrastruktur ICT MPHS perlu mematuhi kawalan keselamatan ICT antaranya seperti berikut: a) Memberi kebenaran untuk peralatan ICT tersebut diperiksa apabila diperlukan; b) Diaudit dan diambil bukti berkaitan sekiranya berlaku insiden ICT berpunca daripada peralatan tersebut; c) Memberi perlindungan keatas maklumat MPHS yang diakses mengikut kelas & klasifikasi maklumat tersebut; dan d) Mematuhi DKICT MPHS terkini sepanjang penggunaan peralatan ICT tersebut yang digunakan untuk mengakses perkakasan, maklumat, sistem, rangkaian atau infrastruktur ICT MPHS.	Semua

0503 Keselamatan Persekitaran	
Objektif: Melindungi aset ICT MPHS dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050301 Kawalan Persekitaran	
Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data; b) Semua ruang pejabat khususnya yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; 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 sekali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu;dan	Semua

g) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	
050302 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa: a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b) Peralatan sokongan seperti Uninterruptable Power Supply (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan; dan c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	ICTSO, Penolong Pegawai Teknologi Maklumat, Juruteknik dan Jurutera
050303 Kabel	
Kabel komputer/rangkaian 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;	ICTSO, Penolong Pegawai Teknologi Maklumat dan Juruteknik

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.	

0504 Keselamatan Dokumen	
Objektif: Melindungi maklumat MPHS dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
050401 Dokumen	
Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumen: a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti 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	Semua

	Keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan	
e)	Sistem dokumentasi hanya boleh diakses menggunakan peralatan ICT MPHS atau peralatan ICT sendiri yang telah mendapat kebenaran hak capaian.	

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

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 dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau sebaliknya;	
060103 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	ICTSO dan Penolong Pegawai Teknologi Maklumat

0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Objektif : Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
060201 Perkhidmatan Penyampaian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut:- a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua

0603 Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301 Perancangan Kapasiti	
a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	ICTSO
060302 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui;	ICTSO dan Penolong Pegawai Teknologi Maklumat

0604 Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.	
060401 Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT dari perisian berbahaya: a) Memasang sistem keselamatan untuk mengesan perisian atau	Semua

program berbahaya seperti *antivirus* serta mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa; c) Mengimbas semua perisian atau sistem dengan *antivirus* sebelum menggunakannya; d) Mengemas kini antivirus dengan paten *antivirus* yang terkini; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri program 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) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
060402 Perlindungan dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua

0605 Housekeeping	
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
060501 *Backup*	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, backup hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Membuat backup ke atas semua data kritikal pada sistem utama MPHS mengikut keperluan organisasi. Kekerapan backup bergantung pada tahap kritikal maklumat; b) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; c) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	Penolong Pegawai Teknologi Maklumat

0606 Pengurusan Rangkaian	
Objektif: Melindungi maklumat rangkaian dan infrastruktur sokongan.	
060601 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian perlu dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut: a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d) Firewall hendaklah dipasang serta dikonfigurasi dan diselia oleh Penolong Pegawai Teknologi Maklumat; e) Semua trafik keluar dan masuk hendaklah melalui firewall di bawah kawalan MPHS; f) Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; g) Semua pengguna hanya dibenarkan menggunakan rangkaian	ICTSO, Penolong Pegawai Teknologi Maklumat

MPHS kecuali mendapat kebenaran dari Bahagian Teknologi Maklumat MPHS . h) Sebarang penyambungan rangkaian yang bukan di bawah kawalan MPHS adalah tidak dibenarkan; dan i) Kemudahan bagi Wireless LAN perlu dipastikan kawalan keselamatan. j) Semua dokumen berkaitan rangkaian (Contoh: manual pengguna, *system documentation, network diagram*) perlu disimpan di tempat yang selamat.	

0607 Pengurusan Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
060701 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu. Pengguna media mudah alih perlu memastikan privacy kandungan sentiasa terpelihara. Media mudah alih yang digunakan untuk menyimpan (sementara) atau memindahkan maklumat terperingkat perlu mempunyai encryption.	Semua

060702 Prosedur Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e) Menyimpan semua media di tempat yang selamat; dan f) Media yang mengandungi maklumat terperingkat hendaklah dihapus atau dimusnahkan mengikut peraturan dan prosedur yang betul dan selamat.	Semua
060703 Keselamatan Sistem Dokumentasi	
Dokumentasi untuk setiap sistem (Contoh: manual pengguna, manual sistem, panduan penyelenggaraan) perlu disimpan di tempat yang selamat dan diterhadkan hak capaiannya.	Semua

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

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

b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh MPHS;

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

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

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

f) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

g) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;

h) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;

i) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com dan sebagainya) tidak boleh digunakan untuk tujuan rasmi;

j) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing; k) Pengguna juga perlu melaporkan dengan kadar segera apabila menerima e-mel dan fail kepilan yang tidak diketahui pengirimnya serta meragui asal-usulnya. Pemilik e-mel juga boleh terus menghapuskan e-mel tersebut sekiranya meragui kesahihan e-mel tersebut; l) Pengguna dilarang untuk menghantar e-mel yang berunsur fitnah, ugutan dan hasutan yang boleh mengancam ketenteraman awam. m) Hanya kakitangan MPHS sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi jabatan; dan Jabatan Khidmat Pengurusan perlu memaklumkan sebarang status pengguna (bertukar jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke MPHS di bahagian masing-masing bagi tujuan pengemaskinian e-mel yang terlibat.	

0609	**Perkhidmatan E-Dagang (Electronic Commerce Services)**
Objektif: Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
060901	**E-Dagang**
Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet.	Semua

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Maklumat yang terlibat dalam atas talian perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b) Maklumat yang terlibat dalam transaksi atas talian (online) 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	
060902 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan Memastikan segala maklumat yang hendak dipaparkan telah mendapat arahan daripada Bahagian Korporat.	Semua

0610 Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
061001 Pengauditan dan Forensik ICT	
ICTSO mestilah bertanggungjawab merekod dan menganalisa perkara-perkara berikut:- a) Sebarang percubaan pencerobohan kepada sistem ICT MPHS; b) Serangan kod perosak *(maliCDOus 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 (*bandwith)* rangkaian; g) Aktiviti penyalahgunaan akaun e-mel; dan Aktiviti penukaran alamat IP (IP address) selain daripada yang telah diperuntukkan tanpa kebenaran.	ICTSO

061002 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit *(audit trail).* Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut:- a) Rekod setiap aktiviti transaksi; b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan Maklumat akitiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.	Penolong Pegawai Teknologi Maklumat
061003 Sistem Log	
Fungsi-fungsi sistem log adalah seperti berikut: a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c) Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, Penolong Pegawai Teknologi Maklumat hendaklah melaporkan kepada ICTSO dan CDO.	Penolong Pegawai Teknologi Maklumat

061004 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan 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; dan e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;	Penolong Pegawai Teknologi Maklumat

BIDANG 07
KAWALAN CAPAIAN

0701 Dasar Kawalan Capaian

Objektif:

Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT.

070101 Keperluan Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d) Kawalan ke atas kemudahan pemprosesan maklumat.	BTM MPHS; dan ICTSO

0702 Pengurusan Capaian Pengguna

Objektif:

Mengawal capaian pengguna ke atas aset ICT MPHS.

070201 Akaun Pengguna	
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a) Akaun yang diperuntukkan oleh MPHS sahaja boleh digunakan; b) Akaun pengguna (*user id*) hendaklah unik dan mencerminkan identiti pengguna; c) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan MPHS. Akaun boleh ditarik balik jika kaedah penggunaannya melanggar peraturan; d) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang, dan e) Pentadbir Sistem boleh menggantung dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Bertukar bidang tugas kerja; ii. Bertukar ke agensi lain; iii. Bersara; atau iv. Ditamatkan perkhidmatan.	Semua
070202 Hak Capaian (*Privilege*)	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Penolong Pegawai Teknologi Maklumat

070203 Pengurusan kata laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MPHS 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 katalaluan mestilah sekurang-kurangnya enam (6) aksara dengan gabungan antara huruf dan nombor (alphanumerik); d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; h) Disarankan had masa pengesahan adalah selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; dan i) Kata laluan hendaklah ditukar selepas 90 hari atau selepas	Semua

tempoh masa yang bersesuaian; dan j) Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
070204 Clear Desk dan Clear Screen	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Clear Desk dan Clear Screen bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Menggunakan kemudahan *password screen saver* atau *log out* apabila meninggalkan komputer; b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Semua
0703 Kawalan Capaian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	

070301 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MPHS, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaiannya; c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; dan d) Menghadkan akses kepada *remote diagnostic port* yang hanya dibuka dan digunakan apabila diperlukan.	ICTSO, Penolong Pegawai Teknologi Maklumat
070302 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Penggunaan internet di MPHS hendaklah dipantau secara berterusan oleh Penolong Pegawai Teknologi Maklumat bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *maliCDOus code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MPHS; b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses internet mengikut fungsi kerja dan pemantauan tahap pematuhan;	ICTSO, Penolong Pegawai Teknologi Maklumat, Semua

c) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. ICTSO berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya;

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

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

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

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

h) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MPHS;

i) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CDO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;

j) Akses kepada Wifi MPHS diberikan berdasarkan kategori pengguna (kakitangan / pelawat)

k) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut;-

l) Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video dan lagu yang boleh menjejaskan tahap capaian Internet; dan m) Menyedia, memuat naik, memuat turun dan menyimpan material, teks, ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	

0704 Kawalan Capaian Sistem Pengoperasian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
070401 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; b) Merekodkan capaian yang berjaya dan gagal; dan c) Mengehadkan cubaan tidak berjaya untuk mencegah cubaan meneka katalaluan.	ICTSO, Penolong Pegawai Teknologi Maklumat

0705 Kawalan Capaian Aplikasi dan Maklumat	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.	
070501 Capaian Aplikasi dan Maklumat	
Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi: a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; c) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; d) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah dibolehkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; dan e) Mengehadkan cubaan tidak berjaya untuk mencegah cubaan meneka katalaluan.	ICTSO, Penolong Pegawai Teknologi Maklumat

0706	Peralatan Mudah Alih dan Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan jarak jauh.		
070601	**Peralatan Mudah Alih**	
Perkara yang perlu dipatuhi adalah seperti berikut:- a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.		Semua
070602	**Kerja Jarak Jauh**	
Perkara yang perlu dipatuhi adalah seperti berikut:- a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan. b) Tertakluk kepada pekeliling semasa: i) Pelaksanaan Perintah Kawalan Pergerakan Berkaitan Penularan Wabak Covid-19 Peringkat Pentadbiran Kerajaan Negeri Selangor bertarikh 17 Mac 2020. ii) Operasi Pejabat Kerajaan Semasa Perintah Kawalan Pergerakan Bersyarat (PKPB) bertarikh 2 Mei 2020.		Semua

BIDANG 08
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0801 Keselamatan dalam membangunkan sistem aplikasi

Objektif:

Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

080101 Keperluan keselamatan sistem maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketetapan maklumat; b) Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan sistem *output* untuk memastikan data yang telah diproses adalah tepat; c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan. e) Sekiranya data operasi MPHS digunakan semasa proses ujian sistem, data tersebut mesti dipadam setelah ujian selesai.	ICTSO, Penolong Pegawai Teknologi Maklumat

f) Satu versi sistem sebelum *UAT* perlu disimpan sebagai langkah persediaan untuk proses *rollback* sekiranya diperlukan.	
080102 Pengesahan Data *Input* dan *Output*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b) Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Penolong Pegawai Teknologi Maklumat

0802 Kawalan Kriptografi	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080201 Enkripsi (*Encryption*)	
Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
080202 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
080203 Pengurusan Infrastruktur Kunci Awam (PKI)	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua

0803 Keselamatan Fail Sistem	
Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
080301 Kawalan Fail Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Proses pengemas kini fail sistem hanya boleh dilakukan oleh pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Penolong Pegawai Teknologi Maklumat
0804 Keselamatan Dalam Proses Pembangunan dan Sokongan Sistem	
Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
080401 Prosedur Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Penolong Pegawai

a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod 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 pembekal; c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e) Menghalang sebarang peluang untuk membocorkan maklumat.	Teknologi Maklumat
080402 Pembangunan Perisian Secara *Outsource*	
Pembangunan perisian aplikasi secara outsource perlu dipantau oleh pemilik sistem. Kod sumber (source code) bagi semua aplikasi dan perisian adalah menjadi hak milik MPHS.	ICTSO, Penolong Pegawai Teknologi Maklumat

0805 Kawalan Teknikal Keterdedahan (*Vulnerability*)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
080501 Kawalan dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. 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.	Penolong Pegawai Teknologi Maklumat

BIDANG 9
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif :

Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamat ICT

090101 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera: a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e) Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka.	Penolong Pegawai Teknologi Maklumat

0902 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat Insiden Keselamatan ICT.	
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisa 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 MPHS. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan diselenggarakan. 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 kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; d) Menyediakan tindakan pemulihan segera; e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu; dan f) Melaksanakan program kesedaran kepada kakitangan MPHS	ICTSO

	berkaitan insiden yang berlaku sebagai langkah pencegahan kejadian berulang.	

BIDANG 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	
1001 Dasar Kesinambungan Perkhidmatan	
Objektif : Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
100101 Pelan Pengurusan Kesinambungan Perkhidmatan	
Pelan Kesinambungan Perkhidmatan (*Business Continuity Management* - BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh Jawatankuasa Perkhidmatan dan Teknologi Maklumat dan perkara-perkara berikut perlu diberi perhatian: a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan dan 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	ICTSO

membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;

d) Mendokumentasikan proses dan prosedur yang telah dipersetujui;

e) Mengadakan program kesedaran & latihan berkaitan kepada pengguna mengenai prosedur kecemasan;

f) Membuat *backup*; dan

g) Menguji dan mengemas kini 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 MPHS dan pembekal beserta nombor yang boleh dihubungi (faksimili, 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.

Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan.

Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

Hebahan kepada ahli dan personel Pelan BCM (bahagian yang berkenaan) perlu dilaksanakan dan Pelan BCM perlu sedia untuk diakses apabila diperlukan.

MPHS hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

BIDANG 11 PEMATUHAN	
1101 Pematuhan dan Keperluan Perundangan	
Objektif : Meningkatkan tahap keselamatan ICT bagi mengelak daripada perlanggaran kepada Dasar Keselamatan ICT MPHS.	
110101 Pematuhan Dasar - Dasar Bagi Hak Harta Intelek	
Setiap pengguna di MPHS hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MPHS dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Semua aset ICT di MPHS termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT MPHS selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber MPHS. **<u>Dasar bagi Hak Harta Intelek</u>** Akta Hakcipta (Pindaan) 2012 hendaklah sentiasa dipatuhi bagi menghalang aktiviti menciplak hak cipta orang lain. Perkara berikut perlu diambil kira untuk melindungi harta intelek: a) Penggunaan perisian yang sah; b) Pembelian dari sumber yang sahih; c) Sentiasa mengadakan program kesedaran terhadap dasar perlindungan harta intelek; d) Mengekalkan daftar aset dan mengenalpasti semua keperluan perlindungan terhadap aset;	Semua

e) Menyimpan lesen perisian; f) Memastikan bilangan had lesen tidak melebihi had ditetapkan; dan g) Menjalankan pemeriksaan perisian yang sah dan produk berlesen digunakan.	
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
110103 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua
110104 Keperluan Perundangan	
Keperluan perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di MPHS adalah seperti di **Lampiran 2.**	Semua
110105 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT MPHS boleh dikenakan tindakan tatatertib.	
110106 Perlindungan Maklumat Peribadi	

Setiap kakitangan & pembekal MPHS wajib memastikan semua maklumat peribadi yang boleh dikenalpasti *(Personal Identifiable Information – PII)* yang dikumpulkan, diproses, disimpan atau digunakan oleh MPHS dilindungi dengan sewajarnya dan selaras dengan keperluan piawaian ISO 27001, undang-undang dan peraturan yang berkenaan di Malaysia. Setiap kakitangan & pihak ketiga MPHS juga wajib mengambil langkah-langkah yang sewajarnya untuk memastikan bahawa akses kepada maklumat peribadi adalah terhad kepada pihak yang memerlukan akses tersebut sahaja, dan maklumat tersebut akan diproses dan digunakan dengan cara yang selamat dan beretika.	Semua
110107 Peraturan Kawalan Kriptografi	
Penggunaan kawalan kriptografi di MPHS perlu memenuhi piawaian keselamatan maklumat dan peruntukan undang-undang, dan hanya akan digunakan untuk tujuan yang dibenarkan sahaja. PYB perlu memastikan penggunaan kriptografi adalah selaras dengan polisi dan prosedur MPHS, dan hanya dilakukan oleh individu yang mempunyai kebenaran dan kelayakan yang sewajarnya. PYB juga perlu memastikan bahawa semua kunci kriptografi yang digunakan oleh MPHS dijaga dengan baik dan disimpan dengan selamat, dan hanya diberikan kepada individu yang memerlukan akses tersebut sahaja.	Semua
1102 Kajian Keselamatan Maklumat	
Objektif: Memastikan keselamatan maklumat dilaksanakan dan dikendalikan mengikut dasar dan prosedur organisasi.	
110201	Kajian Bebas/Pihak Ketiga Terhadap Keselamatan Maklumat

Pelaksanaan keselamatan maklumat MPHS hendaklah dikaji secara bebas atau oleh pihak ketiga pada jangka masa yang dirancang atau apabila berlaku perubahan ketara dalam pelaksanaannya.	BTM
110202	Kajian Pematuhan Teknikal
Sistem maklumat hendaklah dikaji supaya selaras dengan pematuhan dasar dan standard keselamatan maklumat organisasi *(seperti Security Posture Assessment – SPA).* Kajian teknikal perlu dilakukan setahun sekali atau mengikut kesesuaian.	BTM

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (Cth: di antara cakera keras dan PC utama) dalam jangka masa yang ditetapkan.
BRP	*Business Resumption Planning* *Pelan Kesinambungan Perkhidmatan*
BTM	Bahagian Teknologi Maklumat (Information Technology Department).
CCTV	Closed-circuit television system Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
CDO	Chief Information Officer Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Data Center	Pusat simpanan data.

GLOSARI	
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi atau penyulitan. Proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
E-mel	Mel Elektronik (Electronic Mail)
Firewall	Sistem yang direkabentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Juga pemisah di antara rangkaian luar dan dalam. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/espionage), penipuan(hoaxes).
GCERT	Government Computer Emergency Response Team Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan.
Hub	Hab 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.
ICTSO	ICT Security Officer adalah pegawai yang bertanggungjawab terhadap keselamatan ICT di sesebuah organisasi.
Insiden Keselamatan	Musibah (adverse event) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.

GLOSARI	
ISDN	Integrated Services Digital Networks menggunakan isyarat digital pada talian telefon analog yang sedia ada.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna pada mana-mana komputer boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Lock	Mengunci komputer.
Log out	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
MaliCDOus Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pegawai Aset	Pegawai yang telah diberi kuasa untuk mentadbir Aset ICT MPHS iaitu Pegawai Aset MPHS.
MPHS	Majlis Perbandaran Hulu Selangor
Pengguna	Semua individu yang menggunakan perkhidmatan / aplikasi / kemudahan ICT yang disediakan oleh MPHS.

GLOSARI	
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti spreadsheet dan word processing ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Pihak Ketiga	Pihak pembekal, perunding atau mana-mana pihak luar yang berurusan dengan MPHS.
PPTM	Gelaran bagi jawatan Penolong Pegawai Teknologi Maklumat di MPHS.
PYB	Pegawai yang bertanggungjawab
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.
Rahsia Besar	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia.
Restoration	Pemulihan ke atas data.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, capaian Internet.
Screen saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Juruteknik	Juruteknik Komputer
PT	Pembantu Tadbir
Sulit	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan

GLOSARI	
	atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian CSMA/CD secara mengurangkan perlanggaran yang berlaku.
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan 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 adalah satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Virus	Aturcara yang bertujuan merosakkan data atau sistem aplikasi.
WAN	Wide Area Network Rangkaian yang merangkumi kawasan yang luas.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran 1

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT MAJLIS PERBANDARAN HULU SELANGOR

Nama (Huruf Besar) : ----------

No. Kad Pengenalan : ----------

Jawatan : ----------

Jabatan/Bahagian/Unit : ----------

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT MPHS; dan

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

Tandatangan :

Tarikh :

Pengesahan Setiausaha, Majlis Perbandaran Hulu Selangor

(**AWALUDDIN BIN ZAKARIA, AMS**)
b.p. Tuan Yang Dipertua,
Majlis Perbandaran Hulu Selangor

Tarikh: ...

Lampiran 2

SENARAI PERUNDANGAN DAN PERATURAN

a. Arahan Keselamatan,
b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”,
c. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS),
d. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT),
e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan”,
f. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam,
g. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian InsidenKeselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
h. 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;
i. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
j. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
k. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
l. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

m. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
n. Akta Tandatangan Digital 1997,
o. Akta Rahsia Rasmi 1972,
p. Akta Jenayah Komputer 1997,
q. Akta Hak cipta (Pindaan) Tahun 1997,
r. Akta Komunikasi dan Multimedia 1998,
s. Perintah-Perintah Am,
t. Arahan Perbendaharaan,
u. Arahan Teknologi Maklumat 2007,
v. Garis Panduan Keselamatan MAMPU 2004;
w. Standard Operating Procedure (SOP) ICT MAMPU;
x. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
y. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010
z. Pelaksanaan Perintah Kawalan Pergerakan Berkaitan Penularan Wabak Covid-19 Peringkat Pentadbiran Kerajaan Negeri Selangor bertarikh 17 Mac 2020
aa. Operasi Pejabat Kerajaan Semasa Perintah Kawalan Pergerakan Bersyarat bertarikh 2 Mei 2020
bb. Budaya Kerja Perkhidmatan Awam Semasa Tempoh Perintah Kawalan Pergerakan Pemulihan (PKPP) Pentadbiran Kerajaan Negeri Selangor bertarikh 9 Jun 2020