POLISI KESELAMATAN SIBER

MAJLIS PERBANDARAN HULU SELANGOR

VERSI 1.0

MAJLIS PERBANDARAN HULU SELANGOR
JALAN BUKIT KERAJAAN
44000 KUALA KUBU BHARU

POLISI KESELAMATAN SIBER

KOD	:	**MPHS-ISMS-P1-01**
NO. TERBITAN	:	**1.0**
TARIKH	:	**20 JUN 2025**

ISO/IEC 27001:2022

POLISI KESELAMATAN SIBER (PKS)

MPHS-ISMS-P1-01

PENGESAHAN DOKUMEN

DISEDIAKAN OLEH
..... **(MOHAMAD RAMDAN BIN IBRAHIM)** Pengurus Projek ISMS Majlis Perbandaran Hulu Selangor
DISEMAK OLEH
..... **(MOHD NORAZIF BIN AHMAD TAMSIS)** Pengarah Projek ISMS Majlis Perbandaran Hulu Selangor
DILULUSKAN OLEH
..... **(SHAIFUL RIZZA BIN HJ. PIAMIN,** P.P.T, C.A(M)**)** Pengerusi Projek ISMS Majlis Perbandaran Hulu Selangor

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.

Polisi Keselamatan Siber MPHS (PKS MPHS) merangkumi Polisi Keselamatan Siber 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) MPHS. Dasar ini juga menerangkan kepada semua pengguna di MPHS mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT MPHS.

OBJEKTIF

Polisi Keselamatan Siber MPHS (PKS 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 Polisi Keselamatan Siber MPHS adalah seperti berikut:

a) Memastikan keselamatan siber MPHS berada ditahap terbaik dan sentiasa dikemaskini;
b) Memastikan kelancaran operasi jabatan yang berlandaskan ICT dengan mencegah serta meminimumkan kerosakan atau kemusnahan aset ICT jabatan;
c) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
d) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;
e) Meningkatkan tahap kesedaran keselamatan ICT kepada para kakitangan, pengguna dan pembekal;
f) Mencegah penyalahgunaan atau kecurian aset ICT MPHS; dan
g) 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.

Polisi Keselamatan Siber 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

Dokumen 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 Polisi Keselamatan Siber MPHS yang 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 terkini

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**

Polisi Keselamatan Siber 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 (BCP).

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 SIBER

MPHS mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman siber yang semakin meningkat hari ini. Justeru itu MPHS telah dan akan terus 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 sentiasa melaksanakan penilaian risiko keselamatan siber 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 siber berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan siber MPHS yang telah dilaksanakan ke atas sistem maklumat MPHS termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah bilik server, kemudahan utiliti dan sistem-sistem sokongan yang lain. MPHS bertanggungjawab melaksanakan dan menguruskan risiko keselamatan siber selaras dengan keperluan Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam terkini.

MPHS juga telah 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
d) yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
e) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

Kawalan keselamatan berikut telah dikaji dan dipilih oleh pihak yang terlibat dalam pelaksanaan keselamatan maklumat di MPHS seiring dengan keperluan keselamatan siber dan piawaian ISMS terkini.

BIDANG 05 KAWALAN ORGANISASI	
5.1 Polisi Keselamatan ICT	
5.1.1 Pelaksanaan Polisi	
Yang Dipertua adalah bertanggungjawab ke atas pelaksanaan arahan yang dibantu oleh Ketua Bahagian Teknologi Maklumat dan lain-lain pegawai yang dilantik.	YDP MPHS
5.1.2 Penyebaran Polisi	
Polisi 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
5.1.3 Penyelenggaraan Dasar	
Polisi Keselamatan Siber 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 Polisi Keselamatan Siber 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

5.1.4 Pengecualian Dasar	
Polisi Keselamatan Siber MPHS adalah terpakai kepada semua pengguna ICT MPHS tanpa sebarang pengecualian diberikan.	Kakitangan MPHS
5.2 Peranan dan Tanggungjawab Keselamatan Siber	
5.2.1 Yang Dipertua MPHS (YDP MPHS)	
Peranan dan tanggungjawab YDP MPHS adalah seperti berikut: a) Memastikan setiap pengguna memahami peruntukan-peruntukan yang ada di bawah Polisi Keselamatan Siber MPHS. b) Memastikan semua pengguna mematuhi Polisi Keselamatan Siber 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
5.2.2 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; b) Bertanggungjawab menyelaras dan mengurus pelan tindakan dan program keselamatan seperti penyediaan PKS MPHS, pelan latihan dan kesedaran pengguna, pengurusan risiko dan pengauditan; c) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MPHS; dan d) Menguatkuasakan pelaksanaan Polisi Keselamatan Siber MPHS di semua Jabatan/Bahagian/Unit di MPHS.	CDO

5.2.3 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 Polisi Keselamatan Siber MPHS; d) Menguatkuasakan Polisi Keselamatan Siber MPHS; e) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber MPHS. f) Menjalankan pengurusan risiko; g) Menjalankan audit, mengkaji semula, merumus tindak balas 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 siber kepada CDO, Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (GCERT) Selangor dan/atau NACSA seterusnya membantu dalam penyiasatan atau pemulihan; k) bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera. l) menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden	ICTSO

baru dapat dielakkan; m) memastikan pematuhan PKS MPHS oleh pihak luaran seperti perunding, kontraktor dan pembekal yang mencapai dan menggunakan aset ICT MPHS untuk tujuan penyelenggaraan, pemasangan, naik taraf dan sebagainya; n) menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan ICT; dan o) memastikan PKS MPHS dikemaskini sesuai dengan perubahan teknologi, arahan jabatan dan ancaman-ancaman dari semasa ke semasa.	
5.2.4 Penolong Pegawai Teknologi Maklumat / Juruteknik Komputer	
Peranan dan tanggungjawab Penolong Pegawai Teknologi Maklumat (PPTM) / Juruteknik Komputer (JK) 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 Polisi Keselamatan Siber 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; dan g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	Penolong Pegawai Teknologi Maklumat/ Juruteknik Komputer

5.2.5 Pentadbir Sistem ICT	
Pentadbir Sistem ICT bagi MPHS terdiri daripada Pegawai Teknologi Maklumat/Penolong Pegawai Teknologi Maklumat atau Juruteknik Komputer yang berperanan seperti berikut: a) Pentadbir Rangkaian dan Keselamatan b) Pentadbir Pangkalan Data c) Pentadbir Portal/Laman Web *(Webmaster)* d) Pentadbir Bilik Server e) Pentadbir Sistem Aplikasi f) Pentadbir E-mel	Pentadbir Sistem ICT
5.2.6 Pentadbir Rangkaian dan Keselamatan	
Pentadbir Rangkaian dan Keselamatan berperanan dan bertanggungjawab seperti berikut: a) memastikan ketersediaan rangkaian setempat (LAN) dan rangkaian luas (WAN) di MPHS; b) memastikan semua peralatan dan perisian rangkaian dan keselamatan diselenggara; c) merancang peningkatan infrastruktur, ciri keselamatan dan prestasi rangkaian sedia ada; d) mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; e) memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; f) memastikan laluan trafik keluar masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian MPHS secara tidak sah; g) menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian sekiranya perlu; dan h) melaksanakan penilaian tahap keselamatan rangkaian dan sistem ICT *(SPA)* serta penilaian risiko keselamatan maklumat.	Pentadbir Rangkaian dan Keselamat-an

5.2.7 Pentadbir Pangkalan Data	
Pentadbir Pangkalan Data berperanan dan bertanggungjawab seperti berikut: a) melaksanakan polisi pengguna pangkalan data berdasarkan PKS MPHS; b) melaksanakan pemantauan dan penyelenggaraan pangkalan data secara berterusan; c) memastikan aktiviti pentadbiran pangkalan data seperti kawalan capaian dan proses pengemaskinian data dilaksanakan dengan teratur; dan d) melaporkan sebarang insiden berkaitan keselamatan pangkalan data kepada ICTSO.	Pentadbir Pangkalan Data
5.2.8 Pentadbir Portal/Laman Web	
Pentadbir Portal/Laman Web berperanan dan bertanggungjawab seperti berikut: a) menerima dan memuat naik kandungan portal/laman web yang telah disahkan oleh pemilik kandungan; b) memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai antara muka; c) memantau prestasi capaian dan membuat penilaian portal/ laman web secara berkala; d) memastikan rekabentuk portal/laman web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; e) melaksanakan kawalan keselamatan terhadap sistem pengoperasian dan perisian lain di pelayan web; f) melaksanakan proses *backup* dan *restore* secara berkala; dan g) melaporkan sebarang isu pelanggaran keselamatan portal/ laman web kepada ICTSO.	Pentadbir Portal/ Laman Web

5.2.9 Pentadbir Bilik Server	
Pentadbir Bilik Server berperanan dan bertanggungjawab seperti berikut: a) memastikan persekitaran fizikal dan keselamatan Bilik Server dalam keadaan baik dan selamat; b) memastikan keselamatan data dan sistem aplikasi di dalam Bilik Server; dan c) melaporkan sebarang pelanggaran keselamatan Bilik Server kepada ICTSO.	Pentadbir Bilik Server
5.2.10 Pentadbir Sistem Aplikasi	
Pentadbir Sistem Aplikasi berperanan dan bertanggungjawab seperti berikut: a) mengkaji cadangan pembangunan atau penyelenggaraan sistem; b) membuat kajian semula serta menambah baik sistem sedia ada; c) membuat pemantauan dan penyelenggaraan terhadap sistem. d) bertanggungjawab dalam aspek pelaksanaan keseluruhan sistem; e) menyediakan dokumentasi sistem yang berkaitan; f) memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; g) memastikan kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya; h) mematuhi dan melaksanakan prinsip PKS dalam pewujudan akaun pengguna ke atas setiap sistem aplikasi; dan i) melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah seliaannya	Pentadbir Sistem Aplikasi
5.2.11 Pentadbir E-mel	
Pentadbir E-mel berperanan dan bertanggungjawab seperti berikut: a) menentukan setiap akaun yang diwujud atau dibatalkan setelah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar, bersara atau melanggar dasar dan polisi) perlu dilakukan dengan segera atas tujuan keselamatan maklumat.	Pentadbir E-mel

b) membekukan akaun pengguna semasa pengguna bercuti panjang atau sebab-sebab lain atas arahan Ketua Jabatan. c) memastikan kemudahan capaian e-mel melalui pelbagai peralatan ICT dan medium komunikasi d) melaporkan sebarang pelanggaran penggunaan perkhidmatan e-mel kepada ICTSO.	
5.2.12 Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti berikut: a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber MPHS; b) Mengetahui dan memahami implikasi keselamatan ICT dari sudut kesan dan tindakannya; c) Melaksanakan arahan-arahan Polisi Keselamatan Siber 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 Polisi Keselamatan Siber 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	Pengguna
5.2.13 Jawatankuasa Perkhidmatan dan Teknologi Maklumat	
Jawatankuasa Perkhidmatan dan Teknologi Maklumat (JPTM) berfungsi sebagai penyelaras perkara berkaitan perkhidmatan, ICT dan keselamatan siber MPHS seperti berikut: a) Memperakukan kepada MPHS hal-hal berhubung dengan senarai	Ahli JPTM

perjawatan dan perubahan/ pertambahan jawatan mengikut perenggan 16 (1) dan (3), Akta 171; b) Memperakukan cadangan dasar-dasar berkaitan dengan perjawatan, perkhidmatan dan pengurusan sumber manusia; c) Memperakukan Pekeliling-Pekeliling Perkhidmatan untuk diguna pakai di MPHS; d) Mengesyorkan kepada MPHS perkara-perkara yang berkaitan dengan pembangunan modal insan bagi tujuan peningkatan kualiti dan prestasi perkhidmatan; e) Membincangkan mengenai dasar berkaitan kebajikan kakitangan MPHS; f) Mengkaji dan mengesyorkan kepada MPHS cadangan-cadangan bagi program pembangunan teknologi maklumat dan komunikasi; g) Mencadangkan kepada MPHS hal-hal berkaitan perancangan dan pelaksanaan sistem pengkomputeran di PBT; h) Mempertimbangkan dan memperakukan laporan latihan kakitangan dalaman; i) Mempertimbangkan dan memperakukan laporan Jabatan/ Bahagian/ Unit Undang-undang; dan j) Mengkaji cadangan peruntukan undang-undang yang baru dan pindaan/ tambahan kepada yang sedia ada (yang berkaitan).	
5.2.14 Jawatankuasa ISMS	
Jawatankuasa ISMS berfungsi dan berperanan seperti berikut a) mewujud, melaksana, operasi, memantau, menyemak, menyelenggara dan menambahbaik sistem pengurusan keselamatan maklumat di MPHS; b) memberi input, merancang, menyedia dokumentasi ISMS, membuat pengesahan, mengoperasi ISMS, melulus serahan aktiviti-aktiviti projek dan mengurus ISMS bagi memastikan penambahbahbaikan dapat dilaksanakan secara berterusan; c) melapor kemajuan projek dalam Mesyuarat Pengurusan MPHS dan setara.	AJK ISMS

5.3 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
5.4 Tanggungjawab Pihak Pengurusan	
Pihak pengurusan MPHS bertanggungjawab dalam memastikan kakitangan dan pihak yang berurusan dengan MPHS memahami dan mematuhi perundangan, peraturan, pekeliling dan Polisi Keselamatan Siber MPHS serta menyediakan sumber untuk pelaksanaan kawalan keselamatan maklumat di MPHS.	Pihak Pengurusan MPHS
5.5 Hubungan dengan Pihak Berkuasa	
Pentadbiran MPHS hendaklah memastikan senarai perhubungan dengan pelbagai pihak yang berkaitan diwujudkan dan dikemas kini. Ia merupakan sumber rujukan kakitangan MPHS mengetahui senarai perhubungan pihak berkuasa yang berdekatan. Perkara yang perlu dipatuhi adalah seperti berikut: a) mengenal pasti peraturan yang berkuatkuasa dalam melaksanakan peranan dan tanggungjawab jabatan/unit. b) mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan seperti	Semua jabatan

pembekal perkhidmatan, utiliti, kecemasan, keselamatan dan kesihatan. c) melaporkan sebarang insiden keselamatan dengan segera	
5.6 Hubungan dengan Kumpulan Berkepentingan Yang Khusus	
Kakitangan MPHS perlu mempunyai hubungan baik dengan pihak berkepentingan yang khusus bagi: a) meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikut perkembangan terkini mengenai keselamatan maklumat b) menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini c) berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	Kakitangan MPHS
5.7 Perisikan Ancaman *(Threat Intelligence)*	
MPHS perlu mengenal pasti, memahami, dan meramal ancaman siber supaya langkah-langkah pencegahan dan tindak balas yang sesuai dapat diambil untuk melindungi aset maklumat dan memastikan keselamatan siber MPHS.	BTM
5.8 Keselamatan Maklumat dalam Pengurusan Projek	
Keselamatan maklumat perlu diambil kira dalam pengurusan projek bagi melindungi maklumat dengan merujuk kepada ISMS. Perkara-perkara berikut hendaklah dipatuhi iaitu: a) memastikan objektif keselamatan maklumat dimasukkan di dalam objektif projek b) melaksanakan penilaian risiko keselamatan maklumat pada peringkat pelaksanaan projek c) memastikan keselamatan maklumat diambil kira semasa pembangunan projek d) memastikan implikasi keselamatan maklumat ditangani secara teratur dan berkesan.	Pasukan Projek ISMS

5.9	**Inventori Maklumat dan Lain-Lain Aset Berkaitan**	
	MPHS perlu mewujudkan satu inventori lengkap dan terkini bagi semua maklumat dan aset berkaitan (seperti peralatan, perisian, peranti storan, dokumen, sistem dan perkhidmatan pihak ketiga) yang digunakan untuk memproses, menyimpan atau menghantar maklumat dengan tujuan memastikan semua maklumat dan aset berkaitan diiktiraf, dikawal, dan dilindungi daripada kehilangan, penyalahgunaan atau akses tanpa kebenaran. Inventori ini hendaklah: a) Diselenggara secara sistematik dan dikemas kini secara berkala. b) Mengandungi butiran pemilikan aset, klasifikasi maklumat, lokasi aset, dan butiran lain yang diperlukan. c) Digunakan untuk menyokong pengurusan risiko, insiden keselamatan, pematuhan dan tindakan perlindungan maklumat.	Penolong Pegawai Teknologi Maklumat dan Pegawai Aset
5.10	**Penggunaan Aset Yang Dibenarkan dan Lain-Lain Aset Maklumat Yang Berkaitan**	
	MPHS perlu menetapkan dan menguatkuasakan peraturan penggunaan boleh diterima ke atas semua aset dan aset maklumat berkaitan (seperti komputer, perisian, sistem rangkaian, peranti mudah alih, dan data organisasi) untuk memastikan penggunaan secara bertanggungjawab, sah dan mengikut keperluan MPHS. Kawalan ini dapat memastikan aset MPHS digunakan dengan cara yang selamat, bertanggungjawab dan mematuhi peraturan MPHS serta undang-undang yang berkaitan. Peraturan ini hendaklah: a) Dinyatakan secara jelas dalam polisi/prosedur dan dikomunikasikan kepada semua pengguna; b) Meliputi larangan terhadap penyalahgunaan aset seperti	Penolong Pegawai Teknologi Maklumat, Juruteknik Komputer dan Pengguna

pemasangan perisian tidak sah, akses ke laman web berisiko, dan penggunaan peribadi yang berlebihan; dan c) Disokong oleh pemantauan dan tindakan tatatertib jika berlaku pelanggaran.	
5.11 Pemulangan Aset	
Semua kakitangan MPHS hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.	Kakitangan MPHS
5.12 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan oleh YDP MPHS mengikut peringkat sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; atau d) Terhad.	YDP MPHS
5.13 Pelabelan Maklumat	
Prosedur pelabelan peringkat keselamatan pada maklumat hendaklah dilaksanakan berdasarkan Arahan Keselamatan.	Kakitangan MPHS
5.14 Pemindahan Maklumat	
Kawalan ini bertujuan melindungi maklumat semasa dipindahkan, sama ada secara fizikal atau melalui rangkaian komunikasi termasuk pemindahan secara dalaman antara jabatan atau lokasi, serta pemindahan luaran kepada pihak ketiga, pelanggan, atau rakan niaga. Kawalan ini hendaklah: a) Menetapkan prosedur pemindahan yang selamat, termasuk penggunaan kaedah penyulitan dan saluran komunikasi yang dipercayai. b) Mendefinisikan peranan dan tanggungjawab pihak yang terlibat dalam pemindahan maklumat.	Kakitangan MPHS

c) Memastikan rekod pemindahan didokumenkan untuk tujuan pengesanan dan audit. d) Mempunyai perjanjian (kerahsiaan atau ketidaktirisan maklumat yang mencerminkan keperluan MPHS) untuk pemindahan maklumat sama ada secara elektronik atau cetakan di antara MPHS dan pihak luar mengikut keperluan dan tahap sensitiviti maklumat. e) Memastikan pelupusan maklumat hendaklah mengikut prosedur keselamatan semasa seperti Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) atau tatacara Jabatan Arkib Negara;	
5.15 Kawalan Capaian	
Kawalan capaian dilaksanakan bertujuan untuk memastikan hanya individu yang diberi kebenaran boleh mengakses maklumat dan aset berkaitan mengikut peranan dan tanggungjawab mereka. Kawalan capaian hendaklah: a) Ditentukan dan didokumenkan melalui dasar dan prosedur capaian; b) Dikuatkuasakan menggunakan mekanisme teknikal seperti pengesahan pengguna *(authentication),* kawalan peranan, dan pemantauan aktiviti capaian; dan c) Disemak secara berkala untuk mengelakkan akses tidak sah atau tidak relevan. Kawalan capaian yang perlu dilaksanakan 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	BTM MPHS dan ICTSO

kemudahan atau peralatan mudah alih; dan d) Kawalan ke atas kemudahan pemprosesan maklumat.	
5.16 Pengurusan Identiti	
Setiap kakitangan MPHS yang mengakses sistem maklumat perlu mempunyai identiti yang unik dan dikawal dengan selamat sepanjang kitaran hayat identiti tersebut (penciptaan, perubahan, penggantungan hingga penghapusan). Pengurusan identiti hendaklah: a) Menetapkan proses pendaftaran dan pengesahan identiti pengguna secara formal; b) Mengurus perubahan peranan, pemindahan jabatan, atau penamatan perkhidmatan dengan segera; dan c) Disokong dengan kawalan teknikal seperti direktori pengguna, sistem pengurusan identiti, dan log aktiviti pengguna.	BTM MPHS; dan ICTSO
5.17 Maklumat Pengesahan *(Authentication Information)*	
Maklumat pengesahan (kata laluan, PIN, token keselamatan, dan biometric) perlu dilindungi daripada capaian, penggunaan atau pendedahan tanpa kebenaran sepanjang kitaran hayatnya (penciptaan, penyimpanan, penghantaran hingga pemusnahan). Pengurusan maklumat pengesahan hendaklah: a) Menguatkuasakan piawaian kerumitan dan kitar hayat kata laluan; b) Menggunakan mekanisme selamat untuk penyimpanan seperti kaedah penyulitan atau *hashing*; dan c) Melaksanakan kaedah pengesahan berbilang faktor (MFA) jika perlu, terutamanya untuk akses kritikal.	BTM

5.18 Hak Akses	
Hak akses kepada maklumat, sistem, aplikasi, perkakasan ICT hanya diberikan kepada pengguna yang memerlukan mengikut peranan dan tanggungjawab mereka selepas mendapat kelulusan formal. Hak akses perlu disemak secara berkala untuk memastikan kesesuaian. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a) Akaun yang diperuntukkan oleh MPHS sahaja boleh digunakan; b) Akaun 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 hak akses pengguna atas sebab-sebab berikut: i. Bertukar bidang tugas kerja; ii. Bertukar ke agensi lain; iii. Bersara; atau iv. Ditamatkan perkhidmatan.	BTM
5.19 Keselamatan Maklumat Dalam Hubungan Pembekal	
Pembekal yang mengakses, memproses, menyimpan atau menyediakan perkhidmatan berkaitan ICT MPHS perlu mematuhi keperluan keselamatan maklumat yang telah ditetapkan. Kawalan keatas perhubungan dengan pembekal hendaklah mengambilkira perkara berikut:	Semua Jabatan

a) Merangkumi klausa keselamatan maklumat dalam kontrak atau perjanjian; b) Penilaian risiko (tapisan keselamatan, temuduga dll.) sebelum dilantik dan dipantau secara berterusan mengikut keperluan; c) Menyediakan garis panduan yang jelas tentang pengendalian maklumat terperingkat dan hak akses. d) Menyatakan tindakan yang perlu diambil jika berlaku pelanggaran keselamatan oleh pembekal.	
5.20 Menangani Maklumat Keselamatan Dalam Perjanjian Pembekal	
MPHS hendaklah memastikan bahawa semua perjanjian dengan pembekal yang mempunyai akses kepada maklumat atau sistem MPHS mengandungi klausa yang jelas berkaitan keperluan keselamatan maklumat. Perjanjian ini hendaklah: a) Menyatakan tanggungjawab keselamatan maklumat pembekal secara jelas dan terperinci; b) Merangkumi aspek seperti pengurusan akses, perlindungan data sulit, pelaporan insiden keselamatan, dan pematuhan kepada PKS; atau c) Menyediakan hak kepada MPHS untuk menjalankan audit atau pemantauan berkaitan keselamatan siber terhadap pembekal.	Semua jabatan
5.21 Mengurus Keselamatan Maklumat Dalam Rantaian Bekalan Teknologi Maklumat dan Komunikasi (ICT)	
MPHS hendaklah melaksanakan kawalan keselamatan maklumat yang sesuai ke atas semua pihak dalam rantaian bekalan ICT bagi memastikan keselamatan perkhidmatan, produk dan komponen yang diperoleh daripada pembekal. Langkah ini hendaklah merangkumi:	BTM

a) Penilaian risiko keselamatan terhadap pembekal. b) Keperluan keselamatan dimasukkan dalam perolehan, kontrak atau perjanjian. c) Pemantauan pematuhan keselamatan secara berterusan terhadap pembekal dalam rantaian bekalan. d) Keupayaan organisasi untuk bertindak balas sekiranya berlaku insiden keselamatan berkaitan rantaian bekalan.	
5.22 Pemantauan, Semakan dan Pengurusan Perubahan Perkhidmatan Pembekal	
MPHS hendaklah sentiasa memantau dan menyemak perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan c) Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian. Sebarang perubahan skop perkhidmatan yang diberikan oleh pihak ketiga perlu diurus mengikut keperluan semasa. Ianya termasuklah bekalan, perubahan terhadap perkhidmatan sedia ada dan pertambahan perkhidmatan baru. Penilaian risiko perlu dilakukan bergantung kepada tahap kritikal sesuatu sistem dan impak yang wujud terhadap perubahan tersebut.	Semua jabatan
5.23 Keselamatan Maklumat untuk Penggunaan Perkhidmatan Awan	
MPHS perlu mengenalpasti langkah-langkah keselamatan untuk melindungi data dan aplikasi yang disimpan atau diproses dalam persekitaran awan. Ini termasuk kawalan akses, penyulitan data, dan pemantauan berterusan untuk memastikan keselamatan dan pematuhan terhadap peraturan yang ditetapkan.	BTM

5.24	**Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat**	
5.24.1	**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 Polisi Keselamatan Siber 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.	Kakitangan MPHS	
5.24.2	**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:	ICTSO	

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 berkaitan insiden yang berlaku sebagai langkah pencegahan kejadian berulang.	
5.25 Penilaian dan Keputusan Berkenaan Peristiwa Keselamatan Maklumat	
MPHS hendaklah menilai setiap peristiwa keselamatan maklumat yang dilaporkan bagi menentukan sama ada ia merupakan insiden keselamatan maklumat dan tindakan susulan yang diperlukan.	BTM
5.26 Tindak Balas Terhadap Insiden Keselamatan Maklumat	
MPHS hendaklah membangunkan dan melaksanakan prosedur tindak balas terhadap insiden keselamatan maklumat untuk memastikan tindakan segera, berkesan dan tersusun dapat diambil apabila insiden berlaku.	BTM
5.27 Belajar Daripada Insiden Keselamatan Maklumat	
MPHS hendaklah menjalankan penilaian selepas sesuatu insiden keselamatan maklumat berlaku untuk mengenal pasti punca sebenar, kelemahan kawalan keselamatan dan tindakan pembaikan yang diperlukan. Proses pembelajaran daripada insiden perlu merangkumi: a) Kajian semula terhadap insiden, termasuk garis masa, tindak balas dan Keputusan; b) Analisis punca akar *(root cause analysis)* untuk mengenal pasti	BTM

kegagalan kawalan atau proses; c) Pembangunan pelan tindakan pembaikan bagi mengelakkan insiden serupa berulang; dan d) Pengemaskinian polisi, prosedur dan kawalan keselamatan sedia ada berdasarkan penemuan. e) Penyebaran pembelajaran kepada pihak berkaitan bagi meningkatkan kesedaran dan kesiapsiagaan.	
5.28 Pengumpulan Bukti	
Bukti berkaitan insiden keselamatan maklumat dikumpulkan, didokumenkan dan disimpan dengan betul untuk menyokong siasatan serta tindakan lanjut, termasuk perundangan jika perlu.	BTM
5.29 Keselamatan Maklumat Semasa Gangguan	
Keselamatan maklumat perlu terus dipelihara semasa berlaku gangguan terhadap operasi perkhidmatan MPHS, termasuk semasa pelaksanaan pelan kesinambungan perkhidmatan (BCP) atau pelan pemulihan bencana (DRP). Kawalan ini hendaklah merangkumi: a) Prosedur yang memastikan perlindungan terhadap maklumat sensitif dan sistem penting walaupun dalam keadaan kecemasan atau gangguan. b) Pemeliharaan kawalan capaian dan pencegahan terhadap kebocoran maklumat walaupun semasa sistem utama tidak berfungsi. c) Penilaian risiko berkala terhadap senario gangguan untuk memastikan pelan tindak balas kekal relevan dan berkesan. d) Latihan dan simulasi berkala kepada kakitangan bagi menguji keberkesanan tindakan keselamatan semasa gangguan.	BTM dan Unit Integriti
5.30 Kesediaan ICT untuk Kesinambungan Perkhidmatan	
MPHS perlu memastikan kesiapsiagaan sistem dan infrastruktur teknologi maklumat untuk memastikan operasi harian MPHS dapat	BTM

diteruskan tanpa gangguan dalam situasi kecemasan. Ini termasuk pelan kesinambungan perkhidmatan, pelan pemulihan bencana, ujian berkala dan langkah pencegahan untuk mengurangkan risiko gangguan.	
5.30.1 Pelan Pengurusan Kesinambungan Perkhidmatan	
Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan* - BCP) 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 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 dan latihan berkaitan kepada pengguna mengenai prosedur kecemasan; f) Membuat *backup*; dan g) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. BCP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:-	Unit Integriti

a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; b) Senarai individu MPHS dan pembekal beserta nombor yang boleh dihubungi (telefon, e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan individu 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 BCP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. BCP 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 BCP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan individu yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. Hebahan kepada ahli dan individu BCP (bahagian yang berkenaan) perlu dilaksanakan dan BCP perlu sedia untuk diakses apabila diperlukan.	

MPHS hendaklah memastikan salinan BCP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	
5.31 Undang-Undang, Statutori, Kawal Selia dan Kontrak Perjanjian	
MPHS hendaklah mengenal pasti, mendokumen dan mematuhi semua keperluan undang-undang, statutori, kawal selia dan kontrak yang berkaitan dengan keselamatan maklumat, termasuk keperluan yang berkaitan dengan harta intelek, perlindungan data peribadi, kerahsiaan, audit dan pematuhan industri. Kawalan ini hendaklah meliputi: a) Penilaian dan dokumentasi keperluan undang-undang dan kontrak yang berkaitan dengan pemprosesan, penyimpanan dan pemindahan maklumat; b) Penyemakan berkala terhadap perubahan perundangan dan keperluan kawal selia yang berpotensi memberi kesan kepada sistem dan dasar keselamatan maklumat; c) Latihan dan kesedaran kepada kakitangan tentang tanggungjawab pematuhan undang-undang yang berkaitan; dan d) Pelaksanaan proses dalaman untuk memastikan pematuhan terhadap syarat kontrak dengan pembekal, pelanggan dan pihak ketiga.	Semua jabatan
5.32 Hak Harta Intelek *(Intellectual Property Rights)*	
MPHS hendaklah mengenal pasti, melindungi dan menghormati hak harta intelek (IPR) berkaitan dengan maklumat, perisian, sistem dan bahan lain yang digunakan dalam perkhidmatan dan operasi MPHS. Ini termasuk lesen perisian, hak cipta, paten, tanda dagangan, dan hasil kerja yang dimiliki atau digunakan oleh MPHS. 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	Kakitangan MPHS

perlindungan harta intelek; d) Mengekalkan daftar aset dan mengenalpasti semua keperluan perlindungan terhadap aset; e) Menyimpan lesen perisian; f) Memastikan bilangan had lesen tidak melebihi had ditetapkan; dan g) Menjalankan pemeriksaan perisian yang sah dan produk berlesen digunakan.	
5.33 Perlindungan Rekod *(Protection of Records)*	
Setiap rekod perlu dilindungi daripada kehilangan, kemusnahan, pemalsuan, akses dan pendedahan yang tidak dibenarkan mengikut keperluan perundangan, peraturan, kontrak dan perkhidmatan.	Kakitangan MPHS
5.34 Privasi dan Perlindungan Maklumat Pengenalan Peribadi (PII)	
Setiap kakitangan dan 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 ISMS, undang-undang dan peraturan yang berkenaan di Malaysia. Setiap kakitangan dan 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
5.35 Kajian Semula Bebas Terhadap Keselamatan Maklumat	
Pelaksanaan keselamatan maklumat MPHS hendaklah dikaji semula secara bebas atau oleh pihak ketiga pada jangka masa yang dirancang atau apabila berlaku perubahan ketara dalam pelaksanaannya.	BTM

5.36	**Pematuhan Dasar, Peraturan dan Piawaian Untuk Keselamatan Maklumat**	
Pelaksanaan keselamatan maklumat MPHS hendaklah dikaji semula secara bebas atau oleh pihak ketiga pada jangka masa yang dirancang atau apabila berlaku perubahan ketara dalam pelaksanaannya.		BTM
5.37	**Prosedur Operasi Yang Didokumenkan**	
MPHS perlu menyediakan, menyelenggara dan melaksanakan prosedur operasi yang didokumenkan bagi memastikan sistem dan maklumat dikendalikan secara konsisten, selamat dan terkawal. Dokumen prosedur operasi ini hendaklah: a) Disediakan secara jelas dan boleh diakses oleh kakitangan yang berkaitan. b) Disemak serta dikemas kini secara berkala. c) Diselaraskan dengan keperluan kawal selia, polisi keselamatan maklumat dan keperluan operasi.		Kakitangan MPHS

BIDANG 06 KAWALAN MANUSIA	
6.1 Tapisan Keselamatan	
MPHS perlu menjalankan tapisan keselamatan untuk pegawai dan kakitangan MPHS serta pihak ketiga berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Jabatan Khidmat Pengurusan
6.2 Terma dan Syarat Perkhidmatan	
Semua pegawai dan kakitangan, pembekal, perunding dan pihak-pihak berkepentingan yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa serta mengurus keselamatan aset ICT mengikut perundangan dan peraturan yang ditetapkan oleh MPHS.	Jabatan Khidmat Pengurusan, Bahagian Perolehan, BTM
6.3 Kesedaran, Pendidikan dan 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.	Jabatan Khidmat Pengurusan
6.4 Tindakan Disiplin	
Ketidakakuran kepada PKS, polisi dan prosedur berkaitan keselamatan ICT boleh membawa kepada tindakan tatatertib sekiranya perlu.	Unit Integriti

6.5 Tanggungjawab Selepas Penamatan Atau Pertukaran Pekerjaan	
Kawalan ini bertujuan memastikan semua akses kepada maklumat dan aset MPHS dihentikan selepas penamatan perkhidmatan atau pertukaran peranan seseorang individu. Ini termasuk penamatan akaun pengguna, pemulangan aset seperti komputer, kad akses, dokumen sulit, serta penamatan hak istimewa dan kebenaran lain. MPHS juga hendaklah memastikan pekerja, kontraktor atau pihak ketiga memahami tanggungjawab mereka untuk terus melindungi maklumat sulit dan data organisasi walaupun selepas hubungan pekerjaan ditamatkan.	Jabatan Khidmat Pengurusan
6.6 Kerahsiaan dan *Non Disclosure Agreement (NDA)*	
Perjanjian dengan individu atau pembekal harus merangkumi keperluan untuk menangani sebarang risiko keselamatan maklumat yang berkaitan dengan teknologi maklumat dan komunikasi serta rantaian bekalan produk dan perkhidmatan. Tanggungjawab kerahsiaan atau ketakdedahan hendaklah diperuntukkan di dalam sesuatu perjanjian atau *NDA* yang ditandatangani antara MPHS dan pihak luar yang berkaitan mengikut polisi, prosedur dan keperluan MPHS serta hendaklah dikenalpasti, disemak dan didokumentasi. Tanggungjawab kerahsiaan tersebut hendaklah dipersetujui dan dipatuhi oleh semua pihak bagi memenuhi keperluan keselamatan maklumat yang relevan.	Semua Jabatan
6.7 Kerja Jarak Jauh	
Kakitangan MPHS yang bekerja secara jarak jauh perlu mendapat kebenaran dan mematuhi garis panduan keselamatan yang telah ditetapkan bagi memastikan keselamatan maklumat dan aset MPHS sentiasa terjaga walaupun di luar persekitaran pejabat. Penggunaan peranti yang diluluskan, sambungan rangkaian yang selamat (seperti VPN), akses terhad kepada sistem MPHS, serta	Kakitangan MPHS

perlindungan fizikal terhadap peranti dan maklumat yang digunakan di luar premis organisasi perlu diambilkira semasa kerja jarak jauh.	
6.8 Pelaporan Peristiwa Keselamatan Maklumat	
Semua peristiwa yang berkaitan dengan keselamatan maklumat, termasuk insiden sebenar, cubaan serangan, atau kelakuan mencurigakan, dilaporkan dengan segera kepada pihak yang bertanggungjawab (pengawal keselamatan, ICTSO) melalui saluran yang disediakan. Latihan dan kesedaran juga diberikan supaya setiap kakitangan MPHS mengetahui tanggungjawab mereka dalam mengenal pasti dan melaporkan peristiwa keselamatan maklumat.	Kakitangan MPHS

BIDANG 07 KAWALAN FIZIKAL	
7.1 Perimeter Keselamatan Fizikal	
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) Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana;	Jabatan Khidmat Pengurusan
7.2 Kemasukan 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	Jabatan Khidmat Pengurusan

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; f) Setiap pelawat perlu mengisi log keluar masuk bilik server.	
7.3 Keselamatan Pejabat, Bilik dan Kemudahan	
Keselamatan fizikal untuk pejabat, bilik dan kemudahan seperti pintu berkunci, kad akses dan pengimbas jari hendaklah dilaksanakan.	Jabatan Khidmat Pengurusan
7.4 Pemantauan Keselamatan Fizikal	
Premis MPHS perlu dipantau secara berterusan semasa atau diluar waktu perkhidmatan untuk mencegah akses fizikal yang tidak dibenarkan.	Jabatan Khidmat Pengurusan
7.5 Melindungi Daripada Ancaman Fizikal dan Alam Sekitar	
MPHS hendaklah melaksanakan kawalan untuk melindungi kemudahan pemprosesan maklumat daripada ancaman luaran dan persekitaran seperti bencana alam, kebakaran, banjir, pencemaran, sabotaj, dan pencerobohan fizikal. Reka bentuk premis, sistem keselamatan dan prosedur operasi mestilah mengambil kira risiko-risiko ini dan disesuaikan untuk mengurangkan kesannya. Langkah-langkah ini termasuk penggunaan pengesan asap dan haba, sistem pemadam kebakaran, kawalan suhu dan kelembapan, pengawasan CCTV serta kawalan akses ke kawasan larangan.	Jabatan Khidmat Pengurusan
7.6 Bekerja di Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kakitangan yang tertentu sahaja. Akses ke kawasan ini hendaklah dihadkan hanya kepada individu yang diberi kuasa, dan	Jabatan Khidmat Pengurusan

mempunyai langkah keselamatan fizikal seperti sistem kawalan akses, rakaman CCTV dan pemantauan keselamatan. Langkah tambahan seperti pengiring bagi pelawat, larangan penggunaan peranti rakaman peribadi, dan pengesahan identiti juga hendaklah dipraktikkan bagi memastikan kawasan tersebut kekal terjamin.	
7.7 *Clear Desk dan Clear Screen*	
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 c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Kakitangan MPHS
7.8 Penempatan dan Perlindungan 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 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;	Kakitangan MPHS

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 Komputer yang bertanggungjawab perlu memastikan aktiviti peminjaman dan pemulangan peralatan ICT direkodkan dan menyemak peralatan yang dipulangkan berada dalam keadaan baik dan lengkap.	
7.9 Keselamatan Aset 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 atau PPTM 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.	Kakitangan MPHS

7.10 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti thumb drive, *external hard disk* dan media-media storan fizikal lain. Media-media storan ini 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: 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 terperingkat perlu diletakkan kata laluan supaya hanya orang yang berhak sahaja dapat membukanya.	Kakitangan MPHS

7.11 Utiliti Sokongan	
Peralatan yang kritikal perlu dilindungi dari kegagalan kuasa elektrik dan sebarang gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara yang perlu dipatuhi adalah seperti berikut: i. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; ii. Peralatan sokongan seperti *Uninterruptable Power Supply (UPS)* dan penjana (generator) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya bekalan kuasa berterusan; dan iii. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	BTM
7.12 Keselamatan 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; 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.	BTM

7.13 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; e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada ICTSO.	BTM
7.14 Pelupusan atau Penggunaan Semula Perkakasan	
Pelupusan	
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 membuat penduaan;	Pegawai Aset

c) BTM akan membantu Jabatan Khidmat Pengurusan 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) Kakitangan MPHS 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) Kakitangan MPHS bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti storan mudah alih atau *thumb drive dan hard disk* sebelum menghapuskan	

maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
Penggunaan Semula	
Sebelum peralatan digunakan semula oleh jabatan lain, kakitangan baru atau pihak luar, semua maklumat terdahulu perlu dipadam secara kekal. Ini termasuk penghapusan maklumat peribadi, data pelanggan, atau perisian berlesen yang tidak lagi diperlukan.	Pegawai Aset

BIDANG 08 KAWALAN TEKNOLOGI	
8.1 Peranti Pengguna	
MPHS hendaklah memastikan peranti pengguna seperti komputer riba, telefon pintar, tablet dan peranti mudah alih lain yang digunakan untuk mengakses, memproses atau menyimpan maklumat MPHS, dilindungi dengan kawalan keselamatan yang bersesuaian. Antara kawalan yang boleh dilaksanakan termasuk: a) Pemasangan perisian *antivirus, firewall* dan mekanisme kawalan akses. b) Penyulitan storan data dalam peranti. c) Kemaskini sistem operasi dan aplikasi secara berkala. d) Keupayaan untuk memadam data secara jarak jauh sekiranya peranti hilang atau dicuri.	BTM
8.2 Hak Akses Istimewa	
Hak akses istimewa kepada sistem, aplikasi, dan perkhidmatan yang mengendalikan maklumat sensitif atau kritikal hanya diberikan kepada individu yang benar-benar memerlukannya untuk menjalankan tugas mereka. Langkah-langkah perlindungan termasuk: a) Menetapkan prosedur untuk mengawal permintaan, pemberian, dan pengawasan hak akses istimewa. b) Menggunakan prinsip *"least privilege"* (akses minimum) untuk memastikan hak akses diberikan hanya untuk aktiviti yang diperlukan. c) Memastikan pengauditan dan pengawasan berterusan terhadap semua penggunaan hak akses istimewa. d) Mengubah kata laluan secara berkala dan memastikan kata laluan yang kuat digunakan untuk akses istimewa.	BTM

8.3 Sekatan Capaian Maklumat	
Sekatan akses kepada maklumat dan aset berkaitan berdasarkan prinsip *"need-to-know"* (hanya yang perlu tahu) dan klasifikasi maklumat. Proses sekatan akses ini harus disesuaikan dengan peranan, tanggungjawab, dan keperluan individu serta memastikan bahawa akses diberikan hanya kepada pihak yang berhak.	BTM
8.4 Akses Kepada Kod Sumber	
Akses kepada kod sumber, alat pembangunan, dan *application library* hendaklah dikawal dengan ketat dan diberikan hanya kepada individu yang mempunyai keperluan untuk mengaksesnya berdasarkan peranan mereka. Proses pengurusan akses ini hendaklah ditetapkan untuk memastikan bahawa hanya individu yang berkelayakan dan diberi kuasa dapat mengakses kod sumber. Langkah-langkah kawalan termasuk: a) Menetapkan prosedur pengesahan untuk mengawal akses kepada kod sumber dan alat pembangunan. b) Menggunakan kawalan akses berasaskan peranan *(RBAC)* untuk memberikan akses hanya kepada individu yang perlu. c) Menyediakan audit dan log untuk menjejaki akses kepada kod sumber dan mengesan sebarang akses yang tidak sah.	BTM
8.5 Pengesahan Selamat *(Secure Authentication)*	
Prosedur dan teknologi pengesahan yang selamat hendaklah digunakan untuk memastikan hanya pengguna yang sah dapat mengakses maklumat dan sistem yang dilindungi.	BTM
8.6 Pengurusan 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	BTM

keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	
8.7 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 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.	BTM dan kakitangan MPHS
8.8 Pengurusan Kelemahan Teknikal	
Sistem di MPHS hendaklah dipantau secara berterusan untuk mengenal pasti dan menilai kelemahan teknikal yang boleh dieksploitasi oleh pihak yang tidak bertanggungjawab, dan tindakan pemulihan yang sesuai perlu diambil.	BTM

8.9 Pengurusan Konfigurasi	
Konfigurasi tetapan dan keselamatan untuk perkakasan, perisian, perkhidmatan, dan rangkaian hendaklah ditetapkan, didokumenkan, dilaksanakan, dipantau dan disemak secara berkala.	BTM
8.10 Pemadaman Data *(Data Deletion)*	
MPHS perlu melaksanakan proses pemadaman data dan maklumat dengan selamat untuk memastikan ia tidak dapat dipulihkan atau disalahgunakan. Ini termasuk penggunaan teknik pemadaman seperti penyulitan atau pemusnahan fizikal untuk melindungi maklumat sensitif.	BTM dan Jabatan Khidmat Pengurusan
8.11 Penyamaran Data *(Data Masking)*	
MPHS perlu melindungi data sensitif semasa digunakan dalam persekitaran yang tidak selamat dengan menggantikannya dengan data palsu atau diubah suai tetapi masih mengekalkan struktur dan format asal. Tujuan utama penyamaran data adalah untuk melindungi privasi dan keselamatan maklumat.	BTM
8.12 Pencegahan Kebocoran Data	
MPHS perlu melaksanakan langkah-langkah keselamatan untuk mencegah kehilangan atau pendedahan data sensitif kepada pihak yang tidak sah. Ini termasuk penggunaan perisian DLP *(data loss prevention)*, pemantauan aktiviti pengguna, dan kawalan akses yang ketat.	BTM
8.13 *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;	BTM

b) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; c) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	
8.14 *Redundancy* Kemudahan Pemprosesan Maklumat	
Sistem, aplikasi atau perkakasan yang kritikal perlu dipertimbangkan untuk mempunyai kemudahan *redundancy* dan diuji *(failover test)* keberkesanannya mengikut keperluan.	BTM
8.15 *Logging*	
Semua jenis log *(access logs, security logs, system logs, application logs, audit logs, network logs, event logs, error logs, forensic logs, service logs)* yang merekod aktiviti, pengecualian, kesilapan, dan peristiwa relevan lain hendaklah dihasilkan, disimpan, dilindungi dan dianalisis untuk tujuan pemantauan keselamatan.	BTM
8.16 Pemantauan Aktiviti	
Pemantauan berterusan ke atas rangkaian, sistem, dan aplikasi untuk mengenal pasti sebarang aktiviti yang mencurigakan atau tidak normal perlu dilaksanakan dengan tujuan mengesan dan menangani kemungkinan insiden keselamatan maklumat dengan segera. Tindakan yang sesuai perlu diambil bagi menilai potensi risiko, mengenal pasti punca masalah, dan mengurangkan impak terhadap keselamatan maklumat organisasi.	BTM
8.17 Penyeragaman Jam	
Waktu server dan peralatan ICT yang berpusat dan kritikal perlu diselaraskan dengan satu sumber piawaian waktu menggunakan *Network Time Protocol (NTP) Server*. Masa yang berkaitan dengan sistem pemprosesan maklumat ICT MPHS mestilah diseragamkan mengikut rujukan punca masa yang sama. Ini untuk memastikan ketepatan masa log yang disimpan serta bertujuan untuk mengawal	BTM dan Jabatan Khidmat Pengurusan

integriti log tersebut bagi kegunaan masa hadapan.	
8.18 Penggunaan Program Utiliti Khas	
Penggunaan program utiliti khas yang berkemungkinan mampu untuk mengatasi kawalan sistem dan aplikasi perlu dihadkan dan dikawal ketat.	BTM
8.19 Pemasangan Perisian Pada Sistem Operasi	
Pemasangan perisian oleh pengguna perlu dikawal dan disemak secara berkala bagi memastikan tiada sebarang bentuk ancaman atau gangguan ke atas sistem yang beroperasi.	BTM
8.20 Keselamatan Rangkaian	
Rangkaian dan peralatan rangkaian perlu dilindungi, dikawal dan diurus dengan betul bagi melindungi maklumat dalam sistem dan aplikasi daripada ancaman luar dan dalaman seperti akses tanpa kebenaran, pengintipan atau serangan siber.	BTM
8.21 Keselamatan Perkhidmatan Rangkaian	
MPHS perlu mengenal pasti, melaksanakan dan memantau mekanisme keselamatan, tahap perkhidmatan serta keperluan keselamatan bagi semua perkhidmatan rangkaian yang digunakan.	BTM
8.22 Pengasingan Dalam Rangkaian	
Pengasingan kumpulan perkhidmatan maklumat, pengguna dan sistem maklumat dalam rangkaian perlu dilaksanakan untuk mengurangkan risiko akses tidak sah dan mengawal pergerakan data antara zon rangkaian serta membantu menghadkan skop serangan jika berlaku pencerobohan.	BTM
8.23 Penapisan Web	
MPHS perlu mengawal akses kakitangan kepada kandungan dalam talian. Ini termasuk menyekat akses kepada laman web yang tidak sesuai atau berbahaya untuk melindungi kakitangan, data dan sistem MPHS daripada ancaman siber.	BTM

8.24 Penggunaan Kriptografi	
Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa. Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	ICTSO
8.25 Kitar Hayat Pembangunan Selamat	
MPHS hendaklah menetapkan dan menguatkuasakan peraturan bagi memastikan amalan keselamatan dilaksanakan secara konsisten dalam setiap peringkat pembangunan perisian dan sistem, termasuk reka bentuk, pembangunan, ujian dan penyebaran. Mengintegrasikan kawalan keselamatan dalam kitar hayat pembangunan membantu mengesan dan menangani kelemahan lebih awal, mengurangkan risiko eksploitasi, dan memastikan produk akhir lebih selamat digunakan oleh pengguna serta patuh terhadap keperluan pematuhan dan kawal selia.	BTM
8.26 Keperluan Keselamatan Aplikasi	
Keperluan keselamatan maklumat perlu dilaksanakan apabila membangunkan atau memperoleh aplikasi. Menetapkan keperluan keselamatan sejak awal pembangunan dapat memastikan aplikasi dibina dengan mempertimbangkan kawalan yang bersesuaian untuk melindungi data dan fungsi penting daripada risiko keselamatan.	BTM
8.27 Prinsip Kejuruteraan Sistem Selamat	
MPHS perlu menetapkan, mendokumen, menyelenggara dan melaksanakan prinsip kejuruteraan sistem selamat dalam semua aktiviti pembangunan sistem maklumat. Memastikan prinsip kejuruteraan keselamatan diterapkan dalam reka bentuk sistem membolehkan pembinaan sistem yang teguh, berdaya	ICTSO

tahan dan mampu menangkis ancaman siber secara proaktif.	
8.28 Pengekodan Selamat	
Amalan pengekodan selamat hendaklah diterapkan dalam pembangunan perisian. Pengekodan yang mematuhi piawaian keselamatan membantu mengelakkan kelemahan seperti *injection, buffer overflow* dan kerentanan lain yang boleh dieksploitasi oleh pihak tidak bertanggungjawab.	ICTSO
8.29 Ujian Keselamatan Dalam Pembangunan dan Penerimaan Sistem	
Proses ujian keselamatan hendaklah ditakrif, dilaksanakan dan disepadukan dalam keseluruhan kitar hayat pembangunan sistem, termasuk sebelum penerimaan akhir oleh pengguna atau pentadbir sistem.	ICTSO
8.30 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
8.31 Pengasingan Persekitaran Pembangunan, Ujian dan Operasi	
Persekitaran pembangunan, ujian dan pengeluaran hendaklah diwujudkan secara berasingan dan dilindungi dengan kawalan keselamatan yang sewajarnya. Pengasingan persekitaran memastikan perubahan, ujian dan pembangunan sistem tidak memberi kesan negatif atau mengganggu operasi sistem sebenar. Ia juga mengurangkan risiko akses tidak sah terhadap maklumat pengeluaran yang sensitif serta mengelakkan potensi kehilangan data, kerosakan sistem atau pendedahan kepada kerentanan akibat ujian atau kod pembangunan yang belum stabil. Pendekatan ini penting bagi memastikan keselamatan, integriti dan ketersediaan sistem MPHS.	ICTSO

8.32 Pengurusan 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; 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;	Kakitangan MPHS
8.33 Maklumat Ujian	
MPHS perlu memastikan maklumat yang digunakan untuk pengujian adalah dikawal dan dilindungi. Maklumat ujian yang digunakan semasa pembangunan sistem/aplikasi hendaklah dilupuskan secara kekal *(secured delete)* selepas projek disiapkan/tamat kontrak	BTM
8.34 Perlindungan Sistem Maklumat Semasa Ujian Audit	
Aktiviti audit dan ujian penilaian ke atas sistem maklumat hendaklah dirancang, diluluskan dan dilaksanakan secara terkawal untuk memastikan tiada gangguan terhadap operasi sistem dan perlindungan terhadap maklumat sensitif.	ICTSO

GLOSARI

GLOSARI	
BTM	Bahagian Teknologi Maklumat
CCTV	*Closed-circuit* Kamera Litar Tertutup
CDO	*Chief Digital Officer*
GCERT	*Government Computer Emergency Response Team* Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan
ICT	*Information dan Communication Technology* Teknologi Maklumat dan Komunikasi
ICTSO	*Information dan Communication Technology Security Officer* Pegawai Keselamatan Teknologi Maklumat dan Komunikasi
LAN	*Local Area Network* Rangkaian Setempat
MPHS	Majlis Perbandaran Hulu Selangor
NACSA	*National Cyber Security Agency* Agensi Keselamatan Siber Kebangsaan
PKS	Polisi Keselamatan Siber
Semua	Kakitangan, pembekal dan pihak ketiga MPHS
WAN	*Wide Area Network* Rangkaian Luas
YDP	Yang Dipertua

Lampiran 1

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
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 Polisi Keselamatan Siber MPHS; dan

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

Tandatangan : ----------

Tarikh : ----------

Pengesahan Pegawai Keselamatan ICT (ICTSO)

(MOHAMAD RAMDAN BIN IBRAHIM)
Ketua Bahagian Teknologi Maklumat,
b.p. Yang Dipertua,
Majlis Perbandaran Hulu Selangor

Tarikh:

Lampiran 2

SENARAI PERUNDANGAN DAN PERATURAN

1. Arahan Keselamatan,
2. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”,
3. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS),
4. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT),
5. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan”,
6. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam,
7. 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;
8. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
9. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
10. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
11. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
12. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
13. Akta Tandatangan Digital 1997,
14. Akta Rahsia Rasmi 1972,
15. Akta Jenayah Komputer 1997,

16. Akta Hak cipta (Pindaan) Tahun 1997,
17. Akta Komunikasi dan Multimedia 1998,
18. Perintah-Perintah Am,
19. Arahan Perbendaharaan,
20. Arahan Teknologi Maklumat 2007,
21. Garis Panduan Keselamatan MAMPU 2004;
22. Standard Operating Procedure (SOP) ICT MAMPU;
23. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
24. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010
25. Pelaksanaan Perintah Kawalan Pergerakan Berkaitan Penularan Wabak Covid-19 Peringkat Pentadbiran Kerajaan Negeri Selangor bertarikh 17 Mac 2020
26. Operasi Pejabat Kerajaan Semasa Perintah Kawalan Pergerakan Bersyarat bertarikh 2 Mei 2020
27. Budaya Kerja Perkhidmatan Awam Semasa Tempoh Perintah Kawalan Pergerakan Pemulihan (PKPP) Pentadbiran Kerajaan Negeri Selangor bertarikh 9 Jun 2020
28. Surat Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam
29. Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024
30. Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024