مجليس فرينداراڽ سلايغ
Majlis Perbandaran Selayang

POLISI KESELAMATAN SIBER MAJLIS PERBANDARAN SELAYANG

VERSI 1.0 | 01 JANUARI 2026

JABATAN TEKNOLOGI MAKLUMAT

ISI KANDUNGAN

ISI KANDUNGAN **MUKA SURAT**

ISI KANDUNGAN **MUKA SURAT**

ISI KANDUNGAN **MUKA SURAT**

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
23 DISEMBER 2025	1.0	Mesyuarat Pengurusan MPS Bil 11/2025	01 JANUARI 2026

JADUAL PINDAAN POLISI KESELAMATAN SIBER
MAJLIS PERBANDARAN SELAYANG

TARIKH	VERSI	MUKA SURAT	BUTIRAN PINDAAN
01/01/2026	**1.0**	**-**	Dokumen asal

PENGENALAN

Polisi Keselamatan Siber (PKS) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) Majlis Perbandaran Selayang (MPS). Polisi ini juga menerangkan kepada semua pengguna di MPS mengenai tanggungjawab dan peranan pengguna dalam melindungi aset ICT MPS. PKS ini disediakan berpandu kepada piawaian antarabangsa iaitu ISO/IEC 27001:2022 *Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems*.

OBJEKTIF

Objektif utama PKS adalah seperti berikut:

(a) Memastikan kelancaran operasi jabatan yang berlandaskan ICT dengan mencegah serta meminimumkan risiko 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, tidak boleh disangkal, ketersediaan dan kesahihan;

(c) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan aset ICT; dan

(d) Meningkatkan tahap kesedaran keselamatan ICT kepada para kakitangan, pengguna dan Pihak Ketiga.

PERNYATAAN POLISI

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

Keselamatan siber adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan siber berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan siber iaitu:

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

PKS MPS merangkumi perlindungan ke atas semua bentuk maklumat digital dan bukan digital bertujuan untuk menjamin keselamatan maklumat tersebut dan ketersediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti yang berikut:

(a) **KERAHSIAAN** - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
(b) **INTEGRITI** - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
(c) **TIDAK BOLEH DISANGKAL** - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
(d) **KESAHIHAN** - Data dan maklumat hendaklah dijamin kesahihannya; dan
(e) **KETERSEDIAAN** - Data dan maklumat hendaklah boleh diakses pada bila-bila masa

Selain dari itu, langkah-langkah ke arah menjamin keselamatan siber hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semua jenis 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

Aset ICT MPS terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. PKS MPS menetapkan keperluan-keperluan asas berikut:

a) Data dan maklumat hendaklah boleh dicapaian secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

PKS MPS merangkumi perlindungan ke atas semua bentuk maklumat ICT kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dan yang dibuat salinan. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

a) Data dan Maklumat
Semua data dan maklumat elektronik dan bercetak yang disimpan atau digunakan di pelbagai media termasuk prosedur, manual pengguna, sistem dokumentasi, rekod, pangkalan data dan lain-lain;

b) Peralatan ICT
Semua peralatan komputer seperti komputer peribadi, komputer riba, pencetak, media storan, server, *firewall*, peralatan multimedia & komunikasi dan alat sokongan yang lain;

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

d) Perkhidmatan
Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi- fungsinya. Contohnya Adalah seperti berikut:
   i. perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
   ii. sistem halangan akses seperti sistem kad akses; dan
   iii. perkhidmatan sokongan seperti kemudahan elektrik, pendingin hawa, sistem pencegah kebakaran dan lain-lain.

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

f) Persekitaran Fizikal
Persekitaran fizikal yang merujuk kepada lokasi fizikal yang menempatkan perkara a) – e) di atas.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada PKS MPS 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;

(b) Hak Akses Minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca atau melihat sahaja. Kelulusan khas diperlukan untuk membolehkan pengguna mencipta, menyimpan, mengemas kini, mengubah dan menghapuskan sesuatu data atau maklumat.

(c) Kebertanggungjawaban atau Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Bagi menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesahkan bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

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
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum;

(d) Pengasingan

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

(e) Pengauditan

Tujuan aktiviti ini ialah untuk mengenal pasti insiden keselamatan aset ICT atau keadaan yang mengancam keselamatan aset ICT. Dengan itu, semua log yang berkaitan dengan aset ICT perlu disimpan bagi tujuan jejak audit;

(f) Pematuhan

PKS MPS hendaklah dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

(g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan ketersediaan dan kebolehcapaian bagi meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui proses penduaan (*backup*) dan mewujudkan *Disaster Recovery Plan* (DRP) di bawah Pengurusan Kesinambungan Perkhidmatan (PKP).

(h) Saling Bergantung

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

PENILAIAN RISIKO KESELAMATAN ICT

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

MPS hendaklah melaksanakan penilaian risiko keselamatan siber secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan siber. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan siberberdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan siber hendaklah dilaksanakan ke atas sistem maklumat MPS termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah Bilik *Server* Utama MPS, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

MPS bertanggungjawab melaksanakan dan menguruskan risiko selaras dengan Surat Pekeliling Am Bilangan 3 Tahun 2024: Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam.

MPS perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

(a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

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

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

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

RINGKASAN POLISI KESELAMATAN SIBER MPS

Maklumat perniagaan MPS adalah salah satu aset kritikal Majlis dan ia terdedah kepada kedua-dua ancaman keselamatan luaran dan dalaman. Maklumat perniagaan MPS wujud dalam salinan cetak, elektronik dan audio visual dan dasar ini merangkumi perlindungan aset perniagaan sepanjang kitaran hayatnya, daripada penciptaan kepada penghantaran, penyimpanan dan pemusnahan. Ia boleh dihantar dengan tangan, dihantar secara elektronik, melalui pos atau disampaikan secara lisan.

Sebagai dasar korporat, perlindungan dan kawalan yang mencukupi hendaklah diwujudkan untuk memastikan pemeliharaan kerahsiaan, ketersediaan dan integriti maklumat perniagaan MPS, dalam semua bentuk, dan infrastruktur sokongannya. Polisi ini hendaklah disemak sekurang-kurangnya sekali setiap 3 tahun, atau sekiranya terdapat perubahan polisi dalam tempoh kurang dari tiga (3) dari semakan akhir polisi.

Polisi ini mengandungi sepuluh (10) bahagian yang telah ditanda aras dengan ISO/IEC 27001:2022:

a) Polisi Keselamatan Siber
   MPS hendaklah mewujudkan struktur tadbir urus keselamatan maklumat dengan peranan dan tanggungjawab untuk mengurus dan mengekalkan keselamatan maklumat dalam persekitaran operasi serta untuk melindungi kemudahan pemprosesan maklumat yang dicapaian, diproses, disampaikan kepada, atau diuruskan oleh pihak luar. MPS juga hendaklah memastikan pematuhan dengan PKS serta keperluan keselamatan berkanun, pengawalseliaan dan kontrak lain yang berkaitan.

b) Keselamatan Sumber Manusia
   MPS hendaklah memastikan bahawa pekerja, kontraktor dan pengguna pihak ketiga memahami tanggungjawab mereka sebelum bekerja dan bahawa mereka sedar tentang ancaman dan kebimbangan keselamatan maklumat, tanggungjawab dan liabiliti mereka serta mereka dilengkapi untuk menyokong Polisi Keselamatan Siber MPS semasa pekerjaan itu. Selepas penamatan atau pertukaran pekerjaan, MPS juga hendaklah memastikan mereka meninggalkan MPSdengan teratur.

c) Pengurusan Aset
   MPS hendaklah memastikan bahawa tanggungjawab ditetapkan untuk aset maklumat dan semua aset maklumat hendaklah diklasifikasikan dan dikendalikan berdasarkan nilainya, keperluan undang-undang, dan kritikal kepada MPS.

d) Pengurusan Maklumat
   MPS hendaklah menentukan klasifikasi maklumat perniagaan dan cara mengendalikannya untuk memastikan pengendalian maklumat yang sesuai tanpa melanggar keselamatan maklumat.

e) Pengurusan Identiti dan Capaian

MPS hendaklah memastikan bahawa capaian kepada maklumat perniagaan dan infrastruktur sokongannya adalah berdasarkan dasar kawalan capaian yang menggabungkan keperluan perniagaan dan keselamatan MPS. Pengurusan capaian pengguna hendaklah disediakan untuk memastikan bahawa hanya pekerja yang diberi kuasa dan kakitangan kontrak mempunyai capaian kepada maklumat perniagaan serta infrastruktur sokongannya.

f) Hubungan dengan Pembekal

Dasar untuk pembekal atau pembekal perkhidmatan luar hendaklah diwujudkan untuk memastikan keperluan keselamatan maklumat ditangani dan dipersetujui semasa pelaksanaan projek.

g) Pengurusan Insiden Keselamatan Maklumat

MPS hendaklah memastikan bahawa peristiwa keselamatan maklumat dan kelemahan yang berkaitan dengan sistem maklumat dilaporkan dan dikomunikasikan dengan berkesan untuk tindakan pembetulan tepat pada masanya diambil.

h) Kawalan Fizikal dan Persekitaran

MPS hendaklah menghalang capaian fizikal yang tidak dibenarkan, kerosakan, dan gangguan kepada premis dan maklumat MPS dengan menentukan kawasan selamat untuk kemudahan pemprosesan maklumat yang kritikal atau sensitif. MPS juga hendaklah memastikan semua peralatan perniagaan dilindungi daripada ancaman fizikal dan alam sekitar.

i) Kawalan Teknologi dan Operasi

MPS hendaklah mewujudkan prosedur dan tanggungjawab operasi yang sesuai untuk memastikan operasi selamat bagi kemudahan pemprosesan maklumat dan melaksanakan tahap keselamatan maklumat yang sesuai selaras dengan perjanjian penyampaian perkhidmatan pihak ketiga dan meminimumkan kegagalan sistem melalui perancangan dan penerimaan sistem. MPS hendaklah mengekalkan integriti dan ketersediaan maklumat dan kemudahan pemprosesan maklumat melalui perlindungan terhadap serangan berniat jahat, sandaran maklumat, keselamatan rangkaian, pembangunan perisian selamat, dan pemantauan aktiviti pemprosesan maklumat yang tidak dibenarkan.

j) Pengurusan Kesinambungan Perkhidmatan ICT

MPS hendaklah mewujudkan prosedur dan tanggungjawab operasi semasa berada di dalam situasi kecemasan atau ketergangguan perkhidmatan ICT. Kesinambungan perkhidmatan ICT, termasuklah keselamatan dan ketersediaan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan perkhidmatan ICT di MPS.

BAB 1
KAWALAN ORGANISASI

BAB 1 | KAWALAN ORGANISASI

1.1 POLISI UNTUK KESELAMATAN MAKLUMAT

Objektif:

Memastikan polisi keselamatan maklumat bersesuaian, berterusan dan seiring dengan hala tuju pengurusan dalam menyokong keselamatan maklumat selari dengan fungsi MPS, undang-undang dan keperluan kontrak perjanjian.

1.1.1 Pelaksanaan Polisi	Tanggungjawab
Polisi Keselamatan Siber (PKS) MPS ini akan dikuat kuasakan oleh Yang Dipertua (YDP) MPS, dan dibantu oleh Pengurusan MPS yang terdiri daripada Timbalan Yang Dipertua (TYDP) selaku Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO) dan semua Pengarah, Ketua Bahagian dan Ketua Unit.	YDP, TYDP (CDO), ICTSO, Pengarah Jabatan, Ketua Bahagian dan Ketua Unit

1.1.2 Penyebaran Polisi	Tanggungjawab
Polisi ini hendaklah dipaparkan kepada umum dan disebarkan kepada semua Warga MPS dan Pihak Ketiga. Sebarang perubahan yang telah dipersetujui oleh Pengurusan MPS / Jawatankuasa Perkhidmatan dan Teknologi (JPTM), hendaklah dimaklumkan kepada semua pengguna MPS.	ICTSO

1.1.3 Penyelenggaraan Polisi	Tanggungjawab
PKS MPS adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan PKS MPS: (a) mengenal pasti dan menentukan perubahan yang diperlukan; (b) mengemukakan cadangan untuk pertimbangan Mesyuarat Pengurusan / Mesyuarat Jawatankuasa Perkhidmatan dan Teknologi Maklumat (JPTM) / mesyuarat yang setara; (c) memaklumkan cadangan pindaan untuk perakuan oleh Mesyuarat Pengurusan / JPTM / mesyuarat yang setara; (d) memaklumkan pindaan yang telah diluluskan oleh Mesyuarat Pengurusan / JPTM / mesyuarat yang setara (e) PKS MPS ini perlu disemak semula sekurang-kurangnya tiga tahun sekali atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	ICTSO, Mesyuarat Pengurusan / Mesyuarat Jawatankuasa Perkhidmatan dan Teknologi Maklumat (JPTM) / mesyuarat yang setara

1.1.4 Pematuhan Polisi	Tanggungjawab
PKS MPS ini mestilah dipatuhi oleh semua pengguna	Pengguna

1.1.5 Pengecualian Polisi	Tanggungjawab
Permohonan pengecualian PKS dan prosedur ICT boleh dibuat dengan melengkapkan borang Permohonan Pengecualian Pematuhan PKS beserta justifikasi dan faedah yang dikaitkan dengan penafian. Permohonan pengecualian ini perlu mendapat kelulusan daripada CDO atau ICTSO. Pengecualian PKS ini adalah merujuk kepada polisi ISMS dan hanya boleh digunakan dalam situasi yang berkaitan untuk tempoh masa maksimum satu (1) tahun. Pengecualian polisi perlu dinilai semula apabila tamat tempoh satu (1) tahun. Permohonan pengecualian polisi ini perlu dimohon dengan menggunakan borang **Permohonan Pengecualian Pematuhan Polisi Keselamatan Siber MPS** seperti di **Lampiran 1**.	Semua

1.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT

Objektif:

Mewujudkan struktur, peranan dan tanggungjawab dalam pengurusan keselamatan maklumat di MPS.

1.2.1 Yang Dipertua, MPS	Tanggungjawab
Yang Dipertua MPS adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah PKS MPS; b) Memastikan semua pengguna mematuhi PKS MPS; c) Memastikan semua keperluan organisasi (sumber kewangan sumber manusia dan perlindungan keselamatan) adalah mencukupi; d) Memastikan penilaian risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam PKS MPS; dan e) Mempengerusikan Mesyuarat Pengurusan / Mesyuarat Jawatankuasa Perkhidmatan dan Teknologi Maklumat.	YDP

1.2.2 Ketua Pegawai Digital (Chief Digital Officer - CDO)	Tanggungjawab

Ketua Pegawai Digital (CDO) bagi MPS ialah Timbalan Yang Dipertua MPS.

Peranan dan tanggungjawab CDO adalah seperti berikut: CDO

a) Membantu Yang Dipertua dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber;
b) Menentukan keperluan keselamatan ICT; dan
c) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan siber MPS.

1.2.3 Pegawai Keselamatan ICT (ICTSO)	Tanggungjawab

Pegawai Keselamatan ICT (ICTSO) bagi MPS ialah Pengarah Teknologi Maklumat.

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: ICTSO

a) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini;
b) Mengurus keseluruhan program-program keselamatan ICT MPS;
c) Menguatkuasakan pelaksanaan PKS MPS;
d) Memberi penerangan dan pendedahan berkenaan PKS MPS kepada semua pengguna;
e) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS MPS;
f) Menjalankan pengurusan risiko;
g) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MPS berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
h) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
i) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
j) Melaporkan insiden keselamatan ICT kepada Pasukan Tindakbalas Insiden Keselamatan ICT Kerajaan, MPS dan ICTSO memaklumkannya kepada CDO;
k) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;
l) Merancang dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan
m) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.

1.2.4 Pentadbir SIstem ICT	Tanggungjawab
Pentadbir Sistem ICT bagi MPS ialah pegawai yang menguruskan aplikasi di MPS. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam PKS MPS; c) Memantau aktiviti capaian harian sistem aplikasi pengguna; d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e) Melaporkan sebarang perkara atau penemuan mengenai keselamatan siber kepada ICTSO; f) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan siber MPS; dan g) Mengkaji semula dan melaksanakan kawalan keselamatan siber selaras dengan keperluan MPS.	Pentadbir Sistem ICT

1.2.5 Pentadbir Bilik *Server* Utama MPS / Rangkaian	Tanggungjawab
Pentadbir Bilik *Server* Utama MPS / Rangkaian ialah pegawai yang dipertanggungjawabkan mentadbir Bilik *Server* Utama MPS dan seterusnya melaksanakan pematuhan PKS MPS. Pentadbir Bilik *Server* Utama MPS / Rangkaian mempunyai peranan dan tanggungjawab seperti berikut:- a) Menyediakan dan melaksana garis panduan, prosedur dan tatacara pentadbiran Bilik *Server* Utama MPS selaras dengan keperluan PKS MPS; b) Memastikan Bilik *Server* Utama MPS beroperasi sepanjang masa; c) Memastikan keselamatan fizikal dan persekitaran Bilik *Server* Utama MPS sentiasa dlam keadaan baik dan mengambil langkah-langkah untuk mengurangkan risiko ancaman keselamatan siber bagi melindungi perkhidmatan di Bilik *Server* Utama MPS; d) Bertanggungjawab memantau setiap perkakasan dan perisian ICT yang ditempatkan di Bilik *Server* Utama MPS di dalam keadaan yang baik; e) Memantau dan mengawal akses fizikal (keluar dan masuk) ke Bilik *Server* Utama MPS; f) Mengawal dan memantau capaian secara atas talian ke *server*-*server* dan peralatan ICT di Bilik *Server* Utama MPS seperti penyediaan Console Room, buku log dan sebagainya;	Pentadbir Bilik Server Utama MPS / Rangkaian

g) Memantau aktiviti capaian perkhidmatan di Bilik *Server* Utama MPS dan melaporkan kepada ICTSO dengan segera sekiranya berlaku sebarang insiden pelanggaran polisi keselamatan Bilik *Server* Utama MPS;
h) Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di MPS beroperasi sepanjang masa;
i) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada;

j) Memantau penggunaan rangkaian dan melaporkan kepada ICTSO dengan segera sekiranya berlaku penyalahgunaan penggunaan rangkaian; dan
k) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian MPS secara tidak sah seperti melalui peralatan modem dan dial-up tanpa kebenaran;

1.2.6 Pegawai Aset ICT — Tanggungjawab

Pegawai Aset ICT

Pegawai Aset ICT bagi MPS ialah pegawai yang menguruskan peralatan dan aksesori ICT.

Peranan dan tanggungjawab Pegawai Aset ICT adalah seperti berikut:

a) Menentukan kawalan akses pengguna terhadap aset ICT MPS;
b) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik;
c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan siber kepada ICTSO;
d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT;
e) Mengkaji semula dan melaksanakan kawalan keselamatan siber selaras dengan keperluan MPS; dan
f) Bertindak sebagai pegawai yang menguruskan aset-aset ICT Majlis.

1.2.7 Pengguna — Tanggungjawab

Pengguna

Pengguna mempunyai peranan dan tanggungjawab seperti berikut:

a) Membaca, memahami dan mematuhi PKS MPS;
b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya;
c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;
d) Melaksanakan prinsip-prinsip PKS MPS dan menjaga kerahsiaan maklumat MPS;

e) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera;
f) Menghadiri program-program kesedaran mengenai keselamatan siber;
g) Menandatangani **Surat Akuan Pematuhan PKS MPS** sebagaimana di **Lampiran 2**; dan
h) Melaksanakan langkah-langkah perlindungan seperti berikut:
   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 garis panduan keselamatan yang ditetapkan;
   vi. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
   vii. menjaga kerahsiaan maklumat-maklumat terperingkat berkaitan keselamatan ICT.

1.3 PENGASINGAN TUGAS

Objektif:

Menerangkan perbezaan tugas setiap individu dengan lebih jelas dan teratur untuk mencegah daripada berlakunya kebocoran serta kesilapan.

1. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT.

2. 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.

3. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

1.4 TANGGUNGJAWAB PENGURUSAN

Objektif:

Memastikan pihak pengurusan dan Warga MPS memahami peranan serta memenuhi tanggungjawab dalam keselamatan maklumat.

1.4.1 Tanggungjawab Pengurusan — Tanggungjawab

Perkara yang perlu dipastikan adalah seperti berikut:

a) memastikan semua Warga MPS dan pihak ketiga diberi taklimat berkaitan pematuhan ke atas PKS MPS;
b) memastikan Warga MPS dan pihak ketiga bertanggungjawab ke atas keselamatan Aset ICT berdasarkan peraturan yang ditetapkan oleh MPS; dan
c) memastikan sumber yang mencukupi untuk melaksanakan proses dan kawalan yang berkaitan keselamatan MPS.

1.4.2 Jawatankuasa Perkhidmatan dan Teknologi Maklumat (JPTM) — Tanggungjawab

JPTM MPS

Jawatankuasa Perkhidmatan dan Teknologi Maklumat (JPTM) adalah jawatankuasa yang bertanggungjawab dalam meluluskan dan berperanan sebagai penasihat dan membentangkan projek baru ICT.

Keanggotaan JPTM MPS adalah seperti berikut:

Pengerusi : YDP MPS

Ahli : (1) Timbalan Yang Dipertua (CDO)

(2) ICTSO MPS

(3) Semua Pengarah dan Ketua Bahagian

(4) Ahli Majlis

Bidang kuasa :

a) Menetapkan arah tuju dan strategi untuk pelaksanaan ICT MPS;
b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arahtuju/strategi ICT MPS;
c) Merancang dan menentukan langkah-langkah keselamatan siber;
d) Mengikuti dan memantau perkembangan program ICT MPS dan Jabatan di bawahnya, serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT;
e) Menilai dan meluluskan semua perolehan ICT MPS dan Jabatan di bawahnya berdasarkan keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan; dan

f) Menyelaras dan mengemukakan kertas cadangan perolehan ICT bagi MPS dan Jabatan di bawahnya.

1.4.3 Jawatankuasa Teknikal ICT MPS	Tanggungjawab

Jawatankuasa Teknikal ICT (JKTICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan siber dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan siber MPS. — JKICT, MPS

Keanggotaan JKICT MPS adalah seperti berikut:

Pengerusi : Timbalan Yang Dipertua

Ahli :
(1) Jabatan Perundangan
(2) Jabatan Perbendaharaan
(3) Jabatan Khidmat Pengurusan
(4) Jabatan Penilaian & Pengurusan Harta
(5) Jabatan Pengurusan Sisa Pepejal dan Kesihatan
(6) Jabatan Audit Dalam
(7) Jabatan Kontrak dan Ukur Bahan
(8) Jabatan Kejuruteraan
(9) Jabatan Korporat
(10) Jabatan yang terlibat dengan projek ICT

Urus Setia bagi JKICT MPS ialah Jabatan Teknologi Maklumat.

Bidang kuasa:

a) Memperakukan dokumen PKS MPS;
b) Sebagai penasihat bagi projek-projek ICT yang akan dilaksanakan;
c) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan projek ICT;
d) Menerima laporan dan membincangkan hal-hal berkaitan projek ICT semasa; dan
e) Membuat keputusan mengenai tindakan yang perlu diambil berkenaan projek ICT.

1.4.4 Pasukan Tindak Balas Insiden Keselamatan ICT MPS	Tanggungjawab

Struktur organisasi CERT terdiri daripada Pasukan Pemulihan Bencana ICT (DRP-ICT) MPS dan ahli-ahli yang dilantik. — Pasukan CERT MPS

Pengarah CERT disandang oleh YDP manakala Koordinator CERT disandang oleh ICTSO.

Peranan dan tanggungjawab CERT adalah seperti berikut:

a) Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden;
b) Merekod dan menjalankan siasatan awal insiden yang diterima;
c) Menangani tindak balas (response) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;
d) Menasihatkan Jabatan dan Bahagian supaya mengambil tindakan pemulihan dan pengukuhan;
e) Memaklumkan sebarang ancaman dan insiden keselamatan ICT kepada Jabatan dan Bahagian; dan
f) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baharu dapat dielakkan.

1.5 HUBUNGAN DENGAN PIHAK BERKUASA

Objektif:

Menyediakan senarai perhubungan pihak berkuasa berkaitan sekiranya berlaku kejadian yang menjejaskan keselamatan maklumat dan perkhidmatan ICT.

Tanggungjawab Pengurusan	Tanggungjawab
Perkara yang perlu diambil kira berkaitan hubungan dengan pihak berkuasa adalah tidak terhad seperti berikut: a) *Malaysian Emergency Response System* 999 (Polis, Bomba, Agensi Pertahanan Awam Malaysia); b) *National Disaster Management Agency* (NADMA); c) *National Cyber Security Agency* (NACSA); d) *CyberSecurity* Malaysia; dan e) CSIRT Selangor	ICTSO

1.6 HUBUNGAN DENGAN PIHAK BERKEPENTINGAN

Objektif:

Memastikan maklumat yang diperlukan oleh pihak berkepentingan dengan MPS disediakan.

Tanggungjawab Pihak Berkepentingan	Tanggungjawab
Pihak berkepentingan terdiri daripada pembekal, perunding, pemegang taruh, pelawat dan pihak-pihak lain yang terlibat dalam pengurusan, penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan. Perkara yang perlu dipatuhi: a) mengenal pasti risiko ke atas keselamatan maklumat dan memastikan pelaksanaan kawalan yang sesuai ke atas maklumat tersebut; b) memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga; c) akses kepada aset ICT MPS perlu berlandaskan perjanjian dan peraturan yang telah ditetapkan. Perjanjian yang dimeterai perlu mematuhi perkara-perkara berikut: i. Akta Keselamatan Siber 2024 (Akta 854); ii. Perakuan Akta Rahsia Rasmi 1972; iii. Hak Harta Intelek; iv. Tapisan Keselamatan; dan v. PKS MPS. d) melaksanakan keselamatan dan menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber MPS seperti di LAMPIRAN 2, serta *Non-Disclosure Aggreement* bagi perakuan untuk tidak membocorkan sebarang maklumat rasmi yang diperoleh dari MPS seperti di LAMPIRAN 3; dan e) pihak berkepentingan kategori pelawat sahaja dikecualikan daripada mematuhi peraturan a hingga c seperti di atas.	

1.7 RISIKAN ANCAMAN

Objektif:

Memastikan maklumat yang diperlukan oleh pihak berkepentingan dengan MPS disediakan.

Pengurusan Risikan Ancaman	Tanggungjawab
Operasi rangkaian dan infrastruktur MPS dipantau menggunakan perkakasan dan perisian tertentu. Rekod aktiviti dan log dikumpulkan dan dianalisis bagi mengenal pasti ancaman serangan siber bagi membolehkan tindakan mitigasi diambil secara tepat dan berkesan.	ICTSO, Pentadbir Bilik *Server* Utama MPS / Rangkaian

Analisis yang dikenal pasti dikategorikan kepada tiga jenis maklumat ancaman iaitu kaedah serangan, metodologi serangan dan perincian maklumat penyerang.

1.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK

Objektif:

Memastikan keselamatan maklumat diambil kira dalam pengurusan projek.

Keselamatan Maklumat Dalam Pengurusan Projek	Tanggungjawab
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) objektif keselamatan maklumat hendaklah diambil kira dan dilaksanakan dalam pengurusan projek merangkumi semua fasa pelaksanaan projek; b) pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan; dan c) penyediaan spesifikasi perolehan hendaklah memasukkan keperluan ciri-ciri keselamatan.	ICTSO, Pentadbir SIstem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

1.9 MAKLUMAT INVENTORI DAN ASET

Objektif:

Memastikan pengurusan maklumat dan aset dikenal pasti, dikelaskan, direkodkan, diselenggarakan dan penempatan ditetapkan untuk perlindungan keselamatan.

1.9.1 Inventori dan Penempatan Maklumat Serta Aset ICT	Tanggungjawab
Semua maklumat dan Aset ICT di MPS hendaklah diuruskan mengikut peraturan dan tatacara yang berkuat kuasa seperti berikut: a) memastikan maklumat dan Aset ICT yang dikenal pasti direkodkan serta dikemas kini mengikut peraturan semasa yang berkuat kuasa. b) memastikan pengemaskinian maklumat berkaitan instalasi dan perubahan aset; c) maklumat pemilik Aset ICT, lokasi dan status Aset ICT hendaklah dikemas kini dari semasa ke semasa; d) setiap maklumat dan Aset ICT perlu diklasifikasikan mengikut kategori kerahsiaan;	Pegawai Aset, Pembantu Pegawai Aset, Kerani Aset

e) memastikan Aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja. Penukaran pemilik hendaklah dilaksanakan sekiranya terdapat perubahan; dan
f) pemeriksaan Aset ICT hendaklah dilaksanakan sekurang-kurangnya satu kali setahun.

1.9.2 Tanggungjawab Pemilik	Tanggungjawab
Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MPS. Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi: a) memastikan semua aset ICT dikenal pasti, dikelas, didokumen, diselenggara dan dilupus. Maklumat aset ICT direkod dan dikemas kini dalam Sistem e-Aset mengikut peraturan semasa yang sedang berkuat kuasa; b) memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c) memastikan semua pemilik mengesahkan penempatan aset ICT yang ditempatkan di MPS; d) memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan; e) setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalan atau milikan; f) penggunaan aset ICT MPS mestilah untuk tujuan tugas rasmi sahaja; dan g) aset ICT yang perlu dibawa keluar atas urusan rasmi perlu mendapat kelulusan.	Pegawai Aset, Warga MPS

1.10 PENGGUNAAN MAKLUMAT DAN ASET ICT YANG BOLEH DITERIMA PENGGUNAAN MAKLUMAT DAN ASET YANG DITERIMA

Objektif:

Memastikan setiap maklumat dan Aset ICT yang berkaitan dilindungi, digunakan dan dikendalikan dengan sewajarnya.

1.10.1 Penggunaan Maklumat dan Aset ICT	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) warga MPS dan pihak ketiga yang mempunyai capaian ke atas maklumat dan Aset ICT hendaklah bertanggungjawab terhadap keperluan perlindungan serta	Warga MPS, Pihak Ketiga, Pentadbir Sistem ICT, Pegawai Aset ICT

pengendalian keselamatan maklumat;

b) menyediakan prosedur pengurusan pengendalian maklumat yang merangkumi penggunaan, kebenaran, perkongsian dan pemantauan maklumat;
c) memastikan kawalan capaian yang dibenarkan mengikut tahap klasifikasi pengelasan maklumat;
d) menyelenggarakan rekod berkaitan senarai pengguna yang dibenarkan untuk capaian maklumat;
e) memastikan kawalan ke atas salinan maklumat, storan maklumat dan perlu melaksanakan pelabelan media storan dengan jelas; dan
f) memperoleh kebenaran untuk melaksanakan pelupusan maklumat dan aset berdasarkan tatacara pelupusan semasa yang sedang berkuat kuasa.

1.10.2 Pengendalian Maklumat dan Aset ICT	Tanggungjawab
Pengendalian Aset ICT hendaklah dilaksanakan mengikut Tatacara Pengurusan Aset Alih Kerajaan.	Warga MPS, Pegawai Aset ICT

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut:

a) aktiviti yang melibatkan pemprosesan maklumat seperti penyalinan, penyimpanan, penghantaran, perkongsian dan pemusnahan maklumat mestilah mengikut peraturan yang berkuat kuasa;
b) menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
c) memeriksa maklumat dan menentukan maklumat tepat dan lengkap dari semasa ke semasa;
d) menentukan maklumat sedia untuk digunakan;
e) menjaga kerahsiaan kata laluan; dan
f) mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

1.11 PEMULANGAN ASET ICT

Objektif:

Memastikan proses pemulangan aset ICT dilaksanakan apabila berlaku perubahan dan penamatan perkhidmatan, kontrak atau perjanjian.

1.11.1 Pemulangan Aset ICT	Tanggungjawab
Memastikan semua Aset ICT dikembalikan kepada MPS mengikut peraturan dan terma perkhidmatan yang ditetapkan bagi pegawai yang:	Warga MPS, Pegawai Aset ICT

a) bertukar keluar;
b) bersara;
c) meninggal dunia; dan
d) ditamatkan perkhidmatan; dan diarahkan oleh Ketua Jabatan.

1.11.2 Peminjaman Aset ICT	Tanggungjawab
Tatacara peminjaman aset adalah seperti yang berikut: a) mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh MPS bagi membawa keluar aset ICT bagi tujuan yang dibenarkan; b) melindungi dan mengawal aset ICT sepanjang masa; c) merekodkan aktiviti peminjaman dan pemulangan aset ICT; dan d) menyemak aset ICT ketika peminjaman dan pemulangan dilakukan.	Warga MPS, Pegawai Aset ICT

1.12 KLASIFIKASI MAKLUMAT

Objektif:

Memastikan pengenalpastian dan pemahaman tentang keperluan perlindungan maklumat mengikut kepentingan di MPS.

1.12.1 Pengelasan Maklumat	Tanggungjawab
Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan (Semakan dan Pindaan 2017) seperti yang berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; d) Terhad; e) Dokumen Rasmi; dan f) Data Terbuka.	Pegawai Pengelas Maklumat

1.13 PELABELAN MAKLUMAT

Objektif:

Memastikan pelabelan maklumat dilaksanakan bagi memudahkan pengurusan penyimpanan maklumat.

1.13.1 Pelabelan Maklumat	Tanggungjawab
Semua maklumat dilabelkan mengikut klasifikasi maklumat sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan (Semakan dan Pindaan 2017).	Pegawai Pengelas Maklumat

1.14 PEMINDAHAN MAKLUMAT

Objektif:

Memastikan keselamatan semasa pemindahan maklumat kepada pihak ketiga atau sebaliknya. Pemindahan maklumat secara dalaman atau luaran hendaklah mengikut syarat atau perjanjian yang ditetapkan.

1.14.1 Pemindahan Maklumat	Tanggungjawab
Penghantaran atau pemindahan maklumat yang mengandungi maklumat terperingkat boleh dilaksanakan melalui medium elektronik atau media storan fizikal. Penghantaran fail bersaiz besar boleh menggunakan kaedah muat turun fail dengan memaklumkan lokasi Universal Resource Locator (URL) atau kaedah pemampatan untuk mengurangkan saiz fail dengan memastikan ciri-ciri keselamatan dilaksanakan. a) kawalan ke atas pemindahan maklumat daripada dicerobohi, diubah, disalin, dimusnahkan dan sebagainya; b) pemindahan maklumat hendaklah direkodkan bagi kawalan pengesanan; c) menggunakan kaedah pengesahan yang selamat sekiranya pemindahan maklumat menggunakan rangkaian awam; d) memastikan maklumat elektronik yang hendak dipindahkan perlu dilindungi menggunakan enkripsi Secure Socket Layer (SSL) atau Application Programming Interface (API). e) pemindahan maklumat melalui media storan seperti cloud storage, hard disk, USB flash drive dan media storan lain perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan ketersediaan untuk digunakan; dan f) penghantaran dokumen terperingkat mestilah menggunakan medium penghantaran rasmi jabatan.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pentadbir E-mel, Warga MPS

1.15 KAWALAN CAPAIAN

Objektif:

Memastikan akses bagi menghalang capaian yang tidak dibenarkan kepada maklumat dan lain-lain yang berkaitan aset.

1.15.1 Keperluan Kawalan Capaian	Tanggungjawab
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong kawalan capaian pengguna sedia ada.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

1.15.2 Capaian Pengguna	Tanggungjawab
Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut: a) akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b) akaun ID pengguna hendaklah mencerminkan identiti pengguna; c) pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika kaedah penggunaannya melanggar peraturan; d) penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan e) pemilik akaun dan capaian pengguna adalah tertakluk kepada peraturan jabatan dan tindakan pengemaskinian atau pembatalan hendaklah diambil atas sebab berikut: i. pengguna bercuti panjang dalam tempoh waktu melebihi enam bulan; ii. bertukar bidang tugas kerja; iii. bertukar ke agensi lain; iv. bersara; atau ditamatkan perkhidmatan.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

1.15.3 Hak Capaian	Tanggungjawab
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat, atas prinsip perlu mengetahui (need-to-know-basis). Keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pegawai dan kakitangan yang dibenarkan sahaja.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

1.15.4 Capaian Sistem Pengoperasian	Tanggungjawab
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian terhadap sistem komputer. Kemudahan ini juga perlu bagi: a) mengenal pasti identity / terminal / lokasi bagi setiap pengguna yang dibenarkan; b) merekodkan capaian yang berjaya dan gagal; c) membolehkan pengesahan kata laluan dilaksanakan berdasarkan kriteria kata laluan yang kukuh; dan d) mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf super user; Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c) Menghadkan dan mengawal penggunaan program; dan d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi bagi tempoh 15 minit	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

1.15.5 Capaian Aplikasi dan Maklumat	Tanggungjawab
Bertujuan melindungi sistem maklumat dan aplikasi sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di MPS adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah- langkah berikut perlu dipatuhi: a) pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b) setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti- aktiviti yang tidak diingini; c) menyediakan paparan dasar privasi / notis penafian kepada pengguna ketika menggunakan aplikasi bagi melindungi maklumat daripada sebarang bentuk penyalahgunaan; d) memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e) maklumat tarikh login terakhir hendaklah direkodkan; digalakkan *session timeout* dilaksanakan.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

1.15.6 Capaian Rangkaian	Tanggungjawab
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) mewujudkan segmen rangkaian yang bersesuaian bagi membezakan di antara rangkaian MPS dan rangkaian awam; b) mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dengan peralatan yang menepati kesesuaian penggunaannya; c) memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; d) capaian pengguna jarak jauh (*remote user*) perlulah dikawal dan dipantau; e) capaian fizikal dan logikal ke atas peralatan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal; dan f) semua rangkaian yang dikongsi (*shared networks*), terutama yang keluar daripada rangkaian MPS, polisi perlu diwujudkan untuk mengawal capai oleh pengguna.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

1.15.7 Capaian Jarak Jauh	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (encryption); b) lokasi bagi akses ke sistem ICT MPS hendaklah dipastikan selamat; c) penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pentadbir Bilik *Server* Utama MPS / Rangkaian. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini; dan d) penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pentadbir Bilik *Server* Utama MPS / Rangkaian. Capaian jarak jauh hendaklah menggunakan kemudahan yang disediakan oleh jabatan.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

1.15.8 Capaian Internet	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) penggunaan Internet di MPS hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian dan Keselamatan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kawalan ini akan dapat melindungi daripada sebarang bentuk ancaman ke atas rangkaian MPS; b) penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; c) polisi Content Filtering mestilah digunakan dan dipantau bagi mengawal akses Internet. Pengguna boleh memohon pengecualian mengikut fungsi kerja untuk pertimbangan; dan	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

d) penggunaan teknologi packet shaper adalah mengikut keperluan bagi menguruskan penggunaan bandwidth yang maksimum dan lebih berkesan.

1.16 PENGURUSAN IDENTITI

Objektif:

Memastikan ID pengguna adalah unik dan sesuai ke atas entiti untuk mengakses sistem dan aset MPS lain yang berkaitan.

1.16.1 Proses Pengurusan Identiti

Tanggungjawab

ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Pentadbir E-mel, Warga MPS

Proses pengurusan identiti perlu memastikan perkara berikut dipatuhi:

a) memastikan ID pengguna hendaklah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat;
b) memastikan identiti yang diberikan kepada lebih dari seorang individu (identiti bersama) hanya dibenarkan jika ada keperluan dan tertakluk kepada kelulusan serta direkodkan;
c) memastikan perkakasan yang memerlukan ID pengguna hendaklah mendapatkan kelulusan serta pengawasan berterusan;
d) merekodkan semua penggunaan dan pengurusan identiti pengguna;
e) pewujudan ID pengguna hendaklah mendapat sokongan oleh Penyelia / Ketua Kerani / Ketua Unit / Ketua Bahagian /Pegawai / Pengarah.
f) membatalkan, menamatkan dan menukar peranan akaun pengguna berdasarkan pemakluman oleh Ketua Bahagian/ Cawangan /Unit/ PTB atas sebab berikut:
    i. bertukar bidang tugas kerja;
    ii. bertukar ke agensi lain;
    iii. bersara;
    iv. ditamatkan perkhidmatan; dan
    v. pengguna bercuti panjang dalam tempoh waktu melebihi enam (6) bulan.
g) proses semakan akses pengguna perlu dilaksanakan untuk mengkaji semula kebenaran dan pembatalan capaian pengguna ke atas semua aplikasi dan perkhidmatan; dan
h) dilarang menggunakan nama atau menyamar sebagai individu lain dalam mana-mana perkhidmatan dalam talian.

1.16.2 Prosedur Pendaftaran atau Penamatan Akses

Tanggungjawab

Pentadbir Sistem ICT

Prosedur bagi penyediaan atau pembatalan akses perlu memastikan perkara berikut:

a) memastikan identiti yang diwujudkan memenuhi keperluan tugasan berkaitan;

b) mengesahkan identiti pengguna yang memohon sebelum pewujudan ID pengguna;
c) mewujudkan ID pengguna;
d) mengkonfigurasi dan mengaktifkan ID pengguna; dan
e) menyediakan atau membatalkan hak akses berdasarkan kelulusan atau pemakluman.

1.17 PENGESAHAN MAKLUMAT

Objektif:

Memastikan pengesahan entiti yang betul untuk mengelakkan kegagalan capaian maklumat.

1.17.1 Proses Pengesahan Maklumat	Tanggungjawab
Proses penyediaan dan pengurusan pengesahan maklumat perlu berdasarkan perkara berikut: a) penjanaan kata laluan peribadi sementara semasa proses pendaftaran yang unik untuk setiap individu. Pengguna diwajibkan menukar kata laluan apabila log masuk kali pertama; b) kata laluan default bagi Pihak Ketiga perlu ditukar serta- merta selepas selesai pemasangan sistem, perkakasan atau perisian; dan c) menghantar kata laluan kepada pengguna dengan cara yang selamat.	ICTSO, Pentadbir Sistem ICT, Pegawai Aset ICT, Pentadbir E-mel

1.17.2 Tanggungjawab Pengguna	Tanggungjawab
Setiap individu yang mempunyai akses hendaklah memastikan perkara berikut: a) merahsiakan kata laluan dan tidak dikongsi dengan sesiapa melainkan ID pengguna bersama yang diberi kebenaran sahaja; b) kata laluan yang telah terdedah kepada pihak tidak bertanggungjawab perlu ditukar serta-merta; c) kata laluan yang digunakan mestilah kukuh mengikut cadangan amalan terbaik seperti: i. kata laluan tidak boleh diteka atau diperoleh dengan mudah berdasarkan maklumat berkaitan individu (seperti nama, nombor telefon dan tarikh lahir); ii. kata laluan tidak berdasarkan perkataan kamus (dictionary words) atau gabungannya; iii. menggunakan kata laluan yang mudah diingat dan berkualiti iaitu sekurang-kurangnya minimum lapan (8) aksara, dan mesti terdiri daripada kombinasi huruf dan nombor, atau simbol khas.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Pentadbir E-mel, Warga MPS

iv. kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun.

d) menggunakan pengurusan identiti secara berpusat yang selamat seperti *Active Directory* atau tidak menggunakan kata laluan yang sama untuk perkhidmatan dan sistem yang berlainan.

1.17.3 Sistem Pengurusan Kata Laluan	Tanggungjawab
Sistem pengurusan kata laluan hendaklah mematuhi perkara berikut: a) membenarkan pengguna memilih dan menukar kata laluan mereka sendiri; b) menguatkuasakan kata laluan yang kukuh mengikut cadangan amalan baik; c) mewajibkan pengguna menukar kata laluan mereka pada pertama kali log masuk; d) mewajibkan perubahan kata laluan sekiranya berlaku insiden keselamatan, penamatan atau kata laluan yang berkongsi identiti; e) menghalang penggunaan kata laluan yang mempunyai nama pengguna atau gabungan kata laluan daripada sistem yang pernah terdedah atau digodam; f) tidak memaparkan kata laluan pada skrin apabila dimasukkan; g) menyimpan dan menghantar kata laluan dalam bentuk yang dilindungi.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Pentadbir E-mel, Warga MPS

1.18 HAK AKSES

Objektif:

Memastikan hak akses kepada maklumat dan aset lain dibenarkan mengikut keperluan.

1.18.1 Pendaftaran dan Pembatalan Hak Akses	Tanggungjawab
Proses pendaftaran atau pembatalan hak akses fizikal dan logikal yang diberikan adalah seperti yang berikut: a) mendapatkan kebenaran daripada pemilik maklumat dan aset lain yang berkaitan untuk digunakan; b) mengambil kira polisi atau peraturan khas berkaitan hak akses; c) memastikan pengasingan peranan hak akses untuk mengelakkan percanggahan; d) memastikan hak akses dihentikan apabila pengguna tidak perlu mengakses maklumat; e) memberi hak akses sementara untuk kakitangan kontrak atau kakitangan yang memerlukan akses sementara; f) mengesahkan tahap akses yang diberikan adalah mengikut had capaian dan selari dengan keperluan keselamatan maklumat lain;	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Pentadbir E-mel, Warga MPS

g) memastikan bahawa hak akses diaktifkan selepas prosedur pengesahan diluluskan;
h) menyelenggarakan rekod hak akses secara berpusat;
i) melaksanakan perubahan hak akses pengguna yang telah bertukar peranan atau bertukar keluar;
j) menamatkan atau mengemas kini hak akses fizikal atau logikal; dan
k) menyelenggarakan rekod perubahan hak akses fizikal dan logikal pengguna.

1.18.2 Semakan Hak Akses	Tanggungjawab
Semakan berkala terhadap hak akses perlu dilaksanakan seperti perkara berikut: a) selepas berlaku perubahan dalam MPS seperti pertukaran kerja, kenaikan pangkat, penurunan pangkat atau penamatan; b) pengesahan hak akses (privileged access rights) c) selepas diluluskan; dan d) membuat semakan hak akses pengguna secara berkala atau sekurang-kurangnya satu kali setahun atau mengikut keperluan	Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Pentadbir E-mel, Warga MPS

1.18.3 Pertimbangan Sebelum Pertukaran atau Penamatan Pekerjaan	Tanggungjawab
Hak akses pengguna kepada maklumat dan aset lain yang berkaitan perlu disemak, diselaraskan atau dinyahaktifkan sebelum sebarang perubahan atau penamatan berdasarkan penilaian faktor risiko seperti yang berikut: a) pengguna atau pengurusan mengemukakan sebarang permohonan penamatan dan perubahan; b) tanggungjawab semasa pengguna; dan c) nilai aset yang boleh dicapai.	Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

1.19 KESELAMATAN MAKLUMAT DENGAN PIHAK KETIGA

Objektif:

Memastikan semua Pihak Ketiga adalah tertakluk kepada peraturan yang berkuat kuasa.

1.19.1 Keselamatan Maklumat ke Atas Pihak Ketiga	Tanggungjawab
Keselamatan maklumat ke atas Pihak Ketiga hendaklah mematuhi perkara seperti berikut: a) mengenal pasti dan merekodkan Pihak Ketiga yang terlibat dengan aspek kerahsiaan, integriti dan ketersediaan maklumat MPS;	Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

b) mewujudkan kaedah penilaian dan pemilihan Pihak Ketiga berdasarkan klasifikasi maklumat, produk dan perkhidmatan;
c) menilai dan memilih produk atau perkhidmatan Pihak Ketiga yang mempunyai kawalan keselamatan maklumat serta melaksanakan semakan berkala bagi memastikan integriti dan keselamatan maklumat terjamin;
d) mengenal pasti maklumat MPS, perkhidmatan ICT dan infrastruktur fizikal yang boleh diakses, dipantau, dikawal atau digunakan oleh Pihak Ketiga;
e) mengenal pasti jenis komponen dan perkhidmatan infrastruktur ICT yang disediakan oleh Pihak Ketiga yang boleh menjejaskan kerahsiaan, integriti dan ketersediaan maklumat MPS;
f) menilai dan mengurus risiko keselamatan maklumat yang berkaitan dengan:
    i. penggunaan maklumat dan aset Pihak Ketiga;
    ii. kerosakan (malfunction) atau kelemahan produk (termasuk komponen perisian dan subkomponen); atau
    iii. perkhidmatan yang disediakan oleh Pihak Ketiga;
g) memantau pematuhan dan keperluan keselamatan maklumat yang ditetapkan kepada semua Pihak Ketiga;
h) mencegah ketidakpatuhan Pihak Ketiga, sama ada dikesan melalui pemantauan atau sumber lain;
i) pengurusan insiden berkaitan produk atau perkhidmatan di bawah tanggungjawab MPS dan Pihak Ketiga;
j) keupayaan tindakan pemulihan dan pelan kontingensi (contingency plan) untuk memastikan ketersediaan maklumat;
k) program kesedaran dan latihan kepada kakitangan MPS yang melibatkan dengan Pihak Ketiga termasuk mempunyai akses kepada maklumat;
l) memastikan keselamatan maklumat sentiasa terjaga sepanjang tempoh pemindahan maklumat atau aset lain yang berkaitan;
m) memastikan keselamatan maklumat semasa penamatan perkhidmatan Pihak Ketiga merangkumi perkara berikut:
    i. pembatalan hak akses;
    ii. pengendalian maklumat;
    iii. menentukan pemilikan harta intelek;
    iv. pemindahan maklumat sekiranya berlaku pertukaran Pihak Ketiga;
    v. pengurusan rekod;
    vi. pemulangan aset;
    vii. pelupusan maklumat dan aset lain berkaitan secara selamat; dan
    viii. keperluan kerahsiaan yang berterusan.
n) tahap keselamatan kakitangan dan keselamatan fizikal yang perlu dipatuhi Pihak Ketiga dengan mematuhi keperluan berikut:
    i. Polisi Keselamatan Siber (PKS) MPS;
    ii. Akta Rahsia Rasmi 1972; dan
o) tapisan keselamatan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO).

1.20 KESELAMATAN MAKLUMAT DALAM PERJANJIAN PIHAK KETIGA

Objektif:

Memastikan keselamatan maklumat dengan Pihak Ketiga melalui perjanjian yang telah dipersetujui.

1.20.1 Kawalan Keselamatan Maklumat Melalui Perjanjian dengan Pihak Ketiga	Tanggungjawab
Perjanjian dengan Pihak Ketiga perlu diwujudkan untuk memastikan pemahaman yang jelas antara MPS dan Pihak Ketiga mengenai tanggungjawab kedua-dua pihak. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) keterangan serta kaedah maklumat yang boleh diakses; b) pengelasan klasifikasi maklumat berdasarkan kategori rekod rasmi Kerajaan; c) keperluan undang-undang, peraturan dan kontrak, termasuk perlindungan data, pengendalian maklumat pengenalan peribadi, hak harta intelek dan hak cipta; d) kewajipan mematuhi kontrak perjanjian yang dipersetujui termasuk mematuhi keperluan keselamatan yang telah ditetapkan oleh MPS; e) peraturan penggunaan maklumat dan aset lain yang berkaitan; f) prosedur atau syarat kebenaran penggunaan, penamatan dan penggunaan maklumat MPS serta aset lain yang berkaitan dengan kakitangan Pihak Ketiga; g) g) keperluan keselamatan maklumat bagi infrastruktur ICT Pihak Ketiga yang mempunyai akses ke atas maklumat MPS; h) ganti rugi dan langkah pemulihan bagi kegagalan pematuhan kontrak oleh Pihak Ketiga; i) keperluan dan prosedur pengurusan insiden keselamatan; j) keperluan latihan dan program kesedaran untuk topik khusus keselamatan maklumat; k) klausa yang berkaitan penglibatan subkontrak termasuk kawalan perlu dimasukkan dalam perjanjian; l) maklumat pegawai perhubungan bagi pelaporan isu keselamatan maklumat; m) pelaksanaan tapisan keselamatan kakitangan Pihak Ketiga mengikut undang-undang yang berkuat kuasa; n) laporan jaminan pengesahan keselamatan maklumat dan pembuktian oleh Pihak Ketiga; o) hak untuk mengaudit Pihak Ketiga bagi proses dan kawalan yang terkandung dalam kontrak perjanjian; p) obligasi Pihak Ketiga menyediakan laporan secara berkala berkaitan keberkesanan kawalan dan tindakan pembetulan terhadap isu berbangkit dalam masa yang ditetapkan; q) penyelesaian ketidakpatuhan dan proses penyelesaian konflik; r) menyediakan sandaran (*backup*) berdasarkan keperluan MPS dari segi kekerapan, jenis dan lokasi penyimpanan; s) memastikan ketersediaan tapak alternatif pemulihan bencana sekiranya tapak utama gagal berfungsi; t) menyediakan proses pengurusan perubahan;	Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pihak Ketiga

u) kawalan keselamatan fizikal yang selari dengan tahap klasifikasi maklumat;
v) kawalan pemindahan terhadap maklumat fizikal atau logikal;
w) klausa penamatan selepas perjanjian merangkumi pengurusan rekod, pemulangan aset, pelupusan maklumat dan aset lain yang berkaitan secara selamat berdasarkan pematuhan kerahsiaan semasa;
x) maklumat yang disimpan oleh Pihak Ketiga hendaklah dihapus dengan selamat jika tidak lagi diperlukan; dan
y) memastikan penyerahan dokumen dilaksanakan kepada MPS atau pihak lain sebelum kontrak tamat.

1.21 PENGURUSAN KESELAMATAN MAKLUMAT DALAM RANTAIAN MAKLUMAT DAN KOMUNIKASI ICT

Objektif:

Memastikan persetujuan kawalan keselamatan bersama Pihak Ketiga dimeterai.

1.21.1 Kawalan Rantaian Bekalan Maklumat dan Komunikasi	Tanggungjawab
Perjanjian dengan Pihak Ketiga hendaklah mengambil kira keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan rantaian bekalan maklumat dan komunikasi. Perkara yang perlu diambil kira adalah seperti yang berikut: a) menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b) Pihak Ketiga hendaklah menghebahkan keperluan keselamatan maklumat kepada subkontraktor bagi perkhidmatan; c) melaksanakan satu proses/ kaedah pemantauan yang boleh mengesahkan Pihak Ketiga produk dan perkhidmatan mematuhi keperluan keselamatan maklumat MPS; d) memastikan jaminan daripada Pihak Ketiga bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik; e) memastikan komponen produk yang dibekalkan adalah tulen dan tidak diubah daripada spesifikasi asal atau mengikut keperluan MPS; f) memastikan bahawa produk ICT memenuhi standard keselamatan yang ditetapkan atau melalui proses pensijilan rasmi atau amalan terbaik; g) menentukan kaedah-kaedah bagi perkongsian maklumat mengenai rantaian bekalan (supply chain) antara MPS dan Pihak Ketiga; dan h) memastikan pengurusan kitaran hayat dan ketersediaan komponen ICT yang tidak lagi tersedia disebabkan Pihak Ketiga tidak lagi beroperasi atau Pihak Ketiga tidak lagi menyediakan komponen ini disebabkan kemajuan teknologi. Ini bagi mengurangkan impak risiko keselamatan ke atas MPS.	Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pihak Ketiga

1.22 PEMANTAUAN, SEMAKAN DAN PENGURUSAN PERUBAHAN PERKHIDMATAN PIHAK KETIGA

Objektif:

Memastikan pemantauan, penilaian dan pengurusan perubahan dilaksanakan ke atas Pihak Ketiga.

1.22.1 Pemantauan dan Penilaian Perkhidmatan Pihak Ketiga	Tanggungjawab
Pemantauan, kaji semula dan penilaian perkhidmatan Pihak Ketiga adalah seperti yang berikut: a) memastikan tahap perjanjian perkhidmatan Pihak Ketiga selaras dengan kontrak perjanjian; b) laporan perkhidmatan yang dihasilkan oleh Pihak Ketiga hendaklah dipantau dan status kemajuan dikemukakan kepada MPS; c) memaklumkan mengenai insiden keselamatan kepada Pihak Ketiga dan mengkaji maklumat seperti yang dikehendaki dalam perjanjian; d) mengambil tindakan terhadap sebarang insiden keselamatan maklumat yang dikenal pasti; e) menguruskan kelemahan keselamatan maklumat yang dikenal pasti; dan f) Pihak Ketiga yang didapati tidak memenuhi keperluan kontrak perjanjian boleh dikenakan tindakan bersesuaian seperti penalti.	Pentadbir Sistem ICT, Pemilik Projek

1.22.2 Pengurusan Perubahan Perkhidmatan Pihak Ketiga	Tanggungjawab
Setiap perubahan perkhidmatan Pihak Ketiga hendaklah dilaksanakan secara teratur dan mengikut Standard Operating Procedure (SOP) yang ditetapkan. Perkara yang perlu diambil kira adalah seperti yang berikut: a) memastikan perubahan dalam perkhidmatan Pihak Ketiga dipersetujui bersama dan menguntungkan pihak kerajaan; b) memastikan perubahan dalam perjanjian dengan Pihak Ketiga mengambil kira maklumat kritikal MPS, sistem serta proses yang terlibat dan kajian risiko; c) pemantauan dan persetujuan ke atas perubahan perkhidmatan Pihak Ketiga yang merangkumi perkara berikut: i. peningkatan kepada perkhidmatan/ produk sedia ada ii. termasuk rangkaian, perisian, versi dan alatan pembangunan; iii. pembangunan sebarang aplikasi dan sistem baharu; iv. pengubahsuaian atau kemas kini polisi dan prosedur Pihak Ketiga; v. kaedah kawalan baharu atau yang dikemas kini bagi menyelesaikan insiden keselamatan maklumat dan meningkatkan keselamatan maklumat; dan vi. perubahan lokasi perkakasan dan/ atau perkhidmatan.	Pentadbir Sistem ICT

1.23 KESELAMATAN MAKLUMAT BAGI PERKHIDMATAN PENGKOMPUTERAN AWAN

Objektif:

Memastikan pengurusan keselamatan maklumat bagi pengkomputeran awan.

1.23.1 Keselamatan Maklumat untuk Perkhidmatan Pengkomputeran Awan	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mengenal pasti klasifikasi maklumat atau data dalam penggunaan perkhidmatan pengkomputeran awan; b) mengenal pasti ciri-ciri asas dan model perkhidmatan pengkomputeran awan yang hendak digunakan; c) menetapkan tugas dan tanggungjawab ke atas pengurusan perkhidmatan awan; d) menentukan tanggungjawab kawalan keselamatan perkhidmatan awan di antara penyedia dan pengguna perkhidmatan awan; e) memastikan kemampuan dan jaminan kawalan keselamatan maklumat yang dilaksanakan oleh penyedia perkhidmatan awan; f) struktur tadbir urus hendaklah dikenal pasti berdasarkan peranan dan tanggungjawab untuk merancang, mengurus dan mengawal polisi serta fungsi yang berkaitan dengan keselamatan maklumat dalam pengurusan pengkomputeran awan; g) pematuhan pengurusan maklumat rahsia rasmi dalam persekitaran ICT menjadi prasyarat (prerequisite) terhadap sebarang cadangan penggunaan perkhidmatan pengkomputeran awan; h) memastikan pengurusan kontrak dan terma keselamatan dalam penggunaan perkhidmatan pengkomputeran awan; i) memastikan perlindungan migrasi data ke pengkomputeran awan, perlindungan data semasa penghantaran dan perlindungan data dalam simpanan logikal atau fizikal oleh pihak penyedia perkhidmatan; j) memantau, menyemak dan menilai keselamatan maklumat dalam perkhidmatan pengkomputeran awan; k) memastikan pengurusan insiden oleh penyedia perkhidmatan pengkomputeran awan; l) memastikan penyedia perkhidmatan mewujudkan atau mempunyai pelan Pengurusan Kesinambungan Perkhidmatan (PKP); dan m) memastikan penamatan perkhidmatan pengkomputeran awan dilaksanakan mengikut peraturan berkuat kuasa.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Pentadbir E-mel, Warga MPS

1.23.2 Pengurusan Kontrak Perkhidmatan Awan	Tanggungjawab
Perjanjian dengan penyedia perkhidmatan awan perlu mengandungi perkara berikut: a) menyediakan cadangan penggunaan berdasarkan piawaian yang bersesuaian;	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

b) menguruskan kawalan akses ke perkhidmatan pengkomputeran awan berdasarkan keperluan MPS;
c) melaksanakan pemantauan ke atas perisian hasad serta cadangan perlindungan;
d) memproses dan menyimpan maklumat rahsia rasmi MPS yang diluluskan sahaja;
e) memberikan khidmat sokongan sekiranya berlaku insiden keselamatan maklumat;
f) memastikan keperluan keselamatan maklumat dipenuhi sekiranya perkhidmatan pengkomputeran awan dilaksanakan oleh Pihak Ketiga;
g) membantu MPS mengumpul bukti digital sekiranya diperlukan oleh undang-undang;
h) menyediakan khidmat sokongan yang bersesuaian sekiranya perkhidmatan awan tidak disambung guna;
i) menyediakan sandaran ke atas maklumat dan tetapan konfigurasi perkhidmatan awan; dan
j) menyediakan dan mengembalikan maklumat seperti fail konfigurasi, kod sumber dan maklumat MPS sekiranya perkhidmatan pengkomputeran awan ditamatkan.

1.23.3 Pengurusan Perubahan Perkhidmatan Pengkomputeran Awan	Tanggungjawab
Pengurusan perubahan perlu dilaksanakan berdasarkan perkara berikut: a) pertukaran infrastruktur yang mengubah perkhidmatan yang ditawarkan dalam pengkomputeran awan; b) penyimpanan atau pemprosesan maklumat mengikut pemetaan geografi yang baharu mengikut undang- undang; dan c) penyedia melantik syarikat lain sebagai pengendali perkhidmatan pengkomputeran awan.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

1.24 PERANCANGAN DAN PENYEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

Objektif:

Memastikan perancangan pengurusan insiden keselamatan maklumat yang dilaksanakan adalah konsisten dan teratur.

1.24.1 Tugas dan Tanggungjawab	Tanggungjawab
Perkara yang perlu diambil kira adalah seperti yang berikut: a) mewujudkan prosedur bagi mengendalikan pengurusan insiden keselamatan maklumat;	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset, CERT MPS

b) memastikan tindakan pengukuhan serta maklum balas yang cepat, efektif dan teratur bagi setiap insiden keselamatan maklumat;
c) pemakluman kepada agensi kerajaan pusat yang bertanggungjawab dalam menangani insiden keselamatan; dan
d) menyediakan latihan yang bersesuaian kepada pasukan teknikal yang bertanggungjawab ke atas insiden keselamatan.

1.24.2 Prosedur Pengurusan Insiden	Tanggungjawab
Perkara yang perlu diambil kira seperti yang berikut: a) penilaian risiko ke atas insiden yang berlaku; b) pemantauan, pengelasan, analisis dan laporan insiden perlu disediakan sama ada secara manual atau melalui sistem; c) memastikan log aktiviti insiden keselamatan direkodkan; dan d) mengenal pasti punca insiden.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset, CERT MPS

1.25 PENILAIAN DAN TINDAKAN INSIDEN KESELAMATAN MAKLUMAT

Objektif:

Mengenal pasti kategori dan penilaian berasaskan keutamaan ke atas semua insiden keselamatan maklumat.

1.25.1 Penilaian dan Tindakan Insiden Keselamatan Maklumat	Tanggungjawab
Aktiviti keselamatan maklumat hendaklah dinilai dan dianalisis untuk diklasifikasikan sebagai insiden keselamatan maklumat. Perkara yang perlu diambil kira adalah seperti yang berikut: a) mengenal pasti dan mengesahkan kategori serta keutamaan insiden maklumat; dan b) merekodkan dan menyimpan semua tindakan serta keputusan insiden keselamatan maklumat untuk tujuan rujukan masa hadapan.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset

1.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT

Objektif:

Melaksanakan tindak balas yang cepat dan berkesan terhadap insiden keselamatan maklumat.

1.26.1 Tindak Balas Terhadap Insiden Keselamatan Maklumat	Tanggungjawab
Perkara yang perlu diambil kira adalah seperti yang berikut:	ICTSO, CERT MPS

a) mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku;
b) melaksanakan kajian dan analisis;
c) menghubungi pihak berkuasa atau agensi yang berkenaan dengan secepat mungkin;
d) menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;
e) menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;
f) menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan sekiranya perlu;
g) menyediakan tindakan pemulihan (restoration) dengan kadar segera;
h) menangani insiden keselamatan maklumat berdasarkan peraturan yang berkuat kuasa;
i) insiden perlu ditutup secara rasmi dan direkodkan setelah insiden berjaya ditangani; dan
j) melaksanakan pascainsiden untuk mengenal pasti punca insiden.

1.27 PENAMBAHBAIKAN KAWALAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT YANG LEPAS

Objektif:

Meningkatkan kawalan keselamatan berdasarkan analisis dan penyelesaian insiden keselamatan maklumat yang telah dilaksanakan bagi mengelakkan insiden yang sama berulang.

1.27.1 Pengajaran dari insiden keselamatan maklumat yang lepas	Tanggungjawab
Penilaian insiden yang perlu diambil kira adalah seperti yang berikut: a) menambah baik pelan pengurusan insiden; b) mengenal pasti punca insiden yang kerap berlaku bagi melaksanakan kawalan tambahan yang diperlukan untuk mengurangkan risiko; dan c) meningkatkan kesedaran keselamatan maklumat kepada warga MPS.	ICTSO, CERT MPS

1.28 PENGUMPULAN BUKTI

Objektif:

Memastikan pengurusan penyimpanan bukti direkodkan secara konsisten bagi insiden keselamatan maklumat untuk tindakan tatatertib dan undang-undang.

1.28.1 Pengumpulan dan Pengendalian Bukti	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti berikut:	ICTSO, CERT MPS

a) mengenal pasti, mengumpul, menyimpan dan melindungi bahan bukti untuk mengelakkan pengubahsuaian tanpa kebenaran;
b) menyimpan jejak audit, back up secara berkala dan
c) melindungi integriti bahan bukti; dan
d) sistem maklumat perlu merekodkan semua bukti insiden selaras dengan tarikh dan masa kejadian.

1.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN

Objektif:

Memastikan perancangan untuk melindungi perkhidmatan dan maklumat dilindungi semasa berlakunya gangguan.

1.29.1 Perancangan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan

Tanggungjawab

Perkara berikut perlu diberi perhatian:

Pasukan PKP

a) membangunkan Pelan Pengurusan Kesinambungan Perkhidmatan (PKP) dengan mengenal pasti aspek keselamatan maklumat yang terlibat;
b) memastikan keselamatan maklumat dan perkhidmatan sistem maklumat dilindungi semasa gangguan bencana;
c) mengaktifkan PKP mengikut tempoh yang ditetapkan;
d) memastikan tiada gangguan kepada proses dalam penyediaan perkhidmatan MPS; dan
e) memastikan pelan ini diluluskan oleh pegawai yang bertanggungjawab.

1.29.2 Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan

Tanggungjawab

Perkara yang perlu diambil kira adalah seperti yang berikut:

Pasukan PKP

a) mengenal pasti aspek keselamatan maklumat dalam membangunkan pelan kesinambungan perkhidmatan;
b) mengenal pasti aset, tanggungjawab, struktur MPS dan menetapkan prosedur pemulihan yang bersesuaian;
c) mengenal pasti ancaman yang boleh mengakibatkan gangguan terhadap proses perkhidmatan MPS;
d) mengenal pasti kemungkinan dan impak gangguan tersebut serta akibatnya terhadap keselamatan ICT;
e) menjalankan analisis impak MPS;

f) melaksanakan prosedur keselamatan bagi membolehkan pemulihan dapat dilaksanakan dalam jangka masa yang ditetapkan;
g) merekodkan proses dan prosedur yang telah ditetapkan;
h) mengadakan program latihan secara berkala kepada warga MPS mengenai prosedur kecemasan;
i) membuat *backup* mengikut prosedur yang ditetapkan; dan
j) menguji, menyelenggara dan mengemas kini setiap pelan dalam PKP mengikut keperluan.

1.29.3 Mengkaji, Menilai dan Mengesahkan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	Tanggungjawab
Perkara yang perlu diambil kira adalah seperti yang berikut: a) senarai aktiviti teras dan aset yang dianggap kritikal mengikut susunan keutamaan; b) senarai warga MPS dan Pihak Ketiga berserta maklumat perhubungan (nombor telefon dan alamat e-mel); c) alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah terancam; d) menetapkan arahan pemulihan maklumat dan kemudahan yang berkaitan; e) perjanjian dengan Pihak Ketiga untuk mendapatkan penyambungan semula perkhidmatan mengikut keutamaan; f) salinan Pelan Kesinambungan Perkhidmatan perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama; g) Pelan Kesinambungan Perkhidmatan hendaklah diuji secara berkala atau apabila terdapat perubahan dalam persekitaran atau fungsi MPS untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan; dan h) ujian pelan hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab serta peranan mereka apabila pelan dilaksanakan.	CDO, Pasukan PKP

1.30 KETERSEDIAAN ICT BAGI KESINAMBUNGAN PERKHIDMATAN

Objektif:

Memastikan ketersediaan maklumat dan aset ICT yang berkaitan semasa gangguan berdasarkan Pelan Pemulihan Bencana ICT (DRP-ICT).

1.30.1 Pengenalpastian Ketersediaan aset ICT Semasa Gangguan	Tanggungjawab
Perkara yang perlu diambil kira adalah seperti berikut:	Pasukan DRP MPS

a) mengenal pasti Recovery Time Objective (RTO) dan Recovery Point Objective (RPO) untuk sistem aplikasi kritikal mengikut keutamaan;
b) menyediakan Pelan Pemulihan Bencana ICT (DRP-ICT) dan memastikan pelan ini diluluskan oleh pegawai yang bertanggungjawab;
c) menjalankan pengujian bagi memastikan ketersediaan aset ICT dapat berfungsi semasa gangguan; dan
d) senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya.

1.31 KEPERLUAN UNDANG-UNDANG, PERATURAN DAN KONTRAK

Objektif:

Bagi memastikan pematuhan kepada keperluan undang-undang yang berkaitan dengan keselamatan maklumat. Semua keperluan undang-undang berkanun, peraturan dan kontrak perjanjian yang berkaitan dengan MPS perlu ditakrifkan, didokumenkan, dan disimpan sehingga tarikh yang sesuai bagi setiap sistem maklumat.

1.31.1 Pengenalpastian Keperluan Perundangan dan Perjanjian Kontrak	Tanggungjawab
Pihak Ketiga (Pihak Kontraktor/ Perunding) yang melanggar mana-mana klausa dalam integrity pact boleh ditamatkan perkhidmatannya. Senarai Perundangan dan Peraturan yang berkuat kuasa dari semasa ke semasa perlu dipatuhi oleh semua warga MPS adalah seperti di LAMPIRAN 5.	Pihak Ketiga

1.31.2 Kawalan Kriptografi	Tanggungjawab
Kunci enkripsi mestilah dilindungi dengan menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut. Kunci enkripsi mestilah dilindungi dengan menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut. Kriptografi turut merangkumi kaedah-kaedah seperti yang berikut: a) kesemua pelaksanaan sistem hendaklah menggunakan ID atau kata laluan dan dibuat enkripsi; dan b) penggunaan *Public Key Infrastructure* (PKI) yang selamat yang dibekalkan oleh Kerajaan.	Pentadbir Sistem ICT, Pengguna

1.32 HAK HARTA INTELEK

Objektif:

Bagi memastikan pematuhan ke atas undang-undang terhadap harta intelek.

1.32.1 Pematuhan Terhadap Hak Harta Intelek (*Intellectual Property Rights*)	Tanggungjawab
Warga MPS dan Pihak Ketiga perlu mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat. Warga MPS dan Pihak Ketiga hendaklah mematuhi: a) keperluan hak cipta yang berkaitan dengan bahan proprietary, perisian, dan reka bentuk yang diperoleh melalui MPS; b) keperluan pelesenan mengehadkan penggunaan produk, perisian, reka bentuk dan bahan-bahan lain yang diperoleh oleh MPS; c) pematuhan yang berterusan dengan sekatan hak cipta produk dan keperluan pelesenan; dan d) pengguna tidak dibenarkan menggunakan kemudahan pemprosesan maklumat bagi tujuan yang tidak dibenarkan.	Warga MPS, Pihak Ketiga

1.33 PERLINDUNGAN REKOD

Objektif:

Bagi memastikan pematuhan ke atas undang-undang yang berkaitan dengan rekod.

1.33.1 Perlindungan Rekod	Tanggungjawab
Rekod-rekod yang penting (fizikal atau digital) hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian yang tidak dibenarkan, penyebaran yang tidak dibenarkan mengikut undang-undang, peraturan, kontrak, dan keperluan perniagaan Perkara yang perlu dipertimbangkan ialah: a) pengekalan, penyimpanan, pengendalian dan pelupusan rekod dan maklumat; b) jadual penyimpanan rekod perlu dikenal pasti; dan c) inventori rekod.	Warga MPS, Pihak Ketiga

1.34 PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI

Objektif:

Bagi memastikan pematuhan ke atas undang-undang yang berkaitan dengan aspek Keselamatan maklumat peribadi.

1.34.1 Perlindungan dan Privasi Data Peribadi	Tanggungjawab
Privasi dan perlindungan maklumat peribadi pengguna dijamin seperti yang tertakluk dalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkenaan.	ICTSO

1.35 KAJIAN OLEH PIHAK BEBAS / LUARAN BERKAITAN KESELAMATAN MAKLUMAT

Objektif:

Bagi memastikan pendekatan yang digunakan oleh MPS bersesuaian, cukup dan berkesan secara lebih efektif.

1.35.1 Kajian Bebas/ Pihak Ketiga Terhadap Keselamatan Maklumat	Tanggungjawab
Pelaksanaan keselamatan maklumat MPS hendaklah dikaji secara bebas atau oleh Pihak Ketiga pada jangka masa yang dirancang atau apabila perubahan ketara berlaku dalam pelaksanaannya.	Jawatankuasa Pelaksana ISMS, Audit SIRIM

1.36 PIAWAIAN UNTUK KESELAMATAN MAKLUMAT

Objektif:

Memastikan keselamatan maklumat dilaksanakan mengikut polisi keselamatan maklumat serta piawaian dan peraturan semasa.

1.36.1 Pematuhan Dasar dan Standard / Piawaian	Tanggungjawab
MPS hendaklah membuat kajian semula pematuhan berdasarkan standard / piawaian yang berkaitan. Sekiranya kajian semula mendapati berlaku ketidakpatuhan, MPS perlu: a) mengenal pasti punca ketidakpatuhan; b) menilai keperluan tindakan untuk mencapai pematuhan; c) melaksanakan tindakan pembetulan yang sewajarnya; dan d) mengkaji semula tindakan pembetulan yang diambil untuk mengesahkan keberkesanannya dan mengenal pasti apa-apa kekurangan dan kelemahan.	Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

1.36.2 Penilaian Tahap Keselamatan	Tanggungjawab
Sistem maklumat hendaklah diuji selaras dengan pematuhan peraturan semasa yang berkuat kuasa. Penilaian ini perlu dilaksanakan sekurang-kurangnya sekali dalam setahun atau mengikut keperluan.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

1.37 PROSEDUR OPERASI YANG PERLU DIDOKUMENKAN

Objektif:

Prosedur operasi bagi kemudahan pemprosesan maklumat perlu disediakan dan dapat diakses dengan selamat.

1.37.1 Penyediaan Prosedur Operasi	Tanggungjawab
Menyediakan dokumen operasi standard untuk perkara berikut: a) aktiviti yang sentiasa dilaksanakan oleh Warga MPS; b) aktiviti yang jarang dilaksanakan; c) aktiviti yang baharu dan penilaian risiko tidak dapatkan dijalankan dengan betul; dan d) serahan tugas kepada kakitangan baharu.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

1.37.2 Kandungan Dokumen Prosedur Operasi	Tanggungjawab
Dokumen Prosedur Operasi hendaklah diwujudkan, disemak dan dikemas kini mengikut keperluan. Kandungan dokumen yang perlu disediakan adalah seperti yang berikut: a) pegawai bertanggungjawab; b) instalasi dan konfigurasi sistem; c) pemprosesan maklumat secara manual dan automatik; d) sandaran (*backup*); e) jadual keperluan termasuk kebergantungan dengan sistem lain; f) pengendalian ralat; g) khidmat sokongan sekiranya berlaku masalah operasi dan teknikal; h) arahan pengendalian media storan; i) prosedur pemulihan sekiranya berlaku kegagalan sistem; j) pengurusan jejak audit sistem; k) pemantauan ke atas kapasiti prestasi dan keselamatan sistem; dan l) manual penyelenggaraan.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

BAB 2
KAWALAN MANUSIA

BAB 2 | KAWALAN MANUSIA

2.1 Tapisan Keselamatan Individu

Objektif:

Memastikan kakitangan dan orang awam memahami tanggungjawab serta peranan dalam aspek keselamatan ICT sepanjang tempoh perkhidmatan mereka.

2.1.1 Tapisan ke atas Kakitangan Awam (Tapisan Sebelum Pengesahan Pelantikan)	Tanggungjawab
Pengesahan pelantikan perlu mengambil kira perkara seperti yang berikut: a) memeriksa kesahihan maklumat yang merangkumi identiti pengenalan diri, rujukan individu, resume, kelayakan akademik, sijil profesional dan rekod jenayah; b) menjalankan tapisan keselamatan untuk pegawai dan kakitangan yang terlibat. Ia berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; c) mengehadkan capaian dan penggunaan aset kerajaan; dan d) mengambil tindakan seperti menangguhkan pelantikan atau membatalkan pelantikan sekiranya kakitangan tidak melepasi tapisan dalam tempoh yang ditetapkan.	Bahagian Sumber Manusia MPS, ICTSO,

2.1.2 Tapisan ke atas Pihak Ketiga	Tanggungjawab
Tapisan ke atas perkara-perkara berikut: a) memeriksa kesahihan maklumat yang merangkumi identiti pengenalan diri, surat tawaran kerja serta perkara lain yang berkaitan serta bersesuaian dengan tawaran kerja yang diberikan; b) memastikan semua pekerja menjalani tapisan keselamatan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; c) mengehadkan capaian dan penggunaan aset kerajaan; dan d) mengambil tindakan seperti menangguhkan pelantikan atau membatalkan pelantikan individu yang tidak melepasi tapisan dalam tempoh yang ditetapkan.	ICTSO, Pihak Ketiga

2.2 Terma dan Syarat Pelantikan

Objektif:

Memastikan kakitangan dan Pihak Ketiga memahami tanggungjawab serta peranan dalam keselamatan ICT.

2.2.1 Terma dan Syarat Pelantikan	Tanggungjawab
Terma dan Syarat Pelantikan yang perlu dipatuhi adalah seperti yang berikut: a) mengisi dan memperakui pematuhan perjanjian melalui Surat Akuan Pematuhan Polisi Keselamatan Siber (PKS) MPS dan Akta Rahsia Rasmi 1972 (Akta 88) bagi tujuan menjaga kerahsiaan maklumat dan aset ICT yang berkaitan; b) memahami dan bersetuju ke atas tanggungjawab serta hak berkaitan perlindungan keselamatan maklumat; c) memahami peranan dan tanggungjawab dalam keselamatan penyampaian maklumat bagi mengurangkan risiko penyalahgunaan aset ICT; d) mematuhi semua terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan dan ditandatangani; e) bertanggungjawab untuk mengklasifikasikan maklumat dan aset lain yang berkaitan; f) bertanggungjawab untuk mengendali maklumat daripada pihak berkepentingan; dan g) bertanggungjawab untuk mengambil tindakan jika keselamatan maklumat tidak dipatuhi.	ICTSO, Warga MPS, Pihak Ketiga

2.3 PROGRAM KESEDARAN, PENDIDIKAN DAN LATIHAN BERKAITAN KESELAMATAN MAKLUMAT

Objektif:

Memastikan Warga MPS dan Pihak Ketiga mengambil maklum dan jelas berkaitan tanggungjawab ke atas keselamatan maklumat.

2.3.1 Program Kesedaran Keselamatan Maklumat	Tanggungjawab
Perkara-perkara yang perlu dilaksanakan adalah seperti yang berikut: a) mendapatkan sokongan pengurusan atasan berkaitan keselamatan maklumat; b) memberikan kesedaran berkaitan undang-undang, peraturan dan perjanjian; c) melaksanakan program kesedaran berkaitan dengan keselamatan maklumat kepada warga MPS dan Pihak Ketiga secara berterusan semasa melaksanakan tugas-tugas dan tanggungjawab mereka; dan	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

d) memaklumkan senarai perhubungan sekiranya pelanggaran maklumat dikesan oleh warga MPS atau Pihak Ketiga.

2.3.2 Program Latihan dan Pendidikan berkaitan Keselamatan Maklumat	Tanggungjawab
Perkara-perkara berikut hendaklah diberi perhatian: a) mengenal pasti, menyediakan dan menjalankan latihan berkaitan keselamatan maklumat yang bersesuaian dan terkini untuk meningkatkan kemahiran bagi memastikan keselamatan maklumat di tahap yang optimum; b) memastikan latihan dan program kesedaran yang diberikan kepada pengguna dari semasa ke semasa bagi meningkatkan kompetensi pengguna berkaitan keselamatan maklumat; dan c) memastikan prosedur latihan jabatan sentiasa dikemas kini bersesuaian dengan fungsi tugas semasa setiap pengguna.	Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

2.4 TINDAKAN DISIPLIN

Objektif:

Memastikan kakitangan dan Pihak Ketiga memahami kesan pelanggaran ke atas keselamatan maklumat mengikut undang-undang atau peraturan lain-lain yang sedang berkuat kuasa.

2.3.1 Tindakan Pelanggaran Undang-undang dan Peraturan	Tanggungjawab
Tindakan boleh dikenakan ke atas kakitangan dan Pihak Ketiga yang tidak mematuhi keselamatan maklumat. Langkah-langkah yang perlu diambil adalah: a) memastikan adanya proses tindakan perundangan ke atas Pihak Ketiga sekiranya berlaku pelanggaran terhadap Akta Rahsia Rasmi 1972 (Akta 88); dan b) memastikan adanya proses tindakan tatatertib ke atas warga MPS sekiranya berlaku pelanggaran terhadap Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993 [P.U.(A) 395/1993], dasar-dasar Kerajaan, undang-undang serta peraturan yang berkuat kuasa.	ISCSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Pegawai Undang-Undang, Ketua Unit Integriti, Jabatan Khidmat Pengurusan, Warga MPS, Pihak Ketiga

2.5 TANGGUNGJAWAB SELEPAS PERTUKARAN ATAU PENAMATAN KERJA

Objektif:

Melindungi kepentingan jabatan semasa proses pertukaran atau penamatan warga MPS.

2.5.1 Penamatan atau Pertukaran	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) memastikan semua aset ICT dikembalikan kepada MPS mengikut peraturan dan terma perkhidmatan yang ditetapkan; b) melaksanakan pertukaran atau penamatan hendaklah ditakrifkan dengan jelas termasuk: i. perubahan dalam terma dan syarat pertukaran atau penamatan tanggungjawab; ii. tempoh akhir pekerjaan; dan iii. tanggungjawab masih sah selepas penamatan. c) menjaga kerahsiaan keselamatan maklumat walaupun selepas penamatan atau pertukaran; dan d) membatalkan atau menarik balik semua kebenaran hak akses ke atas sistem maklumat mengikut peraturan yang ditetapkan.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Warga MPS, Pihak Ketiga

2.6 PERJANJIAN KERAHSIAAN ATAU *NON-DISCLOSURE AGREEMENT*

Objektif:

Memastikan kerahsiaan maklumat yang boleh diakses oleh warga MPS atau Pihak Ketiga dikenal pasti, didokumenkan, disemak secara berkala dan ditandatangani.

2.6.1 Kerahsiaan Atau *Non-Disclosure Agreement*	Tanggungjawab
Perjanjian kerahsiaan perlu melindungi maklumat berdasarkan undang-undang yang berkuat kuasa terhadap pihak yang berkepentingan dan warga MPS. Kandungan *Non-Disclosure Agreement* yang perlu dipatuhi adalah seperti yang berikut: a) definisi maklumat yang perlu dilindungi; b) tempoh perjanjian kerahsiaan; c) tindakan selepas penamatan perjanjian; d) pengesahan ke atas peminjaman atau akses maklumat perlu dilaksanakan bagi mencegah kebocoran maklumat; e) pemilikan maklumat, kerahsiaan dan harta intelek yang berkaitan dengan perlindungan kerahsiaan maklumat; f) kebenaran untuk menggunakan maklumat rahsia rasmi;	ICTSO, Pihak Ketiga

g) hak untuk mengaudit dan memantau aktiviti yang melibatkan maklumat rahsia rasmi;
h) proses pemakluman dan pelaporan kebocoran atau pendedahan maklumat;
i) syarat pemulangan atau penghapusan maklumat selepas perjanjian tamat; dan
j) tindakan undang-undang sekiranya perjanjian tidak dipatuhi.

2.7 BEKERJA JARAK JAUH

Objektif:

Memastikan kawalan keselamatan terhadap individu yang bekerja jarak jauh untuk melindungi keselamatan maklumat.

2.7.1 Kerja Jarak Jauh	Tanggungjawab
Kebenaran aktiviti kerja jarak jauh di luar premis MPS perlu mematuhi perkara seperti yang berikut: a) keselamatan fizikal bagi lokasi bekerja jarak jauh seperti di rumah atau lokasi yang dibenarkan sahaja; b) kawalan keselamatan yang merangkumi kabinet fail berkunci, peraturan berkaitan remote access, clear desk, pencetakan dan pelupusan maklumat atau aset lain yang berkaitan dan insiden keselamatan; c) mengenal pasti lokasi persekitaran fizikal untuk bekerja jarak jauh; d) menggunakan kawalan komunikasi yang selamat untuk akses ke atas maklumat rahsia rasmi, sistem dan aplikasi kritikal; e) membenarkan peralatan milik persendirian digunakan untuk remote access seperti perisian Remote Desktop; f) mengehadkan konfigurasi rangkaian tanpa wayar (Wi-Fi) dengan membuat pemilihan kategori rangkaian yang selamat; g) penggunaan kawalan peralatan atau perisian keselamatan; dan h) pengesahan dan pengaktifan hak akses jarak jauh yang selamat semasa menggunakan rangkaian luar MPS.	Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Warga MPS, Pihak Ketiga

2.7.2 Garis Panduan Kerja Jarak Jauh	Tanggungjawab
Garis panduan kerja jarak jauh hendaklah mematuhi perkara berikut: a) menetapkan klasifikasi maklumat dan perkhidmatan sistem yang boleh diakses oleh individu bekerja jarak jauh; b) memastikan keselamatan fizikal; c) menyediakan peraturan serta panduan akses peralatan dan maklumat oleh pihak lain;	Pentadbir Bilik *Server* Utama MPS / Rangkaian, Warga MPS, Pihak Ketiga

d) melaksanakan prosedur sandaran dan kesinambungan perkhidmatan; dan
e) membatalkan hak akses dan pemulangan peralatan apabila aktiviti kerja jarak jauh selesai.

2.8 PELAPORAN INSIDEN KESELAMATAN MAKLUMAT

Objektif:

Memastikan insiden dikendalikan dengan berkesan bagi meminimumkan impak supaya tidak menjejaskan sistem penyampaian perkhidmatan.

2.8.1 Pelaporan Insiden Keselamatan Maklumat	Tanggungjawab
Insiden keselamatan merangkumi insiden, pelanggaran dan kerentanan sistem. Warga MPS dan Pihak Ketiga yang menggunakan sistem dan perkhidmatan maklumat MPS dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT. Insiden keselamatan perlu dilaporkan apabila berlaku perkara seperti yang berikut: a) kawalan keselamatan maklumat yang tidak berkesan; b) pelanggaran sebarang kerahsiaan, integriti atau ketersediaan maklumat; c) kesilapan manusia; d) ketidakpatuhan terhadap polisi keselamatan maklumat; e) pelanggaran keselamatan fizikal; f) perubahan sistem yang tidak melalui proses pengurusan perubahan; g) perisian atau perkakasan yang rosak atau tidak berfungsi; h) penyalahgunaan hak akses; i) kerentanan; dan j) percubaan serangan perisian hasad.	CERT MPS, Warga MPS, Pihak Ketiga

BAB 3
KAWALAN FIZIKAL

BAB 3 | KAWALAN FIZIKAL

3.1 PERIMETER KESELAMATAN FIZIKAL

Objektif:

Memastikan kawalan keselamatan fizikal berkaitan maklumat, premis dan kemudahan ICT.

3.1.1 Keselamatan Fizikal	Tanggungjawab

Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh premis. Langkah-langkah keselamatan fizikal adalah seperti yang berikut:

CDO, ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Warga MPS

a) mengehadkan akses masuk ke kawasan yang berkaitan kepada kakitangan yang dibenarkan sahaja berdasarkan kelulusan;
b) menyediakan dan menyemak buku log audit trail akses ke Bilik *Server* Utama MPS secara berkala;
c) menggunakan kad akses untuk kemasukan fizikal ke kawasan penyimpanan maklumat atau kawasan larangan;
d) menyediakan kawasan menunggu atau penerimaan yang boleh dipantau oleh pegawai bertanggungjawab MPS;
e) melaksanakan pemeriksaan fizikal kepada pengguna dan barangan kepunyaan peribadi;
f) memastikan pemakaian pas keselamatan sepanjang berada di premis MPS;
g) memberikan akses yang terhad dan pemantauan kepada kakitangan Pihak Ketiga ke kawasan pemprosesan maklumat atau kawasan larangan apabila diperlukan sahaja;
h) memastikan keselamatan akses ke atas peralatan MPS yang ditempatkan di lokasi berkongsi dengan agensi lain;
i) mengemas kini kawalan keselamatan fizikal dengan lebih kukuh bagi insiden yang kerap berlaku atau meningkat;
j) memastikan pintu masuk lain seperti pintu kecemasan dikawal daripada akses tanpa kebenaran; dan
k) menetapkan proses pengurusan kunci bagi memastikan kunci fizikal atau kod berkunci ke kawasan pemprosesan maklumat atau kawasan larangan dipantau dan direkodkan.

3.2 KAWALAN KEMASUKAN FIZIKAL

Objektif:

Melaksanakan kawalan akses masuk kepada maklumat, premis dan kemudahan ICT.

3.2.1 Kawalan Akses Masuk Fizikal

Tanggungjawab

ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Warga MPS, Pihak Ketiga

Kawalan keluar masuk ke premis MPS seperti kawasan penghantaran, pemunggahan dan kawasan larangan perlu mematuhi perkara seperti yang berikut:

a) mengehadkan akses masuk ke kawasan yang berkaitan kepada kakitangan yang dibenarkan sahaja berdasarkan kelulusan;
b) menyediakan dan menyemak buku log audit trail akses ke Bilik *Server* Utama MPS secara berkala;
c) menggunakan kad akses untuk kemasukan fizikal ke kawasan penyimpanan maklumat atau kawasan larangan;
d) menyediakan kawasan menunggu atau penerimaan yang boleh dipantau oleh pegawai bertanggungjawab MPS;
e) melaksanakan pemeriksaan fizikal kepada pengguna dan barangan kepunyaan peribadi;
f) memastikan pemakaian pas keselamatan sepanjang berada di premis MPS;
g) memberikan akses yang terhad dan pemantauan kepada kakitangan Pihak Ketiga ke kawasan pemprosesan maklumat atau kawasan larangan apabila diperlukan sahaja;
h) memastikan keselamatan akses ke atas peralatan MPS yang ditempatkan di lokasi berkongsi dengan agensi lain;
i) mengemas kini kawalan keselamatan fizikal dengan lebih kukuh bagi insiden yang kerap berlaku atau meningkat;
j) memastikan pintu masuk lain seperti pintu kecemasan dikawal daripada akses tanpa kebenaran; dan
k) menetapkan proses pengurusan kunci bagi memastikan kunci fizikal atau kod berkunci ke kawasan pemprosesan maklumat atau kawasan larangan dipantau dan direkodkan.

3.2.2 Kawalan Keselamatan Pelawat

Tanggungjawab

Khidmat Pelanggan MPS, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

Perkara berikut perlu dipatuhi:

a) setiap pelawat mestilah mendaftar dan mendapatkan pas pelawat di pintu masuk utama;
b) mengesahkan identiti pelawat, memaparkan pas pelawat sepanjang di premis dan mengembalikan pas pelawat selepas selesai urusan;
c) merekodkan maklumat keluar dan masuk pelawat;
d) hanya memberikan kebenaran akses kepada kawasan yang diperlukan sahaja;
e) pelawat perlu diiringi oleh warga MPS di kawasan larangan

3.2.3 Kawasan Penghantaran dan Pemunggahan	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mempunyai akses terhad kepada kawasan penghantaran dan pemunggahan oleh Pihak Ketiga; b) memastikan Pihak Ketiga tidak dibenarkan masuk ke lokasi lain tanpa kebenaran; c) memastikan kawasan penghantaran dan pemunggahan atau tempat lain dikawal semasa proses penghantaran dan pemunggahan; d) memeriksa dan memastikan barang yang dihantar tidak mengandungi bahan letupan atau bahan berbahaya yang lain; e) semua penghantaran barang perlu didaftar mengikut prosedur pengurusan aset; dan f) memastikan barang yang diterima tidak diubah suai tanpa kebenaran.	Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

3.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN ICT

Objektif:

Memastikan keselamatan dan perlindungan daripada sebarang bentuk pencerobohan, ancaman, kerosakan, kecuaian serta akses yang tidak dibenarkan.

3.3.1 Kawalan Pejabat, Bilik dan Kemudahan ICT	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) memastikan kawasan larangan dihadkan daripada akses tanpa kebenaran; b) memastikan penunjuk ke lokasi bilik operasi atau kawasan larangan tidak didedahkan atau hanya memberi petunjuk yang minimum; c) memastikan maklumat kawasan larangan tidak dapat dilihat oleh Pihak Ketiga; dan d) memastikan maklumat perhubungan atau lokasi kawasan larangan tidak didedahkan tanpa kebenaran.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Warga MPS

3.4 PEMANTAUAN KESELAMATAN FIZIKAL

Objektif:

Memantau dan memastikan keselamatan fizikal dikawal

3.4.1 Pemantauan Terhadap Premis Fizikal	Tanggungjawab
Pemantauan kepada bangunan yang menempatkan sistem kritikal perlu dipantau dengan cara berikut: a) memasang dan memantau sistem kamera litar tertutup (CCTV) di dalam dan luar bangunan MPS; b) mengehadkan akses berdasarkan peranan dan tanggungjawab individu melalui Sistem Pengurusan Kad Akses dan/atau Biometrik; c) memastikan pemasangan penggera yang merangkumi semua pintu yang boleh akses masuk ke kawasan larangan; dan d) reka bentuk sistem pemantauan tidak boleh didedahkan tanpa kebenaran untuk mengelakkan kebocoran maklumat dan di pecah masuk.	Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

3.5 PERLINDUNGAN TERHADAP ANCAMAN FIZIKAL DAN BENCANA ALAM

Objektif:

Memastikan infrastruktur yang direka bentuk dilindungi daripada ancaman fizikal dan bencana alam.

3.5.1 Perlindungan Terhadap Ancaman Fizikal dan Bencana Alam	Tanggungjawab
Penilaian risiko ke atas ancaman fizikal dan bencana alam perlu dijalankan secara berkala. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mereka bentuk dan melaksanakan pelan perlindungan fizikal daripada kebakaran dan bencana alam; b) memastikan pelan tindakan perlindungan bagi ancaman berbahaya seperti letupan, kacau-bilau, rusuhan dan sebagainya; dan c) pelan tindakan perlindungan perlu merangkumi kawalan seperti bencana alam, kebakaran, gangguan bekalan elektrik dan letupan.	Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

3.6 BEKERJA DI KAWASAN LARANGAN

Objektif:

Memastikan maklumat dan aset ICT berada di kawasan yang selamat daripada gangguan atau kerosakan daripada pekerja sekitarnya

3.6.1 Kawasan Larangan	Tanggungjawab

Perkara yang perlu dipatuhi adalah seperti yang berikut:

a) memastikan individu yang bekerja di kawasan tersebut memahami tanggungjawab mereka;
b) memantau dan mengawasi setiap kerja yang dijalankan di kawasan larangan;
c) kawasan larangan perlu sentiasa berkunci dan memeriksa ruangan kosong yang ada;
d) fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk melainkan dengan kebenaran;
e) mengawal peranti yang dibenarkan dibawa masuk ke dalam kawasan larangan; dan
f) memaparkan prosedur kecemasan yang mudah dilihat atau diakses.

Pentadbir Sistem ICT, , Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Warga MPS, Pihak Ketiga

3.7 *Clear Desk and Clear Screen*

Objektif:

Memastikan kawalan capaian maklumat yang tidak dibenarkan di atas meja atau di paparan skrin atau di mana-mana lokasi yang boleh diakses semasa dan di luar waktu pejabat.

3.7.1 *Clear Desk and Clear Screen*	Tanggungjawab

Clear Desk and Clear Screen bermaksud tidak meninggalkan maklumat sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

Warga MPS

Perkara yang perlu dipatuhi adalah seperti yang berikut:

a) menggunakan kemudahan password screen saver atau log keluar apabila meninggalkan komputer;
b) menetapkan paparan skrin akan tertutup selepas 10 minit tidak digunakan oleh pengguna;
c) dokumen terperingkat hendaklah disimpan dalam laci atau kabinet fail yang berkunci;
d) membersihkan maklumat sensitif atau kritikal pada papan putih dan jenis paparan lain apabila tidak diperlukan lagi;
e) memastikan semua dokumen diambil segera dari pencetak, pengimbas dan mesin fotostat; dan

f) menghalang penggunaan tanpa kebenaran mesin fotostat dan teknologi penghasilan semula seperti mesin pengimbas atau kamera digital.

3.8 PENEMPATAN DAN PERLINDUNGAN ASET ICT

Objektif:

Memastikan aset ICT ditempatkan di kawasan yang selamat dan dilindungi daripada sebarang bentuk pencerobohan dan ancaman.

3.8.1 Penempatan dan Perlindungan aset ICT	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) kemudahan penyimpanan perlu dilindungi untuk menghalang akses yang tidak dibenarkan; b) kemudahan pemprosesan maklumat yang melaksanakan pengendalian maklumat rahsia rasmi harus ditempatkan dengan teliti untuk mengurangkan risiko maklumat tersebut dapat dilihat oleh pihak yang tidak berkaitan; c) mengadaptasi kawalan untuk mengurangkan risiko potensi ancaman fizikal dan bencana alam seperti kecurian, kebakaran, gangguan bekalan elektrik; dan lain-lain; d) menetapkan larangan makan, minum dan merokok di kedudukan berhampiran dengan kemudahan pemprosesan maklumat; e) pemantauan terhadap keadaan persekitaran seperti suhu dan kelembapan serta keadaan yang boleh menjejaskan operasi kemudahan pemprosesan maklumat; f) pemasangan alat perlindungan kilat; g) peralatan yang memerlukan perlindungan khas perlu dilindungi daripada bahaya atau kerosakan dengan langkah yang sesuai; h) sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; dan i) sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada Pengurus ICT.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Warga MPS, Pihak Ketiga

3.9 KESELAMATAN ASET DI LUAR PEJABAT

Objektif:

Memastikan keselamatan aset ICT yang dibawa keluar dari premis dilindungi.

3.9.1 Peralatan ICT di Luar MPS	Tanggungjawab

Semua peralatan aset ICT MPS yang digunakan di luar pejabat perlu mendapatkan kelulusan terlebih dahulu.

Pegawai Aset ICT, Warga MPS

Perkara yang perlu dipatuhi adalah seperti yang berikut:

a) tidak meninggalkan peralatan atau media yang menyimpan maklumat rahsia rasmi di tempat awam tanpa pengawasan;
b) mematuhi panduan untuk melindungi aset ICT pada setiap masa seperti terdedah kepada haba atau suhu yang tinggi;
c) memastikan maklumat peminjaman atau penggunaan aset ICT/ media storan di luar pejabat direkodkan dan data rahsia rasmi dihapuskan sebelum pemulangan;
d) memastikan kawalan keselamatan diambil kira semasa penggunaan aset ICT di tempat awam;
e) Aset ICT yang hendak dibawa keluar dari Pejabat MPS perlu mengisi Borang Kebenaran Membawa Keluar Aset, KEW.PA-9 dan mendapatkan kelulusan daripada Pengurus ICT; dan
f) mematuhi semua perkara yang dinyatakan di para 3.7.

3.10 MEDIA STORAN

Objektif:

Memastikan media storan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

3.10.1 Pengurusan Media Storan Mudah Alih (*Removal Media*)	Tanggungjawab

Media storan digunakan untuk menyimpan data dan maklumat seperti thumb drive, external drive dan media storan lain.

ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Warga MPS

Pengendalian media storan perlu mematuhi perkara seperti yang berikut:

a) media storan mudah alih hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
b) memastikan media storan mudah alih boleh berfungsi sekiranya diperlukan;
c) memastikan maklumat rahsia rasmi yang disimpan melebihi satu media storan mudah alih mengambil kira risiko kerosakan atau kehilangan maklumat;

d) akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada Pengurus ICT dan pegawai yang dibenarkan sahaja; dan
e) hanya maklumat rasmi dibenarkan untuk disimpan dalam media storan yang dibekalkan oleh MPS.

3.10.2 Keselamatan Pelupusan dan Penggunaan Semula Media	Tanggungjawab
Prosedur pelupusan dan penggunaan semula media storan hendaklah diwujudkan bagi mengurangkan risiko kebocoran maklumat. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) media storan yang akan digunakan semula perlu disanitasi atau diformat terlebih dahulu; b) melupuskan media storan yang mengandungi maklumat rahsia rasmi menggunakan kaedah yang dibenarkan sekiranya tidak diperlukan lagi; c) pelupusan media storan oleh Pihak Ketiga hendaklah mematuhi kawalan keselamatan dan dilaksanakan oleh pihak yang berpengalaman; d) pelupusan maklumat mengikut Tatacara Pelupusan Arkib Negara (Akta Arkib Negara 2003 [Akta 629]); e) penghapusan maklumat atau kandungan media mestilah mendapat kelulusan; f) pelupusan media storan hendaklah direkodkan; g) semua media storan yang hendak dilupuskan mestilah dirujuk kepada Bahagian Digital dan Teknologi Maklumat yang bertanggungjawab berkaitan ICT; dan h) pengguna hendaklah menghapuskan atau memindahkan semua maklumat rasmi/ terperingkat dari media storan sendiri apabila bersara/ bertukar jabatan/ ditamatkan perkhidmatan dan tamat/ ditamatkan kontrak.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT, Warga MPS

3.11 PERKHDMATAN SOKONGAN

Objektif:

Memastikan kawalan ke atas perkhidmatan sokongan ICT dilindungi daripada kegagalan bekalan kuasa dan gangguan fasiliti.

3.11.1 Perkhidmatan Sokongan ICT	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) memastikan peralatan di dalam fasiliti perkhidmatan sokongan beroperasi, dikonfigurasi dan diselenggarakan mengikut spesifikasi pengeluar yang berkaitan;	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

b) memastikan fasiliti perkhidmatan sokongan dinilai semula keupayaannya secara berkala bagi memenuhi keperluan MPS;
c) memastikan peralatan sokongan disemak dan diselenggarakan dari semasa ke semasa mengikut Perjanjian Tahap Perkhidmatan (SLA);
d) menyediakan fasiliti sokongan kedua;
e) memastikan peralatan di dalam fasiliti perkhidmatan sokongan sentiasa disokong oleh *Uninterruptible Power Supply* (UPS);
f) memastikan bekalan kuasa berterusan disalurkan kepada fasiliti sokongan seperti UPS dan penjana kuasa (*generator*) bagi membolehkan Bilik *Server* Utama MPS
beroperasi dengan optimum supaya perkhidmatan fasiliti sokongan di Bilik *Server* Utama MPS mendapat bekalan kuasa berterusan; dan
g) memastikan peralatan sokongan diperiksa dan diuji secara berkala oleh pihak berkaitan.

3.12 KESELAMATAN PENGKABELAN

Objektif:

Memastikan kabel rangkaian dan kuasa elektrik dilindungi daripada gangguan dan pencerobohan.

3.12.1 Keselamatan Kabel	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) kabel kuasa elektrik dan rangkaian yang disambungkan ke sistem maklumat diberi perlindungan yang bersesuaian untuk mengelakkan pemotongan kabel tanpa sengaja; b) mengasingkan kabel kuasa elektrik dan rangkaian untuk mencegah gangguan penghantaran data; Memastikan kabel bagi sistem kritikal mempunyai kawalan tambahan seperti yang berikut: a) pemasangan saluran pelindung berlapis (conduit) dan dalam bilik berkunci; b) semakan dan pemeriksaan teknikal secara berkala untuk mengenal pasti sambungan kabel yang tidak dibenarkan terhadap peranti; c) kawalan akses ke bilik telekomunikasi atau bilik kabel; d) memastikan semua sambungan kabel dilabelkan bagi membolehkan pengenalan fizikal dan pemeriksaan kabel terlibat; dan e) mendapatkan nasihat pakar berkaitan kaedah pengurusan risiko yang timbul daripada insiden atau kerosakan kabel.	ICTSO, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pihak Ketiga

3.13 PENYELENGGARAAN PERALATAN

Objektif:

Memastikan semua peralatan berkaitan perkhidmatan ICT diselenggarakan untuk mengelakkan gangguan operasi MPS.

3.13.1 Penyelenggaraan Peralatan	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) peralatan yang diselenggarakan hendaklah mematuhi spesifikasi dan tempoh penyelenggaraan yang ditetapkan oleh pengeluar; b) pemantauan pelaksanaan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; c) memastikan peralatan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; d) menyimpan rekod penyelenggaraan pencegahan dan pemulihan; e) melaksanakan kawalan yang sesuai bagi tujuan penyelenggaraan pencegahan dan pemulihan sama ada di dalam atau luar premis MPS; f) menyelia kerja-kerja penyelenggaraan yang dilakukan oleh Pihak Ketiga; g) mengawal akses bagi penyelenggaraan yang dilaksanakan secara jarak jauh (remote); h) melaksanakan kawalan keselamatan ke atas penyelenggaraan peralatan di luar premis MPS; i) menyemak dan menguji semua peralatan selepas proses penyelenggaraan bagi memastikan tiada pengubahsuaian yang tidak dibenarkan; dan j) melaksanakan kaedah yang bersesuaian untuk pelupusan atau penggunaan semua peralatan.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pihak Ketiga

3.14 PELUPUSAN ATAU PENGGUNAAN SEMULA PERALATAN

Objektif:

Memastikan kaedah pelupusan dan penggunaan semula peralatan dilaksanakan mengikut peraturan yang berkuat kuasa.

3.14.1 Pelupusan Peralatan	Tanggungjawab
a) maklumat pelupusan hendaklah direkodkan, dikemas kini dan dilaporkan mengikut keperluan; b) warga MPS tidak dibenarkan melakukan perkara-perkara seperti berikut: i. menyimpan mana-mana peralatan yang hendak dilupuskan untuk tujuan peribadi;	ICTSO, Pegawai Aset ICT, Warga MPS

ii. menanggalkan komponen peralatan seperti RAM, *hard disk*, *motherboard* dan sebagainya;
iii. melupuskan sendiri tanpa kelulusan; dan
iv. memindah keluar peralatan yang dilupuskan tanpa kelulusan.

3.14.2 Penggunaan Semula Peralatan	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) semua maklumat di dalam peralatan hendaklah disanitasi atau dihapuskan secara selamat terlebih dahulu sebelum penggunaan semula atau dipindah milik; b) maklumat peralatan yang diguna semula atau dipindah milik hendaklah direkodkan dan dikemas kini; c) warga MPS tidak dibenarkan daripada melakukan perkara-perkara seperti yang berikut: i. menyimpan peralatan berlebihan untuk tujuan peribadi; ii. menanggalkan komponen peralatan seperti RAM, *hard disk*, *motherboard* dan sebagainya; dan iii. menggunakan semula peralatan tanpa kelulusan.	ICTSO, Pegawai Aset ICT, Warga MPS

BAB 4
KAWALAN TEKNOLOGI

BAB 4 | KAWALAN TEKNOLOGI

4.1 ASET ICT PENGGUNA

Objektif:

Melindungi maklumat yang terdapat dalam aset ICT pengguna.

4.1.1 Pengurusan Aset ICT

Tanggungjawab

ICTSO, Pengguna

Perkara yang perlu dipatuhi adalah seperti yang berikut:

a) memastikan jenis dan klasifikasi maklumat yang boleh diakses, diproses atau disimpan dalam aset ICT pengguna;
b) memastikan semua aset ICT pengguna didaftarkan;
c) memastikan pengguna bertanggungjawab ke atas aset ICT;
d) memastikan perisian yang boleh dipasang pada aset ICT pengguna telah mendapat kebenaran;
e) memastikan aset ICT pengguna dikonfigurasi dengan versi perisian atau patches terkini;
f) menetapkan peraturan bagi sambungan ke rangkaian awam, atau rangkaian lain di luar premis menggunakan aset ICT pengguna;
g) memastikan pengguna mematuhi kawalan capaian penggunaan aset ICT pengguna;
h) memastikan pengguna menggunakan kata laluan bagi penyimpanan maklumat terperingkat MPS;
i) memastikan aset ICT pengguna mempunyai perisian antivirus;
j) memastikan peraturan berkaitan remote disabling, deletion atau lockout dipatuhi;
k) memastikan pengguna melaksanakan sandaran bagi maklumat yang disimpan di dalam aset ICT;
l) menggunakan perkhidmatan web dan aplikasi yang dibenarkan sahaja;
m) memastikan pengasingan (hard disk partition) data dan perisian pada aset ICT pengguna; dan
n) MPS berhak untuk mengambil tindakan yang sesuai seperti penamatan akses sekiranya didapati tidak mematuhi peraturan dalam polisi ini.

4.1.2 Tanggungjawab Pengguna

Tanggungjawab

Pengguna

Pengguna aset ICT MPS hendaklah mengambil kira perkara seperti yang berikut:

a) *log out* perisian aplikasi apabila selesai tugas;
b) mengaktifkan mekanisme pengunci atau kawalan yang bersesuaian seperti *password protected screen saver*;
c) log out kerangka utama, *server* dan komputer pejabat apabila sesi bertugas selesai; dan

d) melindungi aset ICT daripada kecurian atau kecuaian.

4.1.3 Penggunaan aset ICT Persendirian atau Bring Your Own Device (BYOD)	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mengasingkan penggunaan bagi tujuan peribadi dan tugasan rasmi. Instalasi perisian yang dibekalkan oleh MPS pada aset ICT persendirian hendaklah mendapatkan kelulusan Pengurus ICT; b) membenarkan akses kepada maklumat yang berkaitan dengan tugasan rasmi dan menghapuskan data rahsia rasmi pada aset ICT persendirian apabila tidak digunakan lagi; c) memastikan hak harta intelek adalah di bawah tanggungjawab pengguna aset ICT persendirian; d) penyalahgunaan aset ICT persendirian adalah di bawah tanggungjawab pengguna sendiri; e) MPS tidak bertanggungjawab ke atas sebarang kerosakan sistem operasi atau perkakasan aset ICT persendirian; dan f) MPS menghormati privasi aset ICT persendirian dengan mengambil langkah pencegahan yang terbaik untuk memastikan keselamatan maklumat. MPS mempunyai hak untuk menjejaki dan meminta akses kepada aset ICT persendirian sekiranya terdapat pelanggaran keselamatan maklumat yang dikenal pasti.	Pengurus Aset ICT, Warga MPS

4.1.4 Sambungan Rangkaian Tanpa Wayar untuk aset ICT	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) a) mengkonfigurasi rangkaian tanpa wayar aset ICT untuk melindungi daripada protokol yang mempunyai kelemahan; b) b) menetapkan bandwidth rangkaian yang bersesuaian bergantung kepada jenis akses; dan c) c) tidak mendedahkan identiti dan kata laluan sambungan rangkaian tanpa wayar.	Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pengguna

4.2 KEBENARAN HAK AKSES

Objektif:

Memastikan akses pengguna, komponen perisian dan perkhidmatan yang disediakan hanya diberikan kepada pengguna yang dibenarkan.

4.2.1 Hak Capaian	Tanggungjawab

Prosedur penetapan dan penggunaan ke atas hak akses hendaklah mengambil kira perkara berikut:

ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pengguna

a) mengenal pasti pengguna yang memerlukan hak akses untuk sistem aplikasi, sistem pengoperasian dan pengurusan pangkalan data;
b) penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat, atas prinsip perlu mengetahui (need-to-know-basis);
c) keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pegawai dan kakitangan yang dibenarkan sahaja;
d) memastikan pengguna mengetahui tanggungjawab hak akses yang diterima;
e) memastikan perbezaan peranan akses untuk pentadbir dan pengguna;
f) sekiranya berlaku perubahan struktur organisasi di MPS, penetapan dan penggunaan ke atas hak akses perlu disemak semula berdasarkan keperluan skop tugas;
g) melarang penggunaan ID pentadbir seperti root bagi akses ke konfigurasi sistem;
h) memberikan hak akses sementara untuk perubahan atau penyelenggaraan yang dilaksanakan oleh Pihak Ketiga;
i) merekodkan semua log masuk untuk kegunaan jejak audit;
j) tidak berkongsi ID pengguna dengan orang lain;
k) menggunakan ID pengguna berdasarkan skop tugas (melaksanakan tugasan harian) dan tidak menggunakan ID pentadbir; dan
l) sebarang perubahan mestilah mendapat kebenaran secara bertulis dan direkodkan.

4.3 KAWALAN AKSES MAKLUMAT

Objektif:

Memastikan hanya akses yang dibenarkan ke atas maklumat dan aset yang berkaitan.

4.3.1 Akses Maklumat dan Aset yang Berkaitan	Tanggungjawab

Bagi memastikan kawalan had akses ke atas maklumat dan aset yang berkaitan, perkara berikut hendaklah dipatuhi:

ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian,

a) tidak membenarkan akses ke maklumat terperingkat bagi pengguna yang tidak dibenarkan; b) menyediakan konfigurasi untuk mengawal akses maklumat di dalam sistem, aplikasi dan perkhidmatan; c) mengawal data yang boleh diakses mengikut kategori pengguna; d) mengawal individu dan kumpulan yang telah dikenal pasti mempunyai akses seperti read, write, delete dan execute; e) menyediakan kawalan fizikal atau kawalan hak akses untuk aplikasi data atau sistem; f) aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; g) mengehadkan kemasukan kata laluan bagi capaian kepada aplikasi adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian akan disekat sehingga ID capaian diaktifkan semula; dan h) akses maklumat melalui capaian jarak jauh adalah tidak digalakkan, penggunaannya terhad kepada perkhidmatan yang diberi kebenaran sahaja.	Pegawai Aset ICT

4.3.2 Akses Maklumat Rahsia Rasmi	**Tanggungjawab**
Untuk melindungi maklumat rahsia rasmi yang kritikal kepada MPS, pengurusan akses perlu mematuhi perkara berikut: a) melaksanakan kawalan untuk akses maklumat mengikut tempoh masa yang dibenarkan; b) melaksanakan kawalan untuk akses maklumat yang diberikan kepada Pihak Ketiga; c) memantau dan menguruskan semua penggunaan atau penyebaran maklumat secara *real-time*; d) maklumat hendaklah dilindungi daripada perubahan, penyalinan dan pengedaran yang tidak dibenarkan (termasuk percetakan); dan e) merekodkan sebarang perubahan ke atas maklumat tersebut.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

4.3.3 Kawalan Pengurusan Akses Maklumat dan Aset yang Berkaitan	**Tanggungjawab**
Perkara yang perlu dilaksanakan untuk melindungi maklumat adalah: a) menetapkan kawalan kebenaran akses berdasarkan identiti, peranti, lokasi atau aplikasi; b) menetapkan klasifikasi maklumat yang perlu dilindungi; c) mewujudkan proses pemantauan dan pelaporan; d) mendapatkan pengesahan dan kebenaran untuk mengakses maklumat; e) mengehadkan akses seperti mempunyai had masa yang dibenarkan; f) menggunakan enkripsi untuk melindungi maklumat (jika perlu); g) menetapkan kebenaran untuk mencetak maklumat (jika perlu); dan	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

h) menghantar pemakluman jika terdapat insiden penyalahgunaan maklumat.

4.4 AKSES KEPADA KOD SUMBER

Objektif:

Akses kepada kod sumber dan persekitaran pembangunan hendaklah dikawal. Ini adalah untuk mengelakkan perubahan yang tidak dibenarkan bagi mengekalkan kerahsiaan.

4.4.1 Kawalan Kod Sumber	Tanggungjawab

Perkara berikut perlu dipatuhi untuk mengawal akses kepada kod sumber bagi meminimumkan potensi kegagalan sistem aplikasi:

Pentadbir Sistem ICT, Pihak Ketiga

a) menguruskan akses kepada kod sumber dan program;
b) source libraries berdasarkan prosedur yang ditetapkan;
c) membenarkan akses read dan write mengikut kebenaran dan menguruskan risiko penyalahgunaan kod sumber;
d) pengemaskinian kod sumber serta pemberian akses kepada kod sumber perlu mematuhi prosedur kawalan perubahan yang diluluskan;
e) tidak membenarkan pengaturcaraan sistem mempunyai akses secara terus kepada repositori kod sumber tetapi melalui perisian pembangunan yang mengawal aktiviti dan kebenaran kepada kod sumber;
f) menyimpan senarai kod sumber di tempat selamat dan memberikan kawalan akses kepada individu yang dibenarkan;
g) menyimpan log audit akses dan perubahan kepada kod sumber; dan
h) memastikan kod sumber bagi sistem aplikasi atau perisian yang dibekalkan oleh Pihak Ketiga ketiga menjadi hak milik MPS.

4.5 PENGESAHAN SELAMAT (*SECURE AUTHENTICATION*)

Objektif:

Memastikan pengguna atau individu menggunakan pengesahan yang sah untuk akses kepada sistem aplikasi dan perkhidmatan yang disediakan.

4.5.1 Pengesahan Prosedur Log Masuk yang Selamat	Tanggungjawab

Bagi sistem yang kritikal, penggunaan multi-factor authentication adalah digalakkan. Prosedur log masuk perlu mematuhi perkara seperti yang berikut:

ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

a) memaparkan maklumat hanya selepas log masuk berjaya;
b) memaparkan notis amaran sistem hanya boleh diakses oleh pengguna yang sah;

c) tidak memaparkan mesej kesilapan semasa log masuk;
d) mengesahkan maklumat identiti yang dikunci masuk (*key-in*) untuk log masuk mencukupi dan betul;
e) melindungi ID pengguna dan kata laluan daripada cubaan log masuk *brute force*;
f) merekodkan jejak audit log masuk yang berjaya dan gagal;
g) menghantar notis keselamatan jika ada potensi percubaan atau pencerobohan ke atas log masuk yang dikesan;
h) tidak memaparkan kata laluan semasa log masuk;
i) tidak menghantar kata laluan dalam clear text melalui rangkaian;
j) menamatkan sesi yang tidak aktif dalam tempoh masa yang ditetapkan; dan
k) mengehadkan tempoh masa sambungan bagi sistem yang kritikal.

4.6 PENGURUSAN KAPASITI

Objektif:

Memastikan penggunaan sumber, seperti tenaga, ruang penyimpanan, atau sumber manusia, akan dipantau dan diubah suai agar sesuai dengan keperluan kapasiti semasa dan keperluan pada masa hadapan.

4.6.1 Pengurusan Kapasiti	Tanggungjawab
Perkara seperti berikut perlu diambil kira: a) kapasiti sistem ICT hendaklah dirancang, diurus dan dikawal dengan terperinci bagi memastikan keperluannya adalah mencukupi serta bersesuaian untuk pembangunan dan operasi sistem ICT semasa atau pada masa akan datang; b) keperluan kapasiti perlu mengambil kira ciri-ciri keselamatan bagi meminimumkan risiko gangguan kepada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang; c) pemantauan kapasiti sistem ICT perlu dilaksanakan untuk memastikan ketersediaan dan kecekapan sistem; d) pengujian tekanan (*stress test*) ke atas sistem dan perkhidmatan hendaklah dilaksanakan untuk memastikan kapasiti mencukupi terutamanya semasa waktu puncak; dan e) dokumen pengurusan kapasiti sumber perlu disediakan terutamanya untuk sistem kritikal.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.6.2 Peningkatan Kapasiti	Tanggungjawab
Perkara berikut perlu dipatuhi untuk meningkatkan kapasiti sumber: a) memastikan sumber manusia mencukupi;	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

b) menyediakan kemudahan dan ruang kerja yang kondusif;
c) melaksanakan perolehan bagi kapasiti yang tidak mencukupi agar sesuai dengan keperluan semasa dan masa hadapan; dan
d) menggunakan pengkomputeran awan (*cloud computing*) sekiranya perlu.

4.6.3 Pengurangan Kapasiti	Tanggungjawab
Perkara berikut perlu dipatuhi untuk mengurangkan kapasiti sumber: a) menghapuskan data lama (*disk space*) yang tidak digunakan lagi; b) melupuskan rekod fizikal mengikut jadual pelupusan rekod jabatan yang telah diluluskan; c) melupuskan sistem aplikasi, pangkalan data atau perkhidmatan ICT yang tidak digunakan lagi; d) mengoptimumkan proses *batch* dan *scheduler*; e) mengoptimumkan kod aplikasi dan kuiri pangkalan data; dan f) mengehadkan *bandwidth* bagi perkhidmatan ICT yang menggunakan kapasiti tinggi (jika perlu).	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.7 PERLINDUNGAN TERHADAP PERISIAN HASAD (*MALWARE*)

Objektif:

Memastikan perisian dan aset berkaitan ICT dilindungi daripada perisian hasad (*malware*). Perlindungan terhadap perisian hasad hendaklah berdasarkan maklumat pengesanan dan pembaikan perisian hasad tersebut, kesedaran keselamatan, akses sistem yang sesuai serta kawalan pengurusan perubahan.

4.7.1 Perlindungan Daripada Perisian Hasad	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) melaksanakan kawalan untuk mencegah dan mengesan perisian yang tidak sah; b) melaksanakan kawalan untuk mencegah dan mengesan laman web yang tidak diketahui dan disyaki tidak selamat; *c) mengurangkan kelemahan yang boleh dieksploitasi oleh perisian hasad (malware);* d) melaksanakan pengesahan ke atas perisian dan maklumat sistem secara berkala terutamanya yang melibatkan sistem kritikal; e) mewujudkan langkah-langkah perlindungan terhadap risiko daripada fail dan perisian yang diperoleh sama ada melalui rangkaian luar atau pada mana-mana medium lain;	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pengguna

f) memastikan perisian keselamatan yang digunakan sentiasa dikemas kini untuk mengimbas komputer dan media storan elektronik. Pengimbasan yang dilaksanakan merangkumi:
   i. mengimbas sebarang data yang diterima melalui rangkaian atau melalui sebarang bentuk media storan elektronik sebelum digunakan;
   ii. mengimbas e-mel dan lampiran yang dimuatturun sebelum digunakan; dan
   iii. mengimbas laman web yang diakses.
g) menetapkan konfigurasi perisian keselamatan untuk mengesan ancaman risiko;
   i. menyediakan polisi berdasarkan amalan terbaik (best practise); dan
   ii. teknik untuk menyekat serangan perisian hasad.
h) melindungi daripada serangan perisian hasad semasa proses penyelenggaraan;
i) memberi kebenaran secara sementara atau kekal untuk menutup perisian pengesanan serangan hasad sekiranya ianya mengganggu operasi harian dengan mendapatkan kelulusan dan direkodkan;
j) menyediakan proses pemulihan dari serangan *malware*, termasuklah data dan perisian *backup*;
k) mengasingkan persekitaran yang berisiko akan menghadapi bencana;
l) menyediakan prosedur kawalan serangan perisian hasad termasuk latihan, proses pemulihan dan pelaporan;
m) menyediakan program kesedaran atau latihan mengenai ancaman perisian berbahaya dan cara mengendalikannya;
n) melaksanakan pengumpulan maklumat perisian hasad yang terkini untuk langkah-langkah pencegahan;
o) mengesahkan maklumat yang berkaitan dengan serangan hasad daripada sumber yang sahih; dan
p) memasukkan klausa tanggungan dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya.

4.8 PENGURUSAN TEKNIKAL KE ATAS KERENTANAN

Objektif:

Mendapatkan maklumat tentang kelemahan yang mungkin wujud dalam sistem maklumat yang digunakan seterusnya mencegah eksploitasi kerentanan teknikal dalam sistem tersebut.

4.8.1 Pmengenalpasti Kerentanan Teknikal	Tanggungjawab
Inventori aset hendaklah mengandungi maklumat sistem seperti nama sistem, perisian yang digunakan, nombor versi dan pemilik yang bertanggungjawab ke atas perisian tersebut.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

Perkara yang perlu dipatuhi adalah seperti yang berikut:

a) menetapkan peranan dan tanggungjawab untuk mengurus kelemahan teknikal seperti pemantauan kelemahan, penilaian risiko, pengemaskinian patches dan lain-lain;
b) mengenal pasti sumber maklumat yang akan digunakan untuk mengesan kelemahan teknikal yang berkaitan dan sentiasa mengemas kini senarai aset sekiranya ada perubahan teknologi atau perisian yang digunakan;
c) memastikan kandungan kontrak perjanjian dengan Pihak Ketiga merangkumi pengurusan dan pelaporan penemuan kelemahan teknikal yang berkaitan;
d) menjalankan pengujian keselamatan untuk mengenal pasti kelemahan yang ada dan memastikan baik pulih dilaksanakan;
e) merancang, merekod dan menguji penilaian keselamatan secara berkala oleh Pentadbir ICT MPS atau Pihak Ketiga yang berkelayakan; dan
f) memastikan penggunaan libraries dan kod sumber luar yang selamat.

4.8.2 Penilaian Kelemahan Teknikal	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) menyemak dan mengesahkan laporan pengujian penilaian keselamatan; dan b) mengenal pasti risiko dan mengambil tindakan pemulihan ke atas penemuan daripada pengujian keselamatan yang telah dilaksanakan.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.8.3 Panduan Menangani Kelemahan Teknikal	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mengambil tindakan yang bersesuaian mengikut tempoh masa yang ditetapkan setelah kelemahan dikenal pasti; b) tindakan mengatasi kelemahan teknikal berdasarkan kategori risiko merujuk kepada pengurusan perubahan atau prosedur pengurusan pengendalian insiden keselamatan; c) menggunakan perisian yang terkini daripada sumber yang sah; d) menguji dan menilai pengemaskinian patches yang telah dilaksanakan sebelum dipasang pada persekitaran sebenar; e) memastikan patches sentiasa dikemas kini terutamanya kepada sistem kritikal di MPS; f) menguji keberkesanan ke atas tindakan pemulihan yang telah dilaksanakan; g) sekiranya pengemaskinian tidak berjaya dilaksanakan, kawalan berikut perlu dipatuhi: i. menggunakan cadangan lain yang diberikan oleh sumber yang sahih (sekiranya ada); ii. menutup perkhidmatan yang terdedah akibat daripada kelemahan teknikal;	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

iii. menambah polisi kawalan akses di segmen rangkaian untuk melindungi sistem, peranti atau aplikasi yang terdedah daripada serangan;
iv. meningkatkan pemantauan untuk mengesan serangan sebenar;
v. meningkatkan kesedaran berkaitan dengan kelemahan teknikal; dan

h) proses pengurusan kelemahan teknikal harus dipantau dan dinilai secara berkala.

4.9 PENGURUSAN KONFIGURASI

Objektif:

Memastikan konfigurasi perkakasan, perisian, perkhidmatan dan rangkaian ICT berfungsi dengan baik dan mengambil kira aspek keselamatan.

4.9.1 Pengurusan Penetapan Konfigurasi	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) memastikan konfigurasi semua perkhidmatan dan perkakasan ditetapkan mengikut keperluan; dan b) peranan, tanggungjawab dan prosedur perlu disediakan untuk memastikan kawalan ke atas perubahan konfigurasi.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.9.2 Amalan Baik (***Best Practise***)	Tanggungjawab
Templat standard untuk konfigurasi perkakasan, perisian, perkhidmatan dan rangkaian perlu disediakan seperti yang berikut: a) menggunakan panduan umum atau amalan terbaik yang tersedia daripada templat Pihak Ketiga atau jabatan lain; b) mempertimbangkan tahap perlindungan yang diperlukan untuk menentukan tahap keselamatan yang mencukupi; c) menyokong dasar keselamatan maklumat yang sedang berkuat kuasa; d) mempertimbangkan keupayaan dan kebolehgunaan konfigurasi keselamatan mengikut keperluan; e) penyeragaman masa (*clock synchronization*); f) menukar kata laluan asal selepas proses instalasi dan penyemakan parameter keselamatan; g) menyediakan *log off* secara automatik mengikut tempoh yang ditetapkan; h) mematuhi terma dan syarat penggunaan lesen; dan i) memastikan salinan sandaran maklumat, perisian dan sistem diselenggara serta diuji secara berkala.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.9.3 Pengurusan Sandaran	Tanggungjawab
Melaksanakan proses sandaran dan pemulihan sama ada maklumat di Bilik *Server* Utama, Pusat Pemulihan Bencana atau lokasi yang dibenarkan serta perlu memastikan perkara berikut dipatuhi: a) memastikan prosedur sandaran dan pemulihan direkodkan dengan lengkap; b) memastikan keperluan keselamatan maklumat bagi proses sandaran dan pemulihan dipenuhi ke atas sistem kritikal MPS yang telah dikenal pasti; c) memastikan salinan sandaran disimpan di lokasi dan jarak yang selamat untuk mengelakkan sebarang kerosakan akibat bencana di Bilik *Server* Utama MPS; d) memastikan perlindungan yang sesuai diberikan ke atas maklumat sandaran selari dengan Bilik *Server* Utama MPS; e) menguji sistem sandaran dan pemulihan bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; f) menetapkan tempoh simpanan maklumat sandaran yang disimpan dan maklumat tersebut perlu dihapus setelah melepasi tempoh yang ditetapkan; g) menyediakan prosedur pengurusan sandaran dan pemulihan; h) membuat aktiviti klon ke atas semua maklumat dan sistem perisian mengikut keperluan atau apabila berlaku perubahan versi; dan	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.10 PENGHAPUSAN MAKLUMAT

Objektif:

Memastikan penghapusan maklumat dilaksanakan mematuhi keperluan undang- undang dan peraturan yang berkuat kuasa.

4.10.1 Penghapusan Maklumat	Tanggungjawab
Perkara berikut hendaklah dipatuhi semasa menghapus maklumat pada sistem, aplikasi dan perkhidmatan: a) memilih kaedah penghapusan yang sesuai; b) merekodkan keputusan penghapusan sebagai bukti; c) bukti penghapusan maklumat perlu disediakan oleh pembekal sekiranya menggunakan perkhidmatan pembekal untuk penghapusan maklumat; dan d) memastikan klausa penghapusan maklumat dimasukkan dalam perjanjian bersama pembekal bagi memastikan penguatkuasaan semasa dan selepas penamatan perkhidmatan.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.10.2 Kaedah Penghapusan Maklumat	Tanggungjawab
Kaedah penghapusan maklumat perlu dipatuhi berdasarkan peraturan dan perundangan yang berkaitan. Maklumat terperingkat perlu dihapuskan sekiranya tidak diperlukan lagi mengikut kaedah berikut: a) menghapuskan versi, salinan dan fail sementara yang tidak boleh digunakan lagi; b) menggunakan pembekal yang diluluskan dan diperakui untuk melaksanakan perkhidmatan pelupusan; c) menggunakan perisian yang diiktiraf untuk pelupusan maklumat; d) menggunakan mekanisme yang bersesuaian untuk melupuskan media storan; e) penyedia perkhidmatan pengkomputeran awan perlu melaksanakan penghapusan maklumat mengikut peraturan yang ditetapkan; dan f) semasa peralatan dipulangkan kepada pembekal, media storan perlu disanitasi dan data dihapuskan untuk mengelakkan maklumat terperingkat terdedah.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.11 PENYEMBUNYIAN DATA (*DATA MASKING*)

Objektif:

Memastikan paparan data sensitif dihadkan mengikut peraturan, keperluan organisasi dan perundangan yang berkuat kuasa.

4.11.1 Teknik Penyembunyian Data	Tanggungjawab
Antara teknik untuk penyembunyian data dalam sistem aplikasi termasuk: a) enkripsi (pengguna yang mempunyai *decryption key* sahaja boleh melihat data tersebut); b) menggantikan data dengan “Null” atau menghapuskan salah satu huruf / nombor (menghalang pengguna yang tidak dibenarkan untuk melihat mesej penuh); c) mengubah nombor atau tarikh dari nilai sebenarnya; d) penggantian data (menukar satu nilai kepada yang lain untuk menyembunyikan data sensitif); dan e) menukar nilai dengan nilai *hash* (*hash value*).	ICTSO, Pentadbir Sistem ICT

4.11.2 Pelaksanaan Penyembunyian Data	Tanggungjawab
Semasa melaksanakan penyembunyian data, perkara berikut perlu dipatuhi: a) tidak semua data diberikan akses kepada pengguna. Sistem aplikasi hanya memaparkan data minimum kepada pengguna;	ICTSO, Pentadbir Sistem ICT

b) keperluan perundangan atau peraturan yang berkuat kuasa hendaklah dipatuhi;
c) menyediakan kawalan akses kepada data yang diproses; dan
d) menyediakan jejak audit untuk merekodkan penyediaan dan penerimaan data yang diproses.

4.12 PENCEGAHAN KEBOCORAN DATA (*DATA LEAKAGE PREVENTION*)

Objektif:

Memastikan langkah-langkah pencegahan kebocoran data dilaksanakan pada sistem, rangkaian dan sebarang peranti lain yang memproses, menyimpan atau menghantar maklumat terperingkat.

4.12.1 Pelaksanaan Pencegahan Kebocoran Data	Tanggungjawab
Perkara yang perlu dilaksanakan adalah seperti yang berikut: a) mengenal pasti dan mengklasifikasikan maklumat untuk melindungi kebocoran maklumat; b) memantau punca atau saluran kebocoran data; c) melaksanakan langkah pencegahan untuk mengelakkan kebocoran data; d) mengehadkan capaian pengguna; dan e) memastikan proses sandaran maklumat dilindungi seperti penyulitan (*encryption*) dan kawalan akses.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.13 SANDARAN MAKLUMAT (*INFORMATION BACKUP*)

Objektif:

Memastikan salinan sandaran maklumat, perisian dan sistem diselenggara serta diuji secara berkala.

4.13.1 Pengurusan Sandaran	Tanggungjawab
Melaksanakan proses sandaran dan pemulihan maklumat di Bilik *Server* Utama MPS, Pusat Pemulihan Bencana atau lokasi yang dibenarkan serta perlu memastikan perkara berikut dipatuhi: a) memastikan prosedur sandaran dan pemulihan direkodkan dengan lengkap; b) memastikan keperluan keselamatan maklumat bagi proses sandaran dan pemulihan dipenuhi ke atas sistem kritikal MPS yang telah dikenal pasti; c) memastikan salinan sandaran disimpan di lokasi dan jarak yang selamat untuk mengelakkan sebarang kerosakan akibat bencana di Bilik *Server* Utama MPS; d) memastikan perlindungan yang sesuai diberikan ke atas maklumat sandaran selari dengan Bilik *Server* Utama MPS;	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

e) menguji sistem sandaran dan pemulihan bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan;
f) menetapkan tempoh simpanan maklumat sandaran yang disimpan dan maklumat tersebut perlu dihapus setelah melepasi tempoh yang ditetapkan;
g) menyediakan prosedur pengurusan sandaran dan pemulihan;
h) membuat aktiviti klon ke atas semua maklumat dan sistem perisian mengikut keperluan atau apabila berlaku perubahan versi; dan
i) menyimpan salinan sandaran sekurang-kurangnya di dalam dua (2) media storan yang berasingan.

4.14 REDUNDANCY BAGI KEMUDAHAN PEMPROSESAN MAKLUMAT

Objektif:

Memastikan ketersediaan kemudahan operasi ICT.

4.14.1 Ketersediaan Kemudahan Pemprosesan Maklumat	Tanggungjawab
Mengenal pasti dan mereka bentuk arkitektur sistem dengan kemudahan *redundancy* yang bersesuaian. Perkara yang perlu dipatuhi adalah seperti berikut: a) menyediakan ketersediaan *redundancy* rangkaian bagi kemudahan operasi ICT; b) menyediakan lebih daripada satu (1) kemudahan pusat data yang berlainan lokasi; c) menggunakan sumber punca kuasa elektrik secara *redundancy*; d) menggunakan perkakasan atau perisian yang mempunyai fungsi *automatic load balancing*; dan e) mempunyai komponen pendua dalam perkakasan server atau rangkaian.	ICTSO, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.15 MEREKODKAN LOG (*LOGGING*)

Objektif:

Memastikan log bagi aktiviti, pengecualian, kecacatan, dan peristiwa lain yang berkaitan harus dihasilkan, disimpan, dilindungi, dan dianalisis bagi menghalang daripada akses yang tidak dibenarkan.

4.15.1 Polisi Log Aktiviti	Tanggungjawab
Aktiviti log perlu mengandungi perkara seperti yang berikut: a) ID pengguna;	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server*

b) aktiviti sistem; c) tarikh, masa dan butiran aktiviti yang dilakukan; d) percubaan gagal dan berjaya akses masuk ke sistem; e) perubahan konfigurasi sistem; f) aktiviti sistem pengoperasian; dan g) menyimpan log audit untuk tempoh masa yang dipersetujui.	Utama MPS / Rangkaian

4.15.2 Kawalan Perlindungan Log	Tanggungjawab
Semua pengguna yang mempunyai akses tidak dibenarkan memadam atau menyahaktifkan rekod log. Kawalan perlindungan ke atas rekod log bertujuan untuk melindungi daripada perubahan yang tidak dibenarkan ke atas rekod log seperti yang berikut: a) merekodkan perubahan yang dilakukan; b) fail log yang diubah atau dihapus; c) Kegagalan merekodkan aktiviti log sekiranya media storan penuh; d) melindungi maklumat log daripada capaian yang tidak dibenarkan; e) capaian ke atas log fail *server* hanya kepada pengguna yang dibenarkan sahaja; f) menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; g) sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT atau Pentadbir Bilik *Server* Utama MPS / Rangkaian hendaklah melaporkan kepada ICTSO dan CDO; h) merekodkan dan mengambil tindakan ke atas kesalahan, kesilapan dan/atau penyalahgunaan log; dan i) memastikan masa (*time stamp*) dalam sistem aplikasi diselaraskan dengan waktu rekod log.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.15.3 Analisis Log	Tanggungjawab
Rekod log perlu dianalisis untuk mengenal pasti aktiviti yang boleh menyebabkan sistem aplikasi dicerobohi oleh pihak yang tidak dibenarkan. Aktiviti analisis log perlu mengandungi perkara berikut: a) melaksanakan analisis log; b) merekodkan maklumat bagi setiap insiden atau kejadian keselamatan; c) pengecualian yang dibenarkan telah dikenal pasti dalam polisi; d) keputusan hasil analisis; e) menyemak percubaan yang berjaya atau gagal kepada perkakasan rangkaian atau server; dan	ICTSO, CERT MPS, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

f) memantau, menyemak dan menyelaras kesemua rekod log fizikal untuk mendapatkan analisis yang lebih tepat.

4.15.4 Plog Pentadbir dan Pengguna	Tanggungjawab
Semua log aktiviti pentadbir dan pengguna sistem direkodkan dan log hendaklah dilindungi serta disemak secara berkala. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh sekurang-kurangnya satu tahun atau tempoh yang dipersetujui bagi membantu mengenal pasti kejadian insiden keselamatan; dan b) sekiranya wujud aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT atau Pentadbir Bilik *Server* Utama MPS / Rangkaian hendaklah melaporkan kepada CERT MPS.	ICTSO, CERT MPS, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.16 AKTIVITI PEMANTAUAN

Objektif:

Memastikan rangkaian, sistem, dan aplikasi dipantau bagi sebarang aktiviti anomali yang meragukan supaya tindakan yang sesuai boleh diambil.

4.16.1 Aspek Pemantauan	Tanggungjawab
Tahap pemantauan ditetapkan mengikut keperluan keselamatan maklumat, dasar dan polisi undang-undang yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) trafik keluar masuk rangkaian dan sistem aplikasi; b) akses ke sistem, server, peranti rangkaian dan sebagainya; c) fail konfigurasi bagi aplikasi dan peralatan kritikal; d) log daripada peranti keselamatan; e) log aktiviti sistem aplikasi dan rangkaian; f) memastikan kod sumber yang sahih digunakan dan tidak diubah suai; dan g) penggunaan dan keupayaan sumber seperti CPU, *memory*, dan *bandwidth*.	ICTSO, CERT MPS, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.16.2 Pemantauan Aktiviti Anomali	Tanggungjawab
Perkara yang perlu dipantau adalah seperti yang berikut: a) proses yang ditamatkan tanpa kebenaran;	ICTSO, CERT MPS, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

b) trafik aktiviti yang mengandungi perisian hasad atau meragukan daripada alamat domain atau IP *Address* yang telah dikenal pasti terjejas;
c) ciri-ciri serangan yang dikenal pasti seperti *Distributed Denial-of-Services* (DDOS);
d) aktiviti sistem yang luar biasa seperti *process injection*;
e) proses yang melebihi kebiasaan dan menyebabkan kesesakan trafik;
f) akses yang tidak dibenarkan ke atas sistem;
g) pengimbasan tanpa kebenaran ke atas sistem dan rangkaian;
h) cubaan akses sama ada berjaya atau tidak kepada kemudahan ICT yang dilindungi seperti *server* DNS;
i) aktiviti pengguna atau sistem yang luar biasa daripada kebiasaan; dan
j) serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phishing*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*).

4.16.3 Kawalan Pemantauan Aktiviti Anomali	Tanggungjawab
Perkara yang boleh dilaksanakan dalam pemantauan aktiviti anomali adalah seperti yang berikut: a) memanfaatkan atau menggunakan sistem *threat intelligence*; b) menggunakan kaedah senarai yang disekat atau dibenarkan; c) menggunakan penilaian teknikal keselamatan untuk mengenal pasti garis panduan ciri keselamatan yang dibenarkan; d) menggunakan sistem pemantauan keupayaan untuk mengesan trafik yang meragukan; dan e) menggunakan sistem log untuk tujuan pemantauan.	ICTSO, CERT MPS, Pentadbir Sistem ICT, Pentadbir Bilik Server Utama MPS / Rangkaian

4.17 PENYELARASAN JAM

Objektif:

Memastikan semua aktiviti keselamatan serta data lain yang direkodkan selari dengan Waktu Piawai Malaysia (*Malaysia Standard Time*, MST).

4.17.1 Penyelarasan Waktu	Tanggungjawab
Perkara yang boleh dilaksanakan dalam penyelarasan waktu adalah seperti berikut: a) memastikan waktu bagi sistem pemprosesan maklumat atau peralatan hendaklah diselaraskan dengan Waktu Piawai Malaysia (MST); dan b) penyelarasan waktu bagi perkhidmatan awan hendaklah mengikut Penyedia Perkhidmatan Awan (*Cloud Service Provider*) dan perbezaannya perlu dipantau dan direkodkan untuk mengurangkan risiko percanggahan.	ICTSO, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.18 PENGGUNAAN PROGRAM UTILITI KHAS

Objektif:

Memastikan penggunaan program utiliti tidak menjejaskan kawalan keselamatan maklumat bagi sistem aplikasi.

4.18.1 Penggunaan Program Utiliti Khas	Tanggungjawab
Panduan seperti di bawah perlu dipatuhi: a) mengehadkan dan mengawal bilangan pengguna yang dibenarkan untuk menggunakan program utiliti; b) memastikan penggunaan ID yang unik untuk pengesahan dan kebenaran akses; c) mengenal pasti dan mendokumentasikan program utiliti yang diberikan kebenaran; d) membenarkan penggunaan program utiliti pada waktu luar jangka (*ad-hoc*); e) menghapuskan dan menutup program utiliti yang tidak berkaitan; f) mengehadkan ketersediaan program utiliti; g) menyimpan log program utiliti; dan h) penggunaan program utiliti yang membebankan kapasiti (*bandwidth*) rangkaian perlu dihadkan.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

4.19 INSTALASI PERISIAN

Objektif:

Memastikan penggunaan perisian yang dibenarkan pada peralatan ICT.

4.19.1 Pemasangan Perisian Pada Sistem Pengoperasian	Tanggungjawab
Perkara berikut perlu dipatuhi bagi sebarang pemasangan atau perubahan perisian: a) pengemaskinian versi sistem pengoperasian hanya boleh dilakukan oleh Pentadbir Bilik *Server* Utama MPS / Rangkaian; b) memastikan hanya "*executable code*" yang diluluskan digunakan dalam sistem operasi; c) memasang dan mengemas kini perisian yang telah diuji keberkesanan sahaja; d) memastikan semua sumber *libraries* program yang terkini; e) menggunakan sistem pengurusan konfigurasi untuk mengawal konfigurasi dan dokumentasi sistem; f) menetapkan strategi pembentukan semula (*rollback*) sebelum perubahan dilaksanakan; g) memastikan log audit direkodkan bagi semua pengemaskinian; h) memastikan versi lama perisian diarkibkan dan direkodkan untuk kegunaan memproses data sekiranya diperlukan; i) hanya perisian yang dibenarkan bagi kegunaan di MPS;	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

j) memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; dan
k) mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.

4.20 KESELAMATAN RANGKAIAN

Objektif:

Memastikan pengurusan keselamatan perkhidmatan rangkaian dilaksanakan bagi melindungi maklumat dan kemudahan ICT daripada ancaman.

4.20.1 Keselamatan Peranti Rangkaian	Tanggungjawab
Kawalan keselamatan ke atas rangkaian perlu dilaksanakan bagi melindungi daripada akses yang tidak dibenarkan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) tahap pengelasan maklumat yang diuruskan dalam rangkaian MPS; b) menetapkan tanggungjawab dan prosedur bagi pengurusan peranti rangkaian; c) memastikan pengemaskinian maklumat rangkaian secara berterusan seperti diagram rangkaian dan fail konfigurasi peranti; d) mengasingkan tanggungjawab operasi rangkaian daripada operasi sistem ICT sekiranya perlu; e) menetapkan kawalan untuk melindungi kerahsiaan dan integriti maklumat yang melalui rangkaian awam, rangkaian pihak ketiga atau rangkaian tanpa wayar; f) memantau secara berkala log masuk untuk mengesan insiden keselamatan; g) melaksanakan aktiviti pengurusan rangkaian secara berterusan bagi memastikan perkhidmatan yang optimum; h) melaksanakan pengesahan pengguna sebelum mengakses rangkaian; i) mengehadkan dan mengawal akses ke rangkaian; j) memastikan kawalan dan mengehadkan ke atas semua peralatan lain yang akan menggunakan rangkaian MPS; k) memastikan tindakan pengukuhan ke atas peranti rangkaian; l) mengehadkan akses peranti rangkaian bagi Pentadbir Rangkaian dan Keselamatan berbanding pengguna biasa; m) mengasingkan sementara segmen rangkaian yang terjejas sehingga dipulihkan semula; n) menyahaktifkan protokol rangkaian yang terdedah kepada ancaman; o) memastikan kawalan keselamatan yang sesuai untuk penggunaan *Virtual Private Network* (VPN);	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

p) peralatan rangkaian hendaklah diletakkan di lokasi yang bebas daripada risiko seperti banjir, gegaran dan habuk;
q) semua trafik rangkaian hendaklah melalui peranti keselamatan rangkaian MPS;
r) semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Aggrement* (SLA) yang telah ditetapkan;
s) penggunaan rangkaian tanpa wayar (*wireless*) LAN di MPS hendaklah mematuhi peraturan; dan
t) penggunaan perisian rangkaian seperti *network analyser* hendaklah mendapat kelulusan ICTSO.

4.21 KESELAMATAN PERKHIDMATAN RANGKAIAN

Objektif:

Memastikan keperluan, mekanisme dan tahap keselamatan perkhidmatan rangkaian disemak, dilaksana dan dipantau.

4.21.1 Panduan Perkhidmatan Rangkaian	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mempunyai kawalan akses kepada perkhidmatan rangkaian yang disediakan; b) melaksanakan pengesahan identiti bagi mengakses perkhidmatan rangkaian; c) mengawal akses kepada perkhidmatan rangkaian mengikut peranan yang diluluskan; d) menyediakan prosedur pengurusan rangkaian bagi kawalan keselamatan kepada perkhidmatan rangkaian; e) menggunakan kaedah yang selamat bagi mengakses perkhidmatan rangkaian seperti penggunaan *Virtual Private Network* (VPN) atau rangkaian tanpa wayar; f) merekodkan maklumat seperti masa, lokasi, dan lain-lain semasa penggunaan perkhidmatan rangkaian; g) memantau penggunaan perkhidmatan rangkaian; h) pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian; dan i) Pentadbir Bilik *Server* Utama MPS / Rangkaian bertanggungjawab ke atas insiden keselamatan yang melibatkan perkhidmatan rangkaian.	ICTSO, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.21.2 Keselamatan Perkhidmatan Rangkaian	Tanggungjawab
Aspek keselamatan perkhidmatan rangkaian yang perlu mengambil kira seperti yang berikut:	ICTSO, Pentadbir Bilik *Server* Utama MPS / Rangkaian

a) menggunakan teknologi keselamatan perkhidmatan rangkaian seperti pengesahan identiti, kawalan akses atau penggunaan enkripsi;
b) memastikan peralatan rangkaian mematuhi polisi parameter yang ditetapkan bagi menjamin keselamatan sambungan rangkaian;
c) memastikan kawalan akses kepada perkhidmatan rangkaian dan sistem aplikasi mengikut peranan yang diluluskan;
d) memastikan trafik rangkaian dipantau dan dikawal oleh peralatan keselamatan; dan
e) menggunakan peralatan *Web Content Filtering* bagi mengawal akses ke laman web yang tidak dibenarkan.

4.22 PENGASINGAN RANGKAIAN

Objektif:

Memastikan pengasingan kawalan sempadan ke atas perkhidmatan rangkaian yang disediakan untuk meminimumkan risiko ancaman atau pengubahsuaian yang tidak dibenarkan.

4.22.1 Panduan Pengasingan Rangkaian	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) menyediakan segmen yang hanya untuk kegunaan warga MPS; b) menetapkan segmen yang berbeza bagi pengguna biasa, pentadbir, pelayan, sistem aplikasi dan pihak ketiga; c) mengasingkan akses rangkaian mengikut tahap kritikal dan sensitiviti atau lain-lain keperluan; d) memastikan penggunaan peralatan keselamatan seperti *firewall* atau router bagi mengawal segmen rangkaian; e) melaksanakan polisi kawalan akses melalui *gateway* berdasarkan keperluan dan klasifikasi maklumat; f) mengasingkan rangkaian tanpa wayar dengan rangkaian dalaman kecuali dengan menggunakan kawalan keselamatan seperti *firewall*; g) mengasingkan akses rangkaian tanpa wayar untuk pelawat dan warga MPS; h) mengawal akses kepada peralatan rangkaian bagi pengguna yang dibenarkan sahaja; dan i) mengemas kini hak akses pengguna dan pentadbir sekiranya berlaku perubahan tanggungjawab.	ICTSO, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.23 KAWALAN PENAPISAN WEB

Objektif:

Memastikan akses ke laman web dilindungi dan menyekat akses ke laman web yang tidak dibenarkan.

4.23.1 Panduan Penapisan Web	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) menyekat alamat IP atau domain laman web yang tidak sah; b) memantau laman web yang mempunyai fungsi muat naik maklumat; c) menyekat laman web berbahaya seperti phishing dan *malicious code*; d) mengemas kini pangkalan data (*signature database*) peralatan keselamatan web melalui sumber yang sahih; e) menyekat laman web perkongsian maklumat yang tidak sah (*illegal*); f) memberikan latihan teknikal kepada kakitangan teknikal mengenai pengendalian peralatan laman web; dan g) memberikan program kesedaran kepada pengguna mengenai tatacara akses laman web yang selamat.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.24 PENGGUNAAN KRIPTOGRAFI

Objektif:

Memastikan penggunaan kriptografi untuk melindungi kerahsiaan dan integriti maklumat berdasarkan keperluan MPS dengan mematuhi keperluan undang-undang yang berkaitan.

4.24.1 Penggunaan Kriptografi	Tanggungjawab
Penggunaan kriptografi perlu mematuhi perkara seperti yang berikut: a) memaksimumkan faedah, meminimumkan risiko dan mengelak penyalahgunaan kriptografi berdasarkan kepada peraturan yang berkuat kuasa; b) mengenal pasti kriptografi yang hendak digunakan berdasarkan klasifikasi maklumat; c) memastikan perlindungan maklumat menggunakan kriptografi atau kaedah kawalan yang bersesuaian ke atas peranti mudah alih dan media storan yang dihantar menerusi rangkaian; d) menetapkan peranan dan tanggungjawab bagi: i. pelaksanaan peraturan penggunaan kriptografi; dan ii. pengurusan kunci seperti penjanaan kunci. e) menetapkan kesesuaian penggunaan kriptografi berdasarkan keperluan di MPS; f) melaksanakan pemeriksaan ke atas kandungan maklumat sebelum dienkripsi bagi memastikan tiada *malware* dan kandungan berbahaya;	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

g) kandungan perjanjian perkhidmatan dengan pihak ketiga yang menyediakan perkhidmatan kriptografi perlu mengandungi tanggungjawab, kebolehpercayaan perkhidmatan dan masa tindak balas bagi penyediaan perkhidmatan;
h) maklumat perlu diklasifikasikan mengikut tahap peringkat maklumat seperti Rahsia Besar, Rahsia, Sulit dan Terbuka;
i) media storan seperti *external hard disk*, *thumb drive* dan sebagainya perlu dilaksanakan penetapan kata laluan bagi mengelakkan pencerobohan maklumat; dan
j) penggunaan *Secure Socket Layer* (SSL) adalah diwajibkan bagi semua sistem aplikasi atau pertukaran maklumat dengan pihak ketiga.

4.24.2 Pengurusan Kunci Kriptografi	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) melaksanakan proses penjanaan, penyimpanan, mengarkibkan, pengambilan semula, pengagihan, penamatan dan pemusnahan kunci kriptografi; b) memastikan sistem pengurusan kunci kriptografi perlu berdasarkan piawaian, prosedur atau kaedah yang selamat; c) menjana kunci kriptografi yang berlainan bagi setiap sistem dan aplikasi; d) pengeluaran sijil kunci kriptografi umum; e) pengagihan kunci kriptografi kepada entiti berkaitan termasuk pengaktifan selepas penerimaan; f) menyimpanan dan cara akses kepada kunci kriptografi; g) penukaran atau pengemaskinian kunci; h) pengurusan kunci kriptografi yang terjejas; i) menyahaktifkan kunci kriptografi yang telah terjejas atau pengguna yang tamat perkhidmatan; j) menggantikan kunci kriptografi yang hilang atau rosak; k) mengarkib atau membuat pendua kunci kriptografi; l) memusnahkan kunci kriptografi; m) mengaudit atau merekodkan log aktiviti kunci kriptografi; n) menetapkan tempoh pengaktifan dan menyahaktifkan bagi kunci kriptografi; o) memberikan kerjasama kepada pihak berkaitan sekiranya diperlukan; p) kunci kriptografi perlu dilindungi daripada pengubahsuaian, kehilangan dan akses yang tidak dibenarkan; dan q) peralatan atau perisian yang digunakan untuk menghasilkan, menyimpan, dan mengarkib kunci kriptografi perlu dilindungi.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pegawai Aset ICT

4.24.3 Panduan Penggunaan Kriptografi Untuk Kawalan Keselamatan	**Tanggungjawab**
Penggunaan kriptografi disarankan berdasarkan kategori seperti yang berikut:	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server*

a) kerahsiaan (*confidentiality*): menggunakan enkripsi untuk melindungi maklumat semasa penyimpanan atau penghantaran; b) integriti atau ketulenan (*integrity or authenticity*): menggunakan tandatangan digital untuk mengesahkan ketulenan atau integriti maklumat yang disimpan atau dihantar; c) tidak boleh disangkal (*non-repudiation*): menggunakan kriptografi ke atas bahan bukti bagi sesuatu peristiwa atau tindakan; dan d) pengesahan (*authentication*): menggunakan kriptografi untuk mengesahkan identiti pengguna atau transaksi yang melibatkan sistem aplikasi.	Utama MPS / Rangkaian, Pegawai Aset ICT

4.25 KITARAN HAYAT PEMBANGUNAN YANG SELAMAT

Objektif:

Memastikan pembangunan sistem aplikasi mengguna pakai kitar hayat pembangunan yang selamat

4.25.1 Panduan Pembangunan Sistem yang Selamat	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a) aspek keselamatan pembangunan perlu diambil kira dalam perkhidmatan, infrastruktur, perisian dan sistem; b) mengasingkan persekitaran sebenar (*production*), pembangunan (*development*) dan (*testing/staging*); c) menyediakan panduan keselamatan dalam kitar hayat pembangunan sistem (*development lifecycle*) yang mengambil kira: i. metodologi keselamatan pembangunan sistem; dan ii. garis panduan pengekodan selamat. d) keperluan keselamatan dalam fasa spesifikasi, reka bentuk dan pengurusan projek; e) pengujian keselamatan seperti ujian penembusan, semakan kod pengaturcaraan dan pengujian pepijat (*bugs*) kod pengaturcaraan selepas pengemaskinian; f) penyimpanan kod sumber dan konfigurasi sistem aplikasi di tempat yang selamat; g) memastikan kawalan keselamatan ke atas perubahan versi sistem aplikasi; h) menyediakan keperluan latihan keselamatan sistem aplikasi untuk meningkatkan kemahiran teknikal pengaturcaraan bagi mengenal pasti dan menyelesaikan kelemahan ke atas aplikasi; i) memastikan keperluan lesen diambil kira atau dan menggunakan alternatif lain bagi kawalan kos yang efektif; dan j) memastikan pembangunan yang dilaksanakan oleh pihak ketiga mengambil kira kitar hayat pembangunan secara selamat dalam dokumen kontrak/perjanjian.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.26 KEPERLUAN KESELAMATAN SISTEM APLIKASI

Objektif:

Memastikan semua keperluan keselamatan maklumat dikenal pasti semasa pembangunan atau penambahbaikan sistem aplikasi.

4.26.1 Keperluan Keselamatan Aplikasi

Tanggungjawab

ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

Keperluan keselamatan sistem aplikasi yang perlu diambil kira adalah seperti yang berikut:

a) memastikan pengguna mempunyai tahap akses yang dibenarkan;
b) mengenal pasti jenis maklumat dan tahap klasifikasi yang akan diproses oleh sistem aplikasi;
c) membezakan had akses kepada data dan fungsi dalam sistem aplikasi;
d) ketahanan terhadap ancaman perisian hasad atau gangguan pihak yang tidak dibenarkan;
e) memastikan perundangan dan peraturan dipatuhi bagi transaksi yang dijana, diproses, dilengkapkan atau disimpan;
f) menetapkan keperluan privasi bagi pihak yang terlibat;
g) memastikan maklumat rahsia rasmi dilindungi;
h) memastikan data yang diproses dan dipindahkan dilindungi;
i) memastikan komunikasi antara semua pihak dienkripsi dengan selamat;
j) melaksanakan pengesahan input;
k) mengawal kelulusan yang dijana oleh Sistem Aplikasi seperti mengehadkan kelulusan atau kelulusan melebihi satu orang pelulus;
l) mengawal kebenaran untuk akses kepada *output* yang dihasilkan;
m) mengehadkan kandungan medan *free text* bagi mengawal kapasiti storan;
n) melaksanakan pemantauan dan merekodkan log transaksi ke atas proses kerja;
o) memastikan kawalan keselamatan sistem aplikasi seperti penggunaan perisian log atau sistem pengesanan kebocoran data; dan
p) pengendalian mesej ralat.

4.26.2 Transaksi Perkhidmatan Dalam Talian

Tanggungjawab

ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

Perkara-perkara berikut perlu dipatuhi:

a) memastikan pengguna mempunyai tahap akses mengikut kelulusan atau kebenaran pemilik sistem;
b) memastikan penggunaan mekanisme seperti digital signature, hashing dan lain-lain untuk mengesahkan identiti penghantar dan penerima semasa pertukaran data;
c) memastikan pengesahan berkaitan dengan pihak yang berhak untuk meluluskan kandungan maklumat, penerbitan atau menandatangani dokumen transaksi;

d) memastikan semua pihak memahami aspek kerahsiaan, integriti, serta bukti penghantaran dan penerimaan dokumen;
e) memastikan perkhidmatan sistem aplikasi menggunakan *Secure Socket Layer* (SSL) dalam setiap transaksi; dan
f) menetapkan tempoh transaksi yang disimpan.

4.26.3 Aplikasi Pesanan dan Pembayaran Elektronik	Tanggungjawab
Perkara berikut perlu dipatuhi: a) mengekalkan kerahsiaan dan integriti maklumat pesanan atau pembayaran; b) mengesahkan maklumat pembayaran oleh pelanggan; c) mengelakkan kehilangan atau duplikasi maklumat transaksi; d) menyimpan maklumat transaksi di lokasi yang selamat dan tidak boleh diakses oleh orang ramai; dan e) menggunakan tandatangan atau sijil digital yang sah dan dikeluarkan oleh pihak yang diberi kuasa (*authority*).	ICTSO, Pentadbir Sistem ICT, Pihak Ketiga

4.27 PRINSIP KEJURUTERAAN DAN ARKITEKTUR SISTEM YANG SELAMAT (*SECURE SYSTEM ARCHITECTURE AND ENGINEERING PRINCIPLES*)

Objektif:

Prinsip kejuruteraan keselamatan sistem hendaklah diwujudkan, didokumenkan, dikaji dan diguna pakai ke atas semua pembangunan sistem aplikasi.

4.27.1 Kriteria Kejuruteraan Sistem yang Selamat	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) menyediakan kawalan keselamatan yang diperlukan untuk melindungi maklumat dan sistem aplikasi daripada ancaman yang dikenal pasti; b) mempunyai keupayaan kawalan keselamatan untuk mencegah, mengesan atau melaksanakan tindakan ke atas insiden keselamatan; c) memastikan semua maklumat rahsia rasmi dienkripsi (*encryption*); d) mengenal pasti keperluan kawalan keselamatan yang akan dilaksanakan; e) melaksanakan kawalan keselamatan terhadap individu yang berkaitan; f) memastikan prinsip kejuruteraan mengaplikasikan reka bentuk keselamatan (*security architecture*); g) memastikan kawalan keselamatan infrastruktur seperti penggunaan *Public Key Infrastructure* (PKI*), Identity and Access Management* (IAM), pencegahan kebocoran data dan pengurusan akses dinamik; h) mempunyai kepakaran untuk membangunkan dan menyelenggarakan sistem aplikasi selari dengan teknologi yang digunakan atau dipilih;	Pentadbir Sistem ICT, Pihak Ketiga

i) mengambil kira keperluan kos, masa dan cabaran dalam memenuhi keperluan keselamatan;
j) mengguna pakai konsep amalan terbaik (best practise); dan
k) melaksanakan *Security Posture Assessment* (SPA) dan *hardening* ke atas sistem aplikasi.

4.27.2 Prinsip "Zero Trust"	Tanggungjawab
Perkara yang perlu diambil kira adalah seperti yang berikut: a) kawalan keselamatan tidak boleh bergantung sepenuhnya kepada peralatan keselamatan rangkaian; b) menyemak dan mengesahkan identiti bagi semua akses ke sistem aplikasi; c) memastikan sistem aplikasi menggunakan fungsi enkripsi; d) menyemak dan mengesahkan semua permohonan akses yang diterima; e) memberikan kategori akses paling minimum kepada pengguna; dan f) menggunakan pengesahan keselamatan ketika log masuk atau transaksi yang melibatkan sistem aplikasi seperti *captcha*, *security phrase* dan *Secure Transaction Authorisation Code* (TAC).	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pihak Ketiga

4.28 PENGEKODAN SELAMAT

Objektif:

Memastikan penggunaan kod pengaturcaraan yang selamat bagi meminimumkan kelemahan (*vulnerabilities*) dalam sistem aplikasi.

4.28.1 Fasa Perancangan Pengekodan Selamat	Tanggungjawab
Perkara yang perlu diambil kira adalah seperti yang berikut: a) pembangunan sistem aplikasi sama ada secara dalaman (*in-house*) atau luaran (*outsource*) hendaklah menggunakan pengekodan selamat berdasarkan kepada peraturan dan keperluan yang dikuat kuasakan; b) memastikan amalan dan kelemahan pengekodan yang berlaku sebelum ini dijadikan sebagai sumber rujukan supaya kelemahan keselamatan maklumat yang sama tidak berulang; c) menggunakan perisian Pembangunan seperti *Integrated Development Environments* (IDE) untuk membantu pengekodan selamat; d) penggunaan persekitaran pembangunan semasa fasa pembangunan sistem aplikasi; e) memastikan penggunaan perisian pembangunan yang terkini;	ICTSO, Pentadbir Sistem ICT, Pihak Ketiga

f) memastikan pengaturcaraan atau pihak ketiga yang dilantik mempunyai kemahiran dalam pembangunan sistem aplikasi menggunakan pengekodan selamat; dan
g) memastikan arkitektur, reka bentuk dan standard pengekodan digunakan dalam persekitaran yang selamat.

4.28.2 Fasa Semasa Pengekodan Selamat	Tanggungjawab
Perkara yang perlu diambil kira adalah seperti yang berikut: a) memastikan penggunaan teknik dan struktur pengekodan selamat bagi bahasa pengaturcaraan yang digunakan seperti *pair programming*, *refactoring* dan *test-driven development*; b) merekodkan dan memperbetulkan kelemahan kod sumber yang boleh terdedah kepada ancaman daripada dieksploitasi; c) menggunakan perisian yang terkini dan tidak tamat tempoh *End of Support* (EOS); d) memastikan tidak menggunakan Teknik Pembangunan yang tidak selamat seperti *hard-coded passwords*, *unapproved code samples* dan *unauthenticated web services*; e) melaksanakan pengujian keselamatan maklumat dan tindakan pembaikan; f) memastikan keupayaan integrasi dengan sistem maklumat yang lain; g) sebelum sistem aplikasi digunakan, perkara seperti di bawah hendaklah dilaksanakan: i. memastikan hak akses minimum pengguna; ii. melaksanakan analisis berkaitan kesalahan umum kod pengaturcaraan; dan iii. merekodkan tindakan pembetulan.	ICTSO, Pentadbir Sistem ICT, Pihak Ketiga

4.28.3 Fasa Penyelenggaraan dan Kajian Semula	Tanggungjawab
Perkara yang perlu diambil kira adalah seperti yang berikut: a) memastikan *patches* dan *security* updates perisian sentiasa dikemas kini; b) kelemahan keselamatan maklumat yang dilaporkan hendaklah diambil tindakan; c) ralat dan cubaan serangan hendaklah direkodkan serta disemak secara berkala bagi penambahbaikan ke atas kod pengaturcaraan sekiranya perlu; dan d) kod sumber hendaklah dilindungi daripada akses dan gangguan yang tidak dibenarkan seperti menggunakan fungsi kawalan versi (*version control*). Sekiranya menggunakan libraries luaran, perkara seperti di bawah hendaklah dilaksanakan:	ICTSO, Pentadbir Sistem ICT

a) memastikan *libraries* luaran yang digunakan adalah versi terkini;
b) menggunakan komponen seperti pengesahan kriptografi yang telah disahkan dan stabil;
c) memastikan lesen, keselamatan dan komponen luaran yang sah;
d) memastikan *libraries* boleh diselenggarakan dan diperoleh daripada sumber yang dipercayai; dan
e) ketersediaan sumber yang mencukupi untuk rujukan pembangunan jangka panjang.

Sekiranya software package perlu ditambah baik, perkara seperti di bawah hendaklah dipastikan:

a) risiko kepada fungsi kawalan sedia ada dan integriti perisian tersebut;
b) perlu mendapatkan kebenaran persetujuan daripada pihak ketiga;
c) keperluan untuk mendapatkan perubahan versi terkini;
d) iImplikasi yang akan berlaku sekiranya tanggungjawab penyelenggaraan diberikan kepada MPS; dan
e) keserasian (*compatibility*) dengan perisian yang lain.

4.29 PENGUJIAN KESELAMATAN SEMASA PEMBANGUNAN DAN PENERIMAAN

Objektif:

Pengujian Keselamatan Semasa Pembangunan dan Penerimaan

4.29.1 Pengujian Keselamatan Sistem Aplikasi	Tanggungjawab
Pengujian keselamatan hendaklah merangkumi perkara berikut: a) fungsi keselamatan sistem aplikasi hendaklah diuji semasa fasa pembangunan seperti pengesahan pengguna, kawalan akses, penggunaan kriptografi dan pengekodan selamat b) konfigurasi keselamatan yang melibatkan sistem pengoperasian, *firewalls* dan komponen keselamatan lain hendaklah diuji; c) *Security Posture Assessment* (SPA) hendaklah dilaksanakan ke atas semua sistem aplikasi baharu atau penambahbaikan sistem aplikasi; d) menyemak dan mengesahkan data sebelum dikunci masuk dalam sistem aplikasi bagi menjamin ketepatan maklumat; dan e) melaksanakan semakan dan pengesahan ke atas *output* data yang dihasilkan oleh sistem aplikasi.	ICTSO, Pentadbir Sistem ICT, Pihak Ketiga

4.29.2 Pelan Pengujian Penerimaan Sistem	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut:	ICTSO, Pentadbir Sistem ICT, Pihak Ketiga

a) menyediakan jadual aktiviti pengujian;
b) menyediakan input dan output yang dijangka supaya memenuhi senarai syarat yang telah ditentukan;
c) menetapkan kriteria untuk menilai keputusan;
d) memastikan proses kerja sistem aplikasi memenuhi keperluan pengguna;
e) melaksanakan pengujian fungsi ke atas sistem aplikasi menggunakan data palsu (*dummy input*);
f) melaksanakan keputusan pengujian yang memerlukan tindakan lanjut sekiranya diperlukan;
g) melaksanakan integrasi dan pengujian dengan sistem aplikasi yang lain sekiranya berkaitan; dan
h) melaksanakan ujian prestasi (*performance test*) dan ujian tekanan (*stress test)*.

4.29.3 Pengujian Bebas bagi Pembangunan Dalaman dan Luaran	Tanggungjawab
Pengujian perlu dilaksanakan oleh selain daripada pasukan pembangunan sistem aplikasi. Perkara berikut perlu diambil kira seperti: a) melaksanakan aktiviti semakan kod pengaturcaraan untuk mengenal pasti kelemahan termasuk input dan ralat yang tidak dijangka; b) melaksanakan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem aplikasi; c) melaksanakan pengujian penembusan (*penetration testing*) untuk mengenal pasti reka bentuk dan kod sumber tidak selamat; d) penilaian produk dan perkhidmatan hendaklah dilaksanakan sebelum perolehan dilaksanakan; e) perjanjian bersama pihak ketiga perlu mengandungi keperluan keselamatan; f) pembangunan secara luaran (*outsource*) atau pembelian komponen hendaklah mengikut tatacara perolehan; dan g) persekitaran pengujian hendaklah sama dengan persekitaran sebenar supaya pengujian tersebut tidak boleh disangkal dan boleh dipercayai.	ICTSO, Pentadbir Sistem ICT, Pihak Ketiga

4.30 PEMBANGUNAN SISTEM SECARA LUARAN

Objektif:

Pembangunan sistem aplikasi yang dilaksanakan oleh pihak ketiga perlu dikawal selia dan dipantau bagi memastikan keselamatan maklumat dipatuhi.

4.30.1 Pembangunan Sistem Secara Luaran	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut:	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server*

a) memastikan perjanjian lesen, *Intellectual Property Rights* (IPR) dan kod sumber menjadi hak milik kerajaan; b) memastikan spesifikasi perolehan mengandungi klausa berhubung keperluan keselamatan reka bentuk, keselamatan pengaturcaraan, pengujian, pensijilan keselamatan produk, ketersediaan kod sumber, keperluan pelupusan data, keutamaan terhadap teknologi dan kepakaran tempatan serta keperluan kompetensi pasukan pembangunan; c) menyediakan penilaian keselamatan oleh pihak ketiga; d) melaksanakan pengujian penerimaan untuk memastikan kualiti dan *output* memenuhi keperluan; e) memastikan pembuktian risiko penilaian keselamatan dan privasi di tahap minimum yang boleh diterima; f) memastikan pengujian keselamatan, kelemahan yang dikenal pasti dan tindakan pembetulan dilaksanakan adalah mencukupi sebelum penyerahan projek; g) menguatkuasakan bon perjanjian sekiranya pihak ketiga tidak memenuhi perkhidmatan; h) memasukkan klausa dalam kontrak yang membenarkan pelaksanaan audit terhadap proses pembangunan dan kod sumber; i) melaksanakan keperluan keselamatan untuk persekitaran pembangunan; dan j) mengambil kira perundangan yang berkuat kuasa seperti *Personal Data Act*	Utama MPS / Rangkaian, Warga MPS, Pihak Ketiga

4.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN SEBENAR

Objektif:

Memastikan keselamatan maklumat dalam semua persekitaran ICT dilindungi daripada ancaman oleh pihak tidak dibenarkan.

4.31.1 Aspek Pengasingan Persekitaran ICT	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mewujudkan prosedur keperluan sumber bagi penyediaan persekitaran untuk pembangunan, pengujian dan sebenar; b) mengasingkan persekitaran sebenar dengan pembangunan dalam domain yang berbeza secara *virtual* atau fizikal; c) menetapkan, merekodkan dan melaksanakan peraturan serta pengesahan untuk migrasi sistem aplikasi atau perisian daripada persekitaran pembangunan kepada persekitaran sebenar; d) melaksanakan pengujian ke atas perubahan sistem aplikasi di persekitaran pengujian sebelum digunakan dalam persekitaran sebenar; e) tidak menggunakan maklumat sebenar pada persekitaran pembangunan atau persekitaran pengujian kecuali dengan kawalan keselamatan;	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian, Pihak Ketiga

f) memastikan *compilers*, *editor* dan *tools* pembangunan atau program utiliti lain tidak boleh diakses daripada persekitaran sebenar apabila tidak diperlukan lagi;
g) merekodkan semua penggunaan sumber yang dilaksanakan; dan
h) memantau pelaksanaan penggunaan sumber bagi tujuan perancangan kapasiti.

4.31.2 Langkah Keselamatan bagi Persekitaran Pembangunan Pengujian dan Sebenar	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mengemas kini patches, pembangunan sistem aplikasi, integrasi dan *tools* pengujian seperti *builders*, *integrators*, compilers, sistem konfigurasi dan *libraries*; b) memastikan keselamatan konfigurasi sistem aplikasi dan operasi perisian yang selamat; c) memantau dan memastikan kawalan akses persekitaran; d) memantau kawalan perubahan persekitaran dan kod yang disimpan; dan e) menyediakan sandaran (*backup*) persekitaran sebenar secara berkala.	ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

4.32 PENGURUSAN PERUBAHAN

Objektif:

Memastikan pengurusan perubahan dalam persekitaran ICT dilaksanakan dengan mengambil kira kawalan keselamatan maklumat.

4.32.1 Prosedur Kawalan Perubahan	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) merancang dan menilai impak yang mungkin berlaku ke atas pihak lain yang mempunyai kepentingan atau kebergantungan; b) memastikan perubahan yang dilaksanakan telah mendapat kelulusan; c) memastikan perubahan yang dilaksanakan dimaklumkan kepada pihak berkepentingan; d) perubahan atau pengubahsuaian ke atas perkakasan, perisian atau sistem aplikasi hendaklah diuji, direkodkan dan disahkan sebelum diguna pakai; e) memastikan pelaksanaan perubahan mengambil kira perancangan pembangunan; f) memastikan prosedur pembentukan semula (fallback) dilaksanakan sebagai pelan perancangan luar jangka (*contingency*); g) merekodkan semua perubahan yang dilaksanakan;	ICTSO, Pentadbir Sistem ICT

h) memastikan manual operasi pengguna dan sistem aplikasi diubah mengikut keperluan;
i) memastikan prosedur pelan kesinambungan perkhidmatan dan pemulihan ICT diubah mengikut keperluan;
j) semua aspek mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan;
k) setiap perubahan kepada sistem pengoperasian perlu dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap keselamatan maklumat;
l) perubahan kepada kod pengaturcaraan (*source code*) perlu dihadkan kepada Pentadbir Sistem Aplikasi yang dibenarkan; dan
m) memastikan aktiviti seperti memasang, menyenggara, menghapus dan mengemas kini mana-mana komponen ICT hendaklah mendapatkan kelulusan.

4.32.2 Kawalan Perubahan Kepada Platform	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) perubahan platform hendaklah dikaji bagi membolehkan pengujian yang bersesuaian dilakukan sebelum pelaksanaan; b) memastikan sistem aplikasi, integriti data dan kawalan akses disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilaksanakan; c) ujian penerimaan pengguna perlu dilaksanakan setelah perubahan platform selesai dilaksanakan; dan d) memastikan perubahan yang sesuai diselaraskan kepada pelan kesinambungan perkhidmatan.	ICTSO, Pentadbir Sistem ICT

4.32.3 Kawalan Perubahan Kepada Perisian	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) memastikan perubahan pakej perisian mengambil kira aspek keselamatan maklumat; b) perubahan pakej perisian hanya dilaksanakan oleh pihak yang dibenarkan sahaja; c) melaksanakan pengujian ke atas pakej perisian yang terkini sebelum dimaklumkan kepada semua pengguna; dan d) memastikan perubahan pakej perisian tidak menjejaskan perkhidmatan operasi sistem maklumat.	ICTSO, Pentadbir Sistem ICT

4.33 DATA PENGUJIAN

Objektif:

Memastikan pemilihan data yang digunakan semasa pengujian dilindungi dan dikawal mengikut peraturan yang ditetapkan.

4.33.1 Panduan Penggunaan Data	Tanggungjawab

Perkara yang perlu dipatuhi adalah seperti yang berikut:

CTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

a) melaksanakan kawalan akses yang sama di persekitaran sebenar dan persekitaran pengujian;
b) menyediakan hak akses berlainan setiap kali maklumat digunakan ke persekitaran pengujian;
c) menyimpan log penyalinan dan penggunaan maklumat operasi bagi tujuan jejak audit;
d) data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian;
e) data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat;
f) melindungi maklumat terperingkat dengan pelaksanaan penyembunyian data dan menghapus data setelah pengujian selesai; dan
g) menghapuskan maklumat operasi setelah pengujian selesai untuk mengelakkan data digunakan oleh pihak tidak dibenarkan.

4.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA UJIAN AUDIT

Objektif:

Memastikan penilaian pengujian audit dilaksanakan ke atas proses kerja sistem aplikasi.

4.34.1 Panduan Ujian Audit	Tanggungjawab

Perkara yang perlu dipatuhi adalah seperti yang berikut:

ICTSO, Pentadbir Sistem ICT, Pentadbir Bilik *Server* Utama MPS / Rangkaian

a) mendapatkan kebenaran untuk capaian kepada sistem aplikasi dan data bagi ujian audit;
b) mendapatkan kebenaran untuk melaksanakan ujian audit berdasarkan kawalan dan skop yang dibenarkan;
c) memastikan data yang dibenarkan hanya berstatus *read only* semasa ujian audit dilaksanakan;
d) jika terdapat keperluan capaian kepada sistem aplikasi, pengujian hendaklah dilaksanakan oleh pentadbir yang dibenarkan bagi membantu juruaudit;
e) memastikan keperluan keselamatan perkakasan juruaudit dipatuhi seperti penggunaan antivirus sebelum kebenaran diberikan;

f) membenarkan capaian kepada sistem fail oleh juruaudit dan menghapuskan data tersebut setelah audit selesai atau melaksanakan kawalan keselamatan yang bersesuaian;
g) memastikan penggunaan peralatan audit (*audit tools*) mendapat kelulusan terlebih dahulu;
h) melaksanakan ujian audit di luar waktu bekerja sekiranya menyebabkan gangguan perkhidmatan; dan
i) menyimpan dan memantau semua akses semasa ujian audit.

GLOSARI

GLOSARI

BIL	ISTILAH	PENERANGAN
1.	*Active Directory (AD)*	Teknologi Microsoft yang digunakan untuk mengurus komputer dan peralatan lain dalam rangkaian.
2.	Anomali	Keadaan atau sesuatu yang tidak biasa, luar biasa, atau menyimpang dari norma atau corak yang dijangkakan. Dalam konteks teknikal dan keselamatan maklumat, anomali sering digunakan untuk merujuk kepada tingkah laku atau kejadian yang berbeza daripada kebiasaan, yang mungkin menunjukkan terdapatnya masalah, kecacatan, atau ancaman
3.	*Antivirus*	Perisian yang mengimbas virus pada media storan seperti *hard disk, external hard disk* dan *thumb drive* untuk sebarang kemungkinan adanya virus.
4.	Aplikasi	Perisian komputer atau program yang khusus digunakan untuk peranti mudah alih.
5.	Aset Alih	Aset atau peralatan yang boleh dipindahkan atau dialihkan dari satu tempat ke tempat lain secara mudah termasuk Aset Alih yang dibekalkan bersekali dengan penyediaan bangunan atau infrastruktur lain.
6.	Aset ICT	Sesuatu yang bernilai yang boleh menyebabkan kerugian sekiranya berlaku kehilangan, kerosakan atau perubahan. Dalam konteks keselamatan maklumat, aset boleh dikategorikan kepada beberapa kumpulan antaranya proses kerja, data / maklumat, perisian, perkakasan, perkhidmatan, sumber manusia dan tapak / premis. (Surat Pekeliling Am Bilangan 3 Tahun 2024) Peralatan ICT termasuk perkakasan, perisian, aplikasi, dokumentasi, perkhidmatan, data atau maklumat dan sumber manusia.
7.	*Backup*	Proses penduaan sesuatu dokumen atau maklumat.
8.	*Bandwidth*	Jalur Lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
9.	*Brute Force*	Teknik yang digunakan oleh pencuri atau penggodam untuk meneka kata laluan atau kunci kriptografi dengan mencuba semua kemungkinan kombinasi secara sistematik hingga berjaya.

BIL	ISTILAH	PENERANGAN
10.	*BYDO*	*Bring Your Own Device*
11.	Capaian Jarak jauh	Capaian jarak jauh yang dimaksudkan merangkumi: i. capaian kepada sistem rangkaian dalaman; dan ii. capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan teleworking; atau iii. capaian Jarak Jauh merujuk kepada kemampuan untuk mengakses sistem komputer, rangkaian, atau sumber maklumat dari lokasi yang jauh atau bukan lokasi fizikal yang sama dengan sistem tersebut. Ini membolehkan pengguna untuk bekerja, mendapatkan maklumat, dan menjalankan tugas secara efektif tanpa perlu berada di lokasi yang sama dengan sumber yang ingin diakses.
12.	CCTV	*Closed-circuit television* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
13.	CDO	Chief Digital Officer Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
14.	*Clear Desk dan Clear Screen*	Tidak meninggalkan dokumen data dan maklumat terperingkat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
15.	CERT MPS	*Computer Emergency Response Team* Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan siber di agensi masing-masing dan agensi di bawah kawalannya.
16.	*Denial of Service*	Halangan pemberian perkhidmatan.
17.	*Downloading*	Aktiviti muat-turun sesuatu perisian.
18.	DRC	*Data Recovery Centre* Pusat Pemulihan Data
19.	DRP	*Disaster Recovery Plan* Pelan Pemulihan Bencana
20.	EOS	*End of Support* Tamat sokongan

BIL	ISTILAH	PENERANGAN
21.	*Encryption*	Proses enkripsi (penyulitan) data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
22.	Fasiliti Perkhidmatan Sokongan	Merangkumi peralatan, kemudahan tempat, perkhidmatan penyelenggaraan, sistem notifikasi amaran dan pengujian berkala bagi memastikan kesinambungan perkhidmatan ICT.
23.	*Firewall*	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk peralatan atau perisian atau kombinasi kedua-duanya.
24.	*Forgery*	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft*/*espionage*), penipuan (*hoaxes*).
25.	*Hard disk*	Cakera keras yang digunakan untuk menyimpan data dan boleh di akses lebih pantas.
26.	IAM	*Identity and Access Management*
27.	ICT	*Information and Communication Technology*
28.	ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
29.	IDE	*Integrated Development Environments*
30.	Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
31.	Internet	Sistem rangkaian seluruh dunia, di mana pengguna pada mana-mana komputer boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
32.	Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.

BIL	ISTILAH	PENERANGAN
33.	*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.
34.	*Intrusion Detection System* (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
35.	*Intrusion Prevention System* (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based* IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
36.	IPR	Intellectual Property Rights
37.	ISMS	Information Security Management System
38.	JPTM	Jawatankuasa Perkhidmatan dan Teknologi Maklumat
39.	JTICT	Jawatankuasa Teknikal ICT
40.	Klon	Merujuk kepada salinan yang tepat dan lengkap dari sistem, perisian, atau peranti, termasuk semua data dan konfigurasi yang ada. Klon biasanya digunakan untuk membuat usaha pemulihan yang lebih mendalam atau untuk membina persekitaran kerja yang identik.
41.	Kriptografi	Kaedah untuk menukar data dan maklumat biasa (piawaian format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
42.	LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
43.	*Log out*	Keluar daripada sesuatu sistem atau aplikasi komputer.
44.	*Malicious code*	Merujuk kepada sebarang kod, skrip, atau perintah yang direka untuk melakukan tindakan berbahaya, yang mungkin termasuk *malware*.

BIL	ISTILAH	PENERANGAN
45.	NACSA	*National Cyber Security Agency* Agensi Keselamatan Siber Negara
46.	*Outsource*	Maklumat yang diproses dan diperoleh di luar daripada sesuatu organisasi atau struktur kerja.
47.	Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
48.	Pegawai Keselamatan	Memastikan keselamatan perlindungan di jabatan terjamin sepanjang masa.
49.	Pegawai Rekod Jabatan	Memastikan pelabelan maklumat dilaksanakan bagi memudahkan pengurusan penyimpanan maklumat.
50.	Pembangun Sistem	Individu atau kumpulan teknikal atau Pihak Ketiga yang bertanggungjawab dalam membangunkan sistem aplikasi berdasarkan spesifikasi keperluan sistem yang ditetapkan oleh pemohon/ pemilik proses.
51.	Pembekal	Pembekal barangan atau penyedia perkhidmatan.
52.	Pemilik	Pegawai yang didaftarkan sebagai pemilik aset dan dipertanggungjawabkan ke atas aset tersebut.
53.	Pemilik Projek	Individu yang bertanggungjawab terhadap hampir keseluruhan proses kerja projek tersebut. Pemilik projek memainkan peranan utama menentukan keperluan, spesifikasi dan ciri-ciri serahan (produk atau perkhidmatan) yang akan dihasilkan oleh projek tersebut.
54.	Pemilik Proses	Individu yang bertanggungjawab untuk menentukan keperluan bisnes dan mengesahkan sebarang perubahan yang diperlukan berkaitan dengan bisnes proses.
55.	Pengguna	Pengguna terdiri daripada warga MPS dan Pihak Ketiga yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT MPS.
56.	Pengurus Projek	Individu yang bertanggungjawab untuk merancang dan menguruskan projek dengan baik supaya projek dapat disiapkan mengikut kos, tempoh masa dan kualiti yang telah ditetapkan.

BIL	ISTILAH	PENERANGAN
57.	Peralatan Sokongan ICT	Peralatan yang menyokong penggunaan peralatan ICT bagi memastikan kelancaran ICT contohnya projektor, layar, kabel, speaker dan mikrofon.
58.	Perisian	Program atau atur cara komputer yang dapat digunakan dengan sistem komputer tertentu.
59.	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.
60.	Perisian hasad	Perisian hasad (*malware* atau *malius software*) merujuk kepada pelbagai jenis perisian berniat jahat yang direka untuk mengganggu, merosakkan, atau mendapatkan akses tidak sah kepada sistem komputer dan data.
61.	Pihak Ketiga	Pihak Ketiga terdiri daripada Pembekal, syarikat atau kumpulan syarikat yang dilantik untuk memperbaharui, membekal, menghantar, memasang, mentauliahkan, membangunkan, menguji, dan menyelenggarakan perkakasan atau perisian di MPS.
62.	Pihak Berkepentingan	Pihak berkepentingan terdiri daripada pembekal, perunding, pemegang taruh, pelawat dan pihak-pihak lain yang terlibat dalam pengurusan, penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan.
63.	PKI	*Public-Key Infrastructure* Infrastruktur Kunci Awam
64.	PKP	Pelan Kesinambungan Perkhidmatan
65.	DRP Team	Pasukan Pemulihan Bencana
66.	PPL	*Public Key Infrastructure* Infrastuktur Kunci Awam
67.	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.
68.	Rahsia Besar	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia.

BIL	ISTILAH	PENERANGAN
69.	Rahsia Rasmi	Apa-apa suratan yang dinyatakan dalam Jadual kepada Akta 88 dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi yang boleh dikelaskan sebagai Rahsia Besar/Rahsia/Sulit/Terhad.
70.	Redundancy	Kemudahan pemprosesan maklumat yang direka untuk mempunyai saluran atau sumber tambahan untuk menjamin kelangsungan operasi dan mengurangkan risiko kehilangan data atau kecuaian dalam pemprosesan maklumat.
71.	Restoration	Pemulihan ke atas data.
72.	*Router*	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
73.	*Screen saver*	Imej yang akan diaktifkan pada komputer setelah ia tidak digunakan dalam jangka masa tertentu.
74.	*Server*	Pelayan
75.	Sistem	Kumpulan dari elemen-elemen yang berinteraksi untuk mencapai suatu tujuan tertentu.
76.	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 atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.
77.	SLA	*Service Level Aggrement* Perjanjian Tahap Perkhidmatan
78.	SSL	*Secure Socket Layer* Lapisan Soket Selamat
79.	SPA	*Security Posture Assessment* Penilaian Postur Keselamatan
80.	*Switch*	Alat yang boleh menapis (filter) dan memajukan (forward) isyarat paket data antara segmen rangkaian LAN.
81.	TAC	*Transaction Authorisation Code*

BIL	ISTILAH	PENERANGAN
82.	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.
83.	*Threat*	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
84.	*Uninterruptible Power Supply* (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
85.	VPN	*Virtual Private Network* Penggunaan Rangkaian Maya
86.	Virus	Kod atur cara yang bertujuan merosakkan data atau sistem aplikasi.
87.	WAN	*Wide Area Network* Rangkaian yang merangkumi kawasan yang luas.

L A M P I R A N

Lampiran 1

PERMOHONAN PENGECUALIAN PEMATUHAN

POLISI KESELAMATAN SIBER MPS

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan / Bahagian : .....

Bidang	Butiran Pengecualian	Justifikasi

Tempoh Pengecualian : Tarikh Mula : [ ] - Tarikh Tamat : [ ]

**Tempoh maksima yang dibenarkan adalah selama satu (1) tahun sahaja.*

Pengesahan dan Kelulusan

Ulasan : .....

.....

***Diluluskan / Tidak diluluskan.**

..... Tarikh: .....

( )

b.p. Yang Dipertua, MPS

Lampiran 2

SURAT AKUAN PEMATUHAN

POLISI KESELAMATAN SIBER MPS

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan / Bahagian : .....
(untuk staf MPS sahaja)

Nombor Pekerja : .....
(untuk staf MPS sahaja)

Syarikat : .....
(selain staf MPS sahaja)

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam dokumen Polisi Keselamatan Siber MPS; 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)

.....

( )

b.p. Yang Dipertua, MPS

Tarikh: .....

Lampiran 3

PERJANJIAN KERAHSIAAN *(NON-DISCLOSURE AGREEMENT)*

NAMA PROJEK :	

Saya ..... bernombor kad pengenalan .....

berjawatan ..... dari Syarikat .....

dengan ini:

(a) tidak mendedahkan sebarang maklumat dan memberi perlindungan kerahsiaan yang sewajarnya kepada semua maklumat mengenai projek ini;

(b) tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi mengenai projek ini;

(c) tidak mempunyai kepentingan peribadi terhadap projek ini;

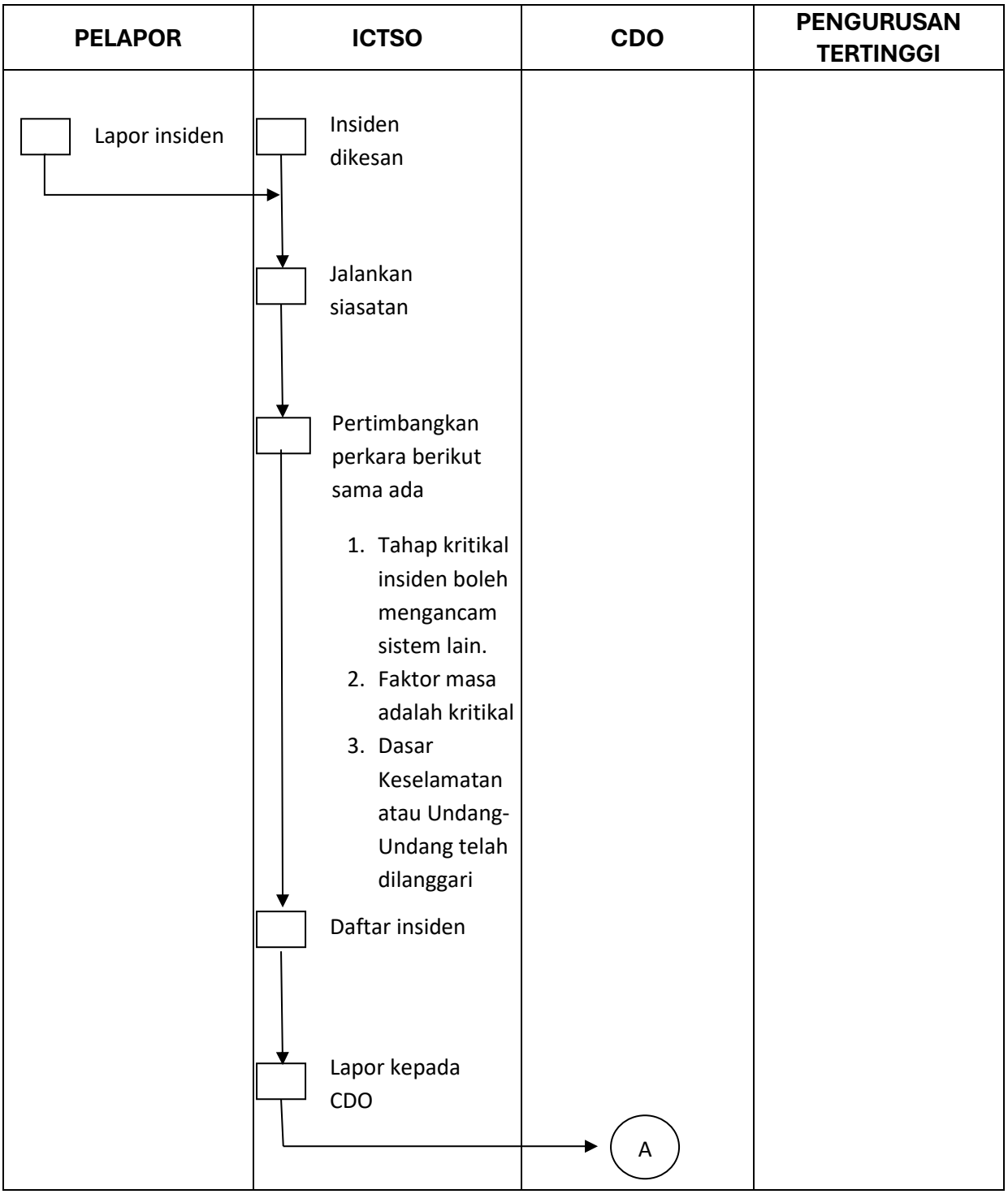
(d) Saya mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkahlaku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

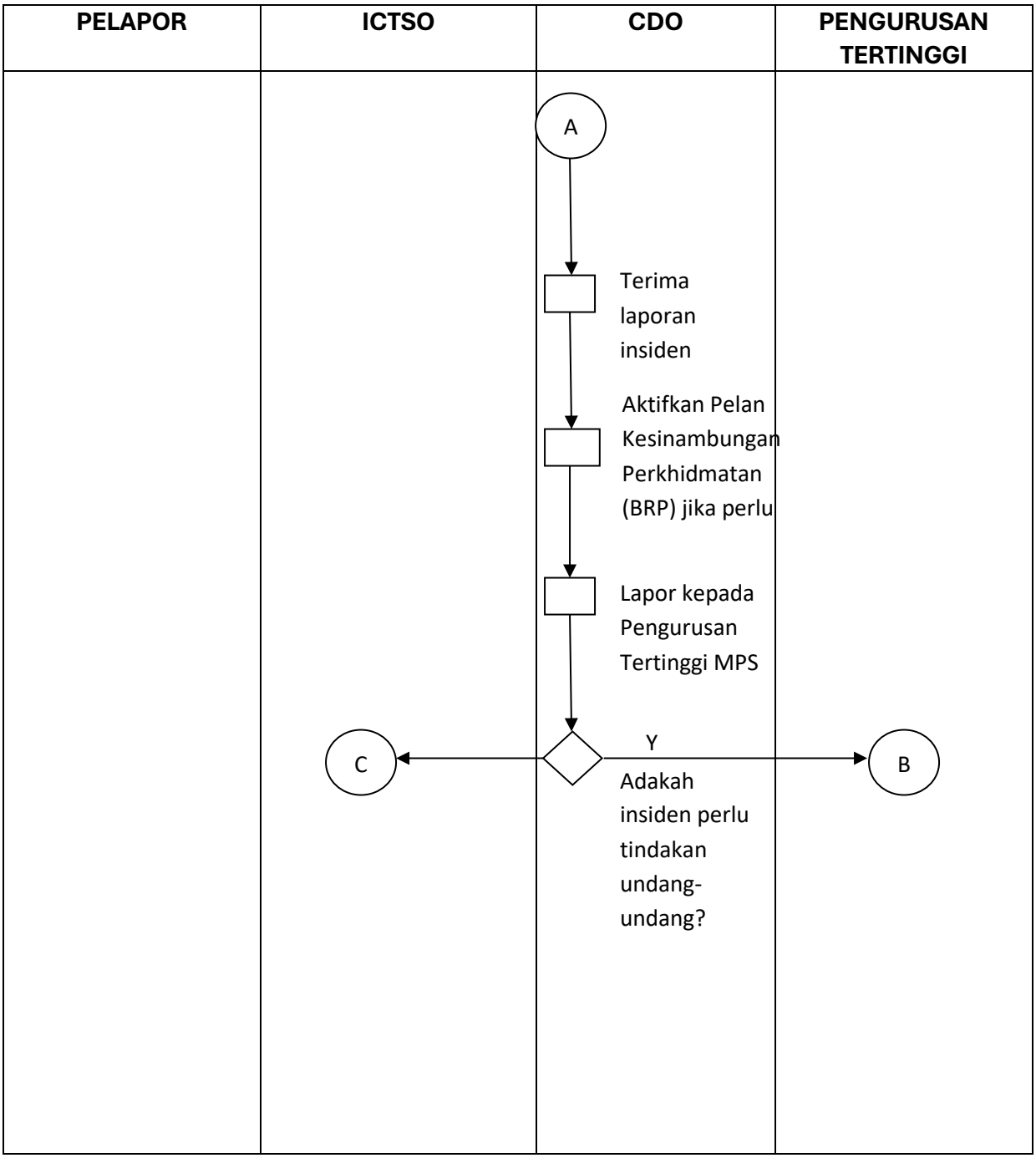
(e) Saya juga memahami dan bersedia untuk diambil tindakan, sekiranya Jabatan Teknologi Maklumat (JTM), Majlis Perbandaran Selayang mendapati saya melanggar perjanjian yang telah ditandatangani ini

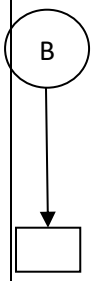
....

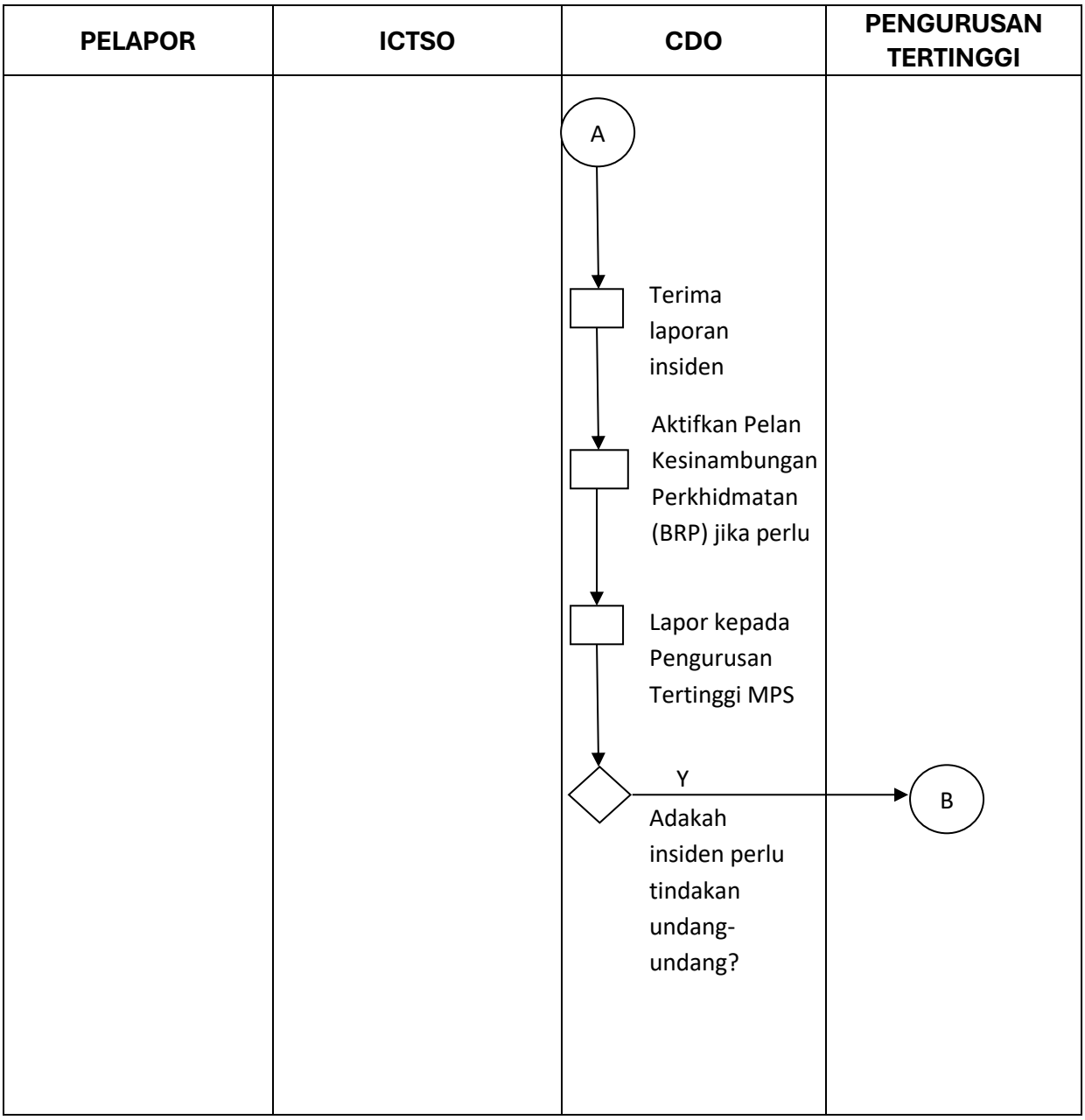
(Tandatangan) (Tarikh)

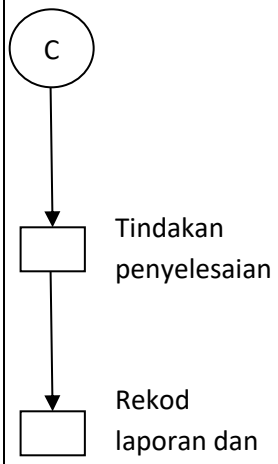
Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT MPS




PELAPOR
ICTSO
CDO
PENGURUSAN TERTINGGI
A
Terima laporan insiden
Aktifkan Pelan Kesinambungan Perkhidmatan (BRP) jika perlu
Lapor kepada Pengurusan Tertinggi MPS
Y
Adakah insiden perlu tindakan undang-undang?
C
B

PELAPOR	ICTSO	CDO	PENGURUSAN TERTINGGI
			 Ambil tindakan ke atas insiden yang menyalahi undang-undang dan peraturan berkaitan


PELAPOR
ICTSO
CDO
PENGURUSAN TERTINGGI
A
Terima laporan insiden
Aktifkan Pelan Kesinambungan Perkhidmatan (BRP) jika perlu
Lapor kepada Pengurusan Tertinggi MPS
Y
Adakah insiden perlu tindakan undang-undang?
B

PELAPOR	ICTSO	CDO	PENGURUSAN TERTINGGI
			

Lampiran 5

SENARAI PERUNDANGAN DAN PERATURAN

1) Arahan Keselamatan;

2) Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

3) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;

4) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT);

5) Pekeliling Kemajuan Penradbiran Awam Bilangan 1 Tahun 2003 – 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 Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

8) 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;

9) Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

10) Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi – Agensi Kerajaan yang bertarikh 23 November 2007;

11) Surat Pekeliling Am Bil. 2 Tahun 2000 – Peranan Jawatankuasa – jawatankuasa di bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

12) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

13) Surat Pekeliling Perbendaharaan Bil. 3/1995 – Peraturan Perolehan Perkhidmatan Perundangan;

14) Akta Tandatangan Digital 1997;

15) Akta Rahsia Rasmi 1972;

16) Akta Jenayah Komputer 1997;

17) Akta Hak Cipta (Pindaan) Tahun 1997;

18) Akta Komunikasi dan Multimedia 1998;

19) Perintah – Perintah Am;

20) Arahan Perbendaharaan;

21) Arahan Teknologi Maklumat 2007;

22) Garis Panduan Keselamatan MAMPU 2004;

23) *Standard Operating Procedure* (SOP) ICT MPS;

24) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;

25) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.

26) *Standard Operating Procedure* (SOP) AM Perintah Kawalan Pergerakan

27) Pekeliling Am Bil. 4 Tahun 2022 bertarikh 1 Ogos 2022 (Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam)

28) Surat Pekeliling Am Bilangan 3 Tahun 2024: Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam

JABATAN TEKNOLOGI MAKLUMAT
MAJLIS PERBANDARAN SELAYANG