KEMENTERIAN
PELABURAN, PERDAGANGAN DAN
INDUSTRI

DASAR
KESELAMATAN ICT

V 4.10

BAHAGIAN PENGURUSAN MAKLUMAT

SEJARAH DOKUMEN

VERSI	KELULUSAN	TARIKH KUATKUASA
1.0	JPICT Bil 3/2009	3 September 2009
2.0	JPICT Bil 1/2010	5 Februari 2010
3.0	JPICT Bil 2/2012	17 April 2012
3.1	Mesyuarat Pengurusan ISMS Bil. 2/2013	28 November 2013
3.2	Mesyuarat Pengurusan ISMS Bil. 1/2015	15 Januari 2015
4.0	Mesyuarat Pengurusan ISMS Bil. 1/2016	1 April 2016
4.1	Mesyuarat Pengurusan ISMS Bil. 2/2017	15 Mac 2017
4.2	Mesyuarat Pengurusan ISMS Bil. 3/2017	11 Mei 2017
4.3	Mesyuarat Pengurusan ISMS Bil. 1/2018	15 Mac 2018
4.4	Mesyuarat Pengurusan ISMS Bil. 1/2019	14 Februari 2019
4.5	Mesyuarat Pengurusan ISMS Bil. 1/2020	2 Mac 2020
4.6	Mesyuarat Pengurusan ISMS Bil. 1/2021	30 Mac 2021
4.7	Mesyuarat Pengurusan ISMS Bil. 2/2021	30 Ogos 2021
4.8	Mesyuarat Pengurusan ISMS Bil. 1/2022	25 Februari 2022
4.9	Mesyuarat Pengurusan ISMS Bil. 1/2023	09 Mac 2023
4.10	Mesyuarat Pengurusan ISMS Bil. 3/2024	29 Mei 2024

KEMENTERIAN PELABURAN, PERDAGANGAN DAN INDUSTRI

JADUAL PINDAAN DASAR KESELAMATAN ICT MITI

TARIKH	VERSI	BUTIR PINDAAN
09 Mac 2023	**4.9**	Rujuk **LAMPIRAN 6** Bilangan 4
29 Mei 2024	**4.10**	Rujuk **LAMPIRAN 6** Bilangan 5

ISI KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT MITI mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) MITI. Dasar ini juga menerangkan kepada semua pengguna di MITI mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT MITI.

OBJEKTIF

Dasar Keselamatan ICT MITI diwujudkan untuk:

(a) Memastikan kesinambungan perkhidmatan sekiranya berlaku sebarang insiden keselamatan yang tidak diingini;

(b) Menghalang dan meminimumkan sebarang insiden keselamatan yang berlaku;

(c) Memastikan kerahsiaan dokumen dan maklumat elektronik sentiasa terpelihara;

(d) Memastikan integriti dokumen dan maklumat elektronik supaya sentiasa tepat, lengkap, sahih dan kemas kini. Ia hanya boleh diubah dengan kaedah yang dibenarkan;

(e) Memastikan punca dokumen dan maklumat adalah daripada sumber yang sah dan tanpa keraguan;

(f) Memastikan akses hanya kepada pengguna-pengguna yang sah; dan

(g) Mencegah salah guna atau kecurian asset ICT Kerajaan.

PERNYATAAN DASAR

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

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

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

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

Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

(a) **Kerahsiaan**

Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

(b) **Integriti**

Data dan maklumat hendaklah tepat, lengkap dan 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 ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

SKOP

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

(a) Data dan maklumat hendaklah boleh diakses 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.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT MITI ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

(a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan MITI. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) Perisian

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

(c) Perkhidmatan

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

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

(d) Data atau Maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif MITI. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod MITI, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

(e) Manusia

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

(f) Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara **(a)** - **(e)** di atas.

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT MITI 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 akses di bawah prinsip ini adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut :

i. Klasifikasi maklumat seperti yang tercatat di dalam Arahan Keselamatan, di mana maklumat dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad.

ii. Tapisan keselamatan pengguna yang mematuhi prinsip bahawa pengguna boleh diberi kebenaran mengakses kategori maklumat tertentu setelah siasatan latarbelakang menunjukkan tiada sebab atau faktor untuk menghalang pengguna daripada berbuat demikian.

(b) Hak Akses Minimum

Hak akses kepada pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan diperlukan untuk membolehkan pegawai mewujud, menyimpan, mengemaskini, mengubah dan membatalkan sesuatu data atau maklumat.

(c) Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT MITI. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah 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 dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

Secara minimum, semua sistem ICT memerlukan persekitaran operasi yang berasingan seperti berikut:

i. Persekitaran pembangunan bagi aplikasi dalam proses pembangunan.
ii. Persekitaran penerimaan bagi pengujian aplikasi.
iii. Persekitaran sebenar bagi pengoperasian aplikasi.

(e) Pengauditan

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

(f) Pematuhan

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

(g) Pemulihan

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

(h) Saling bergantung

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

PENILAIAN RISIKO KESELAMATAN ICT

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

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

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat

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

MITI bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam. MITI 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.

BIDANG 01

PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101 Dasar Keselamatan ICT

Objektif:
Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan MITI dan perundangan yang berkaitan.

010101 Pelaksanaan Dasar	**Tanggungjawab**
Pelaksanaan dasar ini akan dijalankan oleh Ketua Setiausaha (KSU) MITI, dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO) dan semua Pengarah Kanan dan Pengarah Bahagian.	KSU
010102 Penyebaran Dasar	
Dasar ini perlu disebarkan dan dihebahkan kepada semua pengguna ICT MITI (termasuk kakitangan, pembekal, pakar runding dan lain-lain yang berkenaan.)	ICTSO
010103 Penyelenggaraan Dasar	
Dasar Keselamatan ICT MITI adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT MITI: (a) kenal pasti dan tentukan perubahan yang diperlukan; (b) kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatan Kuasa Pemandu ICT (JPICT);	ICTSO

(c) maklum kepada semua pengguna akan perubahan yang telah dipersetujui oleh JPICT; dan (d) kaji semula dasar sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	
010104 Pengecualian Dasar	
Dasar Keselamatan ICT MITI adalah terpakai kepada semua pengguna ICT MITI dan tiada pengecualian diberikan.	Semua Pengguna

BIDANG 02

ORGANISASI KESELAMATAN

0201 Infrastruktur Organisasi Dalaman

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

020101 KSU	**Tanggungjawab**
Peranan dan tanggungjawab KSU adalah seperti berikut: (a) memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT MITI; (b) memastikan semua pengguna mematuhi Dasar Keselamatan ICT MITI; (c) memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan (d) memastikan penilaian risiko dan program keselamatan ICT dilaksanakan berpandukan kepada garis panduan, prosedur dan langkah keselamatan ICT.	KSU
020102 Ketua Pegawai Digital (*Chief Digital Officer-CDO*)	
Ketua Pegawai Digital (CDO) adalah Ketua Setiausaha atau pegawai yang diturunkan kuasa. Peranan dan tanggungjawab beliau adalah seperti berikut: (a) melaksanakan tanggungjawab menjaga keselamatan aset ICT berdasarkan Dasar Keselamatan ICT MITI; (b) menentukan keperluan keselamatan ICT; dan (c) membangun dan menyelaraskan pelaksanaan pelan latihan dan program kesedaran keselamatan ICT.	TKSU(I)

020103 Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) menyedia dan melaksanakan program-program kesedaran keselamatan ICT MITI; (b) menguatkuasakan Dasar Keselamatan ICT MITI; (c) memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MITI kepada semua pengguna; (d) mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MITI; (e) melaksanakan pengurusan risiko; (f) melaksanakan audit, mengkaji semula dan merumus tindak balas pengurusan agensi berdasarkan hasil penemuan audit serta menyediakan laporan berkaitan; (g) memberi amaran terhadap kemungkinan berlakunya ancaman merbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (h) melaporkan insiden keselamatan ICT kepada Pusat Kawalan dan Penyelarasan Siber Negara (NC4), Majlis Keselamatan Negara (MKN) dan memaklumkannya kepada CDO MITI; (i) menyelaras atau membantu siasatan berkenaan dengan ancaman atau sebarang serangan ke atas aset ICT; (j) melaksanakan penilaian keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baharu dapat dielakkan; (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) memperakui proses pengambilan tindakan tatatertib ke atas	Pengurus URKI BPM

pengguna yang melanggar Dasar Keselamatan ICT MITI; dan (m) memberikan kebenaran hak akses yang berkaitan keselamatan ICT kepada pengguna ICT MITI.	
020104 Pengurus ICT	
Pengarah Bahagian Pengurusan Maklumat (BPM) merupakan Pengurus ICT MITI. Peranan dan tanggungjawab beliau adalah seperti berikut: (a) memastikan semua pengguna memahami dan mematuhi Dasar Keselamatan ICT MITI, tatacara dan garis panduan yang dikeluarkan; (b) mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MITI; (c) menentukan kawalan hak akses semua pengguna ICT terhadap aset ICT MITI dan membuat semakan berkala; (d) merangka dan menyemak pelan kontingensi ICT MITI; (e) melaporkan sebarang masalah berkaitan keselamatan ICT kepada CDO; dan (f) menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MITI.	Pengarah BPM
020105 Pentadbir Sistem ICT	
Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut: (a) mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar 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 Dasar Keselamatan ICT MITI;	Pengurus Unit BPM

(c) memantau aktiviti capaian harian pengguna; (d) mengenal pasti dan mengambil tindakan serta-merta terhadap aktiviti-aktiviti yang meragukanseperti pencerobohan dan pengubahsuaian data tanpa kebenaran; (e) menyimpan dan menganalisis rekod jejak audit; (f) menyediakan laporan aktiviti capaian kepada pemilik maklumat berkenaan secara berkala; (g) memastikan setiap pengguna dikenali dengan menggunakan User ID yang unik; dan (h) bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	
020106 Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti berikut: (a) membaca, memahami dan mematuhi Dasar Keselamatan ICT MITI; (b) mengetahui dan memahami implikasi keselamatan ICT serta kesan daripada tindakan ketidakpatuhan terhadap Dasar Keselamatan ICT MITI; (c) melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat MITI; (d) 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;	Pengguna ICT

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. (e) melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; (f) menghadiri program-program kesedaran keselamatan ICT; dan (g) menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MITI sebagaimana di **Lampiran 1**.	
020107 Jawatankuasa Pemandu ICT MITI	
Jawatankuasa Pemandu ICT (JPICT) adalah jawatankuasa yang bertanggungjawab terhadap keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT MITI. Keanggotaan JPICT MITI adalah seperti berikut: Pengerusi: Ketua Setiausaha atau pegawai yang diturunkan kuasa Ahli: (1) Pengarah Kanan / Pengarah Bahagian (2) Ketua Agensi (3) Pengurus Unit BPM Urus Setia: Unit EKP BPM Bidang kuasa: (a) Memperakukan/meluluskan dokumen Dasar Keselamatan ICT MITI, (b) memantau tahap pematuhan keselamatan ICT;	JPICT MITI

(c) memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam MITI yang mematuhi keperluan Dasar Keselamatan ICT MITI; (d) menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; (e) memastikan Dasar Keselamatan ICT MITI selaras dengan dasar-dasar ICT kerajaan semasa; (f) menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; (g) membincang tindakan yang melibatkan ketidakpatuhan terhadap Dasar Keselamatan ICT MITI; (h) membuat keputusan mengenai tindakan yang perlu diambil terhadap sebarang insiden; dan (i) (g) dan (h) adalah tertakluk kepada tindakan tatatertib.	
020108 *Computer Security Incident Response Team* (MITI CSIRT)	
Keanggotaan MITI CSIRT adalah seperti berikut: Pengarah MITI CSIRT: Pengarah BPM Pengurus MITI CSIRT: Pengurus Unit Rangkaian dan Keselamatan ICT Ahli: (a) Pegawai Teknologi Maklumat (1) URKI (b) Pegawai Teknologi Maklumat (2) URKI (c) Pegawai Teknologi Maklumat Operasi (d) Pegawai Teknologi Maklumat APEG (e) Pegawai Teknologi Maklumat UTEK (f) Pegawai Teknologi Maklumat EKP (g) Pegawai Teknologi Maklumat AP (h) Pegawai Teknologi Maklumat AI (i) Personel ICT Malaysian Investment Development Authority (MIDA)	MITI CSIRT

(j) Personel ICT Malaysian External Trade Development Corporation (MATRADE) (k) Personel ICT Malaysia Productivity Corporation (MPC) (l) Personel ICT Malaysian Industrial Development Finance (MIDF) (m) Personel ICT Malaysia Automotive Robotics and IoT Institute (MARii) (n) Personel ICT Malaysia Steel Institute (MSI) (o) Personel ICT Standard and Industrial Research Institute of Malaysia (SIRIM) (p) Personel ICT EXIM Bank (q) Personel ICT Jabatan Standard Malaysia (r) Personel ICT InvestKL (s) Personel ICT Halal Development Corporation (HDC) (t) Personel ICT Majlis Rekabentuk Malaysia (MRM) (u) Personel ICT National Metrology Institute of Malaysia (NMIM) (v) Personel ICT National Aerospace Industry Coordinating Office (NAICO) (w) Personael ICT Collaborative Research in Engineering, Science and Technology (CREST) Peranan dan tanggungjawab 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) mengendali insiden keselamatan ICT dan mengambil tindakan baik pulih yang bersesuaian; (d) mengambil tindakan pemulihan dan pengukuhan; dan (e) menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada warga MITI agensi. (f) menyebarkan makluman berkaitan peranan dan tanggungjawab warga MITI dan agensi di dalam MITI CSIRT.	

020109 Pegawai Keselamatan MITI	
Peranan dan tanggungjawab Pegawai Keselamatan MITI adalah seperti berikut: (a) Menyelia penyediaan kad pengenalan MITI, kad akses, kad pelawat dan kad kuasa; (b) Menyelia Pengawal Keselamatan MITI dan Swasta; (c) Menyelia jadual bertugas pengawal keselamatan MITI dan Swasta; (d) Pengurusan latihan pengungsian bangunan; (e) Pengurusan latihan kebakaran bangunan; (f) Pengurusan jadual keselamatan pejabat; (g) Pengurusan kunci keselamatan di kementerian; (h) Menyelaras Pelan Pengurusan Risiko Bahagian; (i) Menyelaras Mesyuarat Jawatankuasa Keselamatan	Pegawai Keselamatan MITI

0202 Pihak Ketiga

Objektif:
Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (kontraktor, pembekal, penyedia perkhidmatan luaran dan lain-lain).

020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Pihak ketiga terdiri daripada kontraktor, pembekal dan penyedia perkhidmatan luaran. Peranan dan tanggungjawab pihak ketiga adalah bertujuan bagi memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi adalah seperti berikut: (a) membaca, memahami dan mematuhi Dasar Keselamatan ICT MITI; (b) perlu menandatangani *Non-Disclosure Aggrement* (NDA) MITI seperti di **MITI-ISMS-SP-SSMP-01** dan Surat Akuan Pematuhan Dasar Keselamatan ICT MITI seperti di **Lampiran 1**; (c) memahami implikasi keselamatan ke atas sebarang tindakan yang dilakukan; (d) melaporkan dengan segera sebarang aktiviti atau keadaan yang meragukan yang mungkin memberikan ancaman kepada aset ICT; (e) memastikan kerahsiaan maklumat MITI terpelihara; (f) mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian kepada pihak ketiga; (g) mengenal pasti keperluan keselamatan ICT sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; (h) akses kepada aset ICT MITI perlu berlandaskan kepada perjanjian kontrak; (i) memastikan semua syarat dan polisi keselamatan ICT dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai.	CDO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga.

i. Dasar Keselamatan ICT MITI; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; iv. Akta Perlindungan Data Peribadi 2010; dan v. Hak Harta Intelek.	

BIDANG 03

PENGURUSAN ASET

0301 Akauntabiliti Aset

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

030101 Inventori Aset ICT	**Tanggungjawab**
Perkara ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: (a) memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori serta sentiasa dikemaskini; (b) memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (c) memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MITI; (d) peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumenkan dan dilaksanakan; dan (e) setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Warga MITI

0302 Pengelasan dan Pengendalian Maklumat

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

030201 Kategori Maklumat	**Tanggungjawab**
Mengenal pasti kategori maklumat merupakan satu langkah penting dalam memastikan perlindungan yang mencukupi dan bersesuaian dengan kategori maklumat berkenaan. Semua maklumat yang dijana atau dikumpul oleh kementerian dan agensi hendaklah diasingkan mengikut kategori Maklumat Rasmi dan Maklumat Rahsia Rasmi. Kedua-dua kategori boleh mengandungi Maklumat Pengenalan Peribadi (*Personal Identifiable Information* (PII)). Data Terbuka juga merupakan sebahagian daripada Maklumat Rasmi. (a) Maklumat Rahsia Rasmi Merujuk kepada Akta Rahsia Rasmi 1972 [Akta 88], maklumat Rahsia Rasmi adalah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 [Akta 88] dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972. (b) Maklumat Rasmi Maklumat Rasmi adalah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh mana-mana agensi Kerajaan semasa menjalankan urusan rasmi. Maklumat Rasmi ini juga adalah merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.	Pemilik Maklumat

(c) Maklumat Pengenalan Secara Peribadi (PII) PII adalah maklumat yang boleh digunakan secara tersendiri atau digunakan dengan maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu yang juga dikategorikan sebagai Maklumat Rahsia Rasmi. (d) Data Terbuka Data Terbuka adalah maklumat yang bebas digunakan, dikongsi dan diguna semula oleh orang awam, agensi kerajaan dan organisasi swasta untuk pelbagai tujuan. Kementerian dan agensi hendaklah mematuhi pekeliling yang sedang berkuat kuasa. PII dikecualikan daripada Data Terbuka.	
030202 Pengelasan Maklumat	
Setiap maklumat perlu dikelaskan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan Dokumen Terperingkat seperti berikut: (a) Terbuka; (b) Rahsia; (c) Rahsia Besar; (d) Sulit; dan (e) Terhad.	Pemilik Maklumat
030203 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: (a) menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) menentukan maklumat sedia untuk digunakan; (d) menjaga kerahsiaan kata laluan;	Semua Pengguna

(e) mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; (g) menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum; dan (h) menjaga maklumat pengenalan peribadi PII daripada disebar dan disalahguna oleh pihak yang tidak bertanggungjawab.	

BIDANG 04

KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia Dalam Tugas Harian

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

040101 Memulakan Perkhidmatan di MITI	**Tanggungjawab**
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan MITI serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) melaksanakan tapisan keselamatan terhadap pegawai dan kakitangan MITI serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; (c) mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan; dan (d) pekerja sementara juga tertakluk kepada syarat-syarat 040101 (a) – (c) dan sebarang syarat lain yang ditetapkan oleh Bahagian Pengurusan Sumber Manusia.	Semua Pengguna
040102 Semasa Berkhidmat di MITI	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut:	Semua Pengguna

(a) memastikan pegawai dan kakitangan MITI serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MITI; (b) memastikan program kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MITI secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; (c) memastikan adanya proses tindakan disiplin dan / atau undang-undang ke atas pegawai dan kakitangan MITI serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh MITI; (d) memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan boleh dirujuk kepada Bahagian Pengurusan Sumber Manusia MITI; dan (e) pekerja sementara juga tertakluk kepada syarat-syarat 040102 (a) – (d) dan sebarang syarat lain yang ditetapkan oleh Bahagian Pengurusan Sumber Manusia MITI.	
040103 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) memastikan semua aset ICT dikembalikan kepada MITI mengikut peraturan dan / atau terma perkhidmatan yang ditetapkan; (b) membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat merujuk kepada peraturan yang ditetapkan oleh MITI dan / atau terma perkhidmatan; dan (c) pekerja sementara juga tertakluk kepada syarat-syarat 040103 (a) – (b) dan sebarang syarat lain yang ditetapkan oleh Bahagian Pengurusan Sumber Manusia.	Semua Pengguna

BIDANG 05

KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 Keselamatan Kawasan

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

050101 Kawalan Kawasan	**Tanggungjawab**
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan tahap keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (c) Memasang alat penggera atau kamera; (d) Menghadkan jalan keluar masuk; (e) Mengadakan kaunter kawalan; (f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; (g) Mewujudkan perkhidmatan kawalan keselamatan; (h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;	Pegawai Keselamatan MITI

(i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, rusuhan dan bencana; (k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
050102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Setiap warga MITI termasuk pekerja sementara hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan balik kepada Bahagian Pentadbiran MITI apabila warga MITI termasuk pekerja sementara berhenti, bertukar keluar atau bersara; (c) Semua pelawat/pihak ketiga hendaklah mendapatkan Pas Keselamatan Pelawat di Kaunter Pelawat di pintu masuk Bangunan MITI. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (d) Kehilangan pas mestilah dilaporkan dengan segera ke Bahagian Pentadbiran MITI.	Warga MITI/ Pelawat/ Pihak ketiga
050103 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. (a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan	Warga MITI/ Pelawat/ Pihak ketiga

(b) Pelawat/pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi oleh pegawai MITI sepanjang masa sehingga tugas di kawasan berkenaan selesai.	
050104 Keselamatan Pusat Data	
Semua perkakasan ICT berkaitan hendaklah diletakkan di dalam Pusat Data yang mempunyai kemudahan keselamatan, penyaman udara khas, kemudahan perlindungan kebakaran dan pengesanan suhu. Ini bagi memastikan semua perkakasan ICT berkaitan sentiasa selamat daripada pencerobohan atau sebarang ancaman dan membolehkan ia dicapai sepanjang masa. Pusat Data juga perlu dilengkapi dengan ciri-ciri keselamatan lain seperti CCTV dan UPS. Berikut beberapa langkah untuk melindungi perkakasan ICT tersebut: (a) Pemantauan dan pengawalan keluar masuk pengguna ke Pusat Data melalui sistem ***Security Access Door*** dan **CCTV*;*** (b) Hanya personel yang mempunyai kebenaran sahaja yang dibenarkan memasuki Pusat Data; (c) Memastikan Pusat Data sentiasa bersih dan perkakasan ICT bebas daripada habuk; (d) Penyaman udara mestilah berfungsi dengan baik di mana suhunya adalah bersesuaian dengan Pusat Data; dan (e) Semua peralatan keselamatan, sistem pencegahan dan penggera kebakaran, UPS dan penyaman udara mestilah diselenggarakan secara berkala.	BPM/ Penyelenggara Bangunan MITI

0502 Keselamatan Peralatan

Objektif:
Melindungi peralatan ICT MITI dari kehilangan, kerosakan, kecurian serta gangguan terhadap perkhidmatan peralatan tersebut.

050201 Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Warga MITI termasuk pekerja sementara hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (b) Warga MITI termasuk pekerja sementara bertanggungjawab sepenuhnya ke atas semua peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (c) Warga MITI termasuk pekerja sementara dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; (d) Warga MITI termasuk pekerja sementara dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran pihak BPM; (e) Warga MITI termasuk pekerja sementara adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (f) Warga MITI termasuk pekerja sementara mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemaskini di samping melakukan imbasan ke atas media storan yang digunakan; (g) Semua peralatan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran. Sebarang kehilangan aksesori berkaitan peralatan ICT (*mouse, keyboard, security cable lock,* beg *laptop* dan *power adapter*) hendaklah diganti sama atau setara dengan aksesori peralatan ICT yang asal; (h) Peralatan-peralatan kritikal ICT perlu disokong oleh UPS mengikut keperluan; (i) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan	Warga MITI

rangkaian seperti *switches*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;

(j) Semua peralatan ICT yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;

(k) Peralatan ICT yang dipinjam dari stor BPM untuk dibawa keluar dari premis MITI, perlulah mendapat kelulusan Pengarah / Pengurus BPM yang berkenaan atau Pegawai Aset ICT dan direkodkan bagi tujuan pemantauan;

(l) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset ICT dengan segera dan mengikut kepada Tatacara Pengurusan Aset Alih Kerajaan yang masih berkuatkuasa;

(m) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

(n) Warga MITI termasuk pekerja sementara tidak dibenarkan mengubah lokasi peralatan ICT dari tempat asal ia ditempatkan tanpa kebenaran Pihak BPM;

(o) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada pihak BPM untuk dibaikpulih;

(p) Semua peralatan ICT mestilah didaftarkan di dalam Sistem Pengurusan Aset (SPA) dan ditampal dengan pelekat aset rasmi;

(q) Sebarang pelekat selain daripada pelekat aset rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut mudah dikenal pasti;

(r) Semua komputer dan komputer riba yang dibekalkan oleh MITI mesti didaftarkan dengan *Active Directory* (AD);

(s) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;

(t) Warga MITI termasuk pekerja sementara dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pihak BPM;

(u) Warga MITI termasuk pekerja sementara bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (v) Warga MITI termasuk pekerja sementara hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; (w) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan (x) Memastikan *plug* ditanggalkan daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
050202 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti *catridge tape*, *optical disk*, *flash disk*, *external hard disk*, *USB drive* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; (b) Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; (c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; (e) Permohonan dan pergerakan media storan hendaklah direkodkan;	Pentadbir Sistem ICT dan Warga MITI

(f) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; (g) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; (h) Semua data di dalam media storan yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan (i) Penghapusan maklumat atau kandungan media storan mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
050203 Media Tandatangan Digital	
Media Tandatangan Digital adalah teknologi yang digunakan untuk mengesahkan identiti penghantar/penandatangan sesuatu mesej dan digunakan bagi memastikan sesuatu maklumat adalah betul dan sah di dalam transaksi elektronik. Ia bukanlah imej tandatangan individu yang diimbas/*soft copy*. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Warga MITI termasuk pekerja sementara hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan (c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO dan mengikut kepada Tatacara Pengurusan Aset Alih Kerajaan yang masih berkuatkuasa.	Warga MITI
050204 Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MITI; (b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengarah BPM; dan	Warga MITI

(c) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	
050205 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. (a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; (b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan kepada pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus BPM yang berkenaan.	BPM
050206 Peralatan ICT yang dibawa keluar dari premis	
Peralatan ICT yang dibawa keluar dari premis MITI adalah terdedah kepada pelbagai risiko keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan ICT perlu dilindungi dan dikawal sepanjang masa; dan (b) Penyimpanan atau penempatan peralatan ICT mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian seperti tempat berkunci dan terlindung.	Warga MITI

050207 Pelupusan Peralatan ICT

Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau aset bernilai rendah yang dibekalkan oleh MITI dan ditempatkan di MITI.

Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MITI.

(a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran;

(b) Sekiranya maklumat perlu disimpan, maka pengguna hendaklah membuat salinan pendua;

(c) Data yang terdapat di dalam storan peralatan ICT hendaklah dihapuskan mengikut pekeliling yang berkuatkuasa sebelum peralatan ICT tersebut dilupuskan;

(d) Pegawai Aset ICT hendaklah mengenal pasti sama ada peralatan ICT boleh dilupuskan atau sebaliknya;

(e) Peralatan ICT yang hendak dilupuskan perlu disimpan di tempat yang telah dikhaskan bagi menjamin keselamatan peralatan tersebut;

(f) Pegawai Aset ICT bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset;

(g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;

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

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk dijadikan hak milik peribadi.

ii. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hard disk*, *motherboard* dan

sebagainya; iii. Menyimpan dan memindahkan aksesori komputer dan mana-mana peralatan ICT yang berkaitan ke lokasi lain tanpa kebenaran Pegawai Aset ICT; iv. Memindah keluar dari MITI mana-mana peralatan ICT yang hendak dilupuskan; dan v. Melupuskan sendiri peralatan ICT. vi. Maklumat lanjut pelupusan hendaklah merujuk kepada Tatacara Pengurusan Aset Alih Kerajaan AM2.7 (1PP) yang terkini.	
050208 Komputer Riba	
Warga MITI yang menggunakan komputer riba mestilah mematuhi perkara-perkara seperti berikut: (a) Membuat salinan pendua segala maklumat yang berada di dalam komputer riba ke dalam media storan yang lain; (b) Bertanggungjawab untuk menjaga keselamatan komputer riba tersebut daripada sebarang kemalangan atau kecurian; (c) Mematikan (*disable*) fungsi rangkaian tanpa wayar (*wifi, bluetooth, infra red*) sekiranya ia tidak digunakan semasa berada di tempat awam; dan (d) Laporkan dengan segera jika berlaku sebarang insiden berkaitan ICT kepada BPM MITI.	Warga MITI
050209 Peminjaman Peralatan ICT	
Semua peralatan ICT termasuklah komputer, komputer riba, pencetak, projektor, dan aksesori yang berkaitan seperti kabel komputer dan sebagainya~~,~~ adalah hakmilik MITI. Oleh itu setiap peralatan yang dipinjam atau dibawa keluar atau masuk perlulah mengikut prosedur berikut: (a) Pengguna dikehendaki memohon dengan mengisi dan menandatangan borang Senarai Peralatan Yang Dibawa Masuk/Keluar yang disediakan oleh BPM;	Warga MITI

(b) Peralatan yang dipinjam perlulah dikembalikan setelah selesai menggunakannya untuk semakan dan simpanan pihak BPM serta menandatangani borang Senarai Peralatan Yang Dibawa Masuk/Keluar; (c) Peminjam adalah bertanggungjawab untuk memastikan kesemua peralatan dikembalikan dengan sempurna, lengkap dan selamat; dan (d) Sebarang kerosakan dan kegagalan peralatan berfungsi dengan baik hendaklah dilaporkan kepada Unit Sokongan Teknikal dengan segera.	

0503 Keselamatan Persekitaran

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

050301 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan perolehan, penyewaan atau pengubahsuaian hendaklah dirujuk terlebih dahulu kepada Pegawai Keselamatan MITI. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: (a) Merancang dan menyediakan pelan keseluruhan susun atur pejabat (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; (b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi seperti alat pencegah kebakaran dan pintu kecemasan; (c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;	Warga MITI/ Pihak Ketiga

(d) Semua bahan cecair dan mudah terbakar dilarang disimpan berhampiran tempat penyimpanan peralatan ICT; (e) Semua peralatan perlindungan keselamatan hendaklah disemak dan diuji sekurang-kurangnya satu (1) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan (f) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	
050302 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan kuasa yang sesuai hendaklah disalurkan kepada peralatan ICT; (b) Peralatan sokongan seperti UPS dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan (c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	BPM/ Penyelengga-raan Bangunan MITI
050303 Kabel Rangkaian	
Kabel rangkaian komputer hendaklah dilindungi supaya ianya tidak disalahgunakan oleh pengguna yang tidak bertanggungjawab. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: (a) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (b) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan	BPM/ Penyelengga-aan Bangunan MITI

(c) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	
050304 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Langkah-Langkah Keselamatan Sekiranya Berlaku Kebakaran; dan (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Bahagian yang dilantik mengikut aras.	Warga MITI

0504 Keselamatan Dokumen

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

050401 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur Arahan Keselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa berdasarkan Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan Akta Arkib Negara Malaysia; dan	Warga MITI

(e) Dokumen terperingkat yang dihantar secara elektronik hendaklah menggunakan kaedah *encryption* seperti menetapkan kata laluan pada setiap dokumen. (f) Semua dokumen yang disimpan di dalam peralatan ICT seperti Komputer, Komputer Riba dan Tablet perlu dipadamkan sebelum dipulangkan semula kepada BPM.	
050402 Simpanan Data atas Talian (*cloud storage*)	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen rasmi hanya dibenarkan disimpan di *private cloud storage.* (b) Dokumen terperingkat yang disimpan di *public cloud storage* hendaklah menggunakan kaedah *encryption* terlebih dahulu sebelum dimuat naik seperti menetapkan kata laluan pada setiap dokumen. (c) Warga MITI perlu mendapat kelulusan ICTSO untuk mencapai *private cloud storage.*	Warga MITI/ ICTSO

BIDANG 06

PENGURUSAN OPERASI DAN KOMUNIKASI

0601 Pengurusan Prosedur Operasi

Objektif:
Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan. Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat serta melindungi integriti maklumat.

060101 Pengendalian Prosedur	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	Warga MITI
060102 Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi	Warga MITI

kuasa dan mempunyai pengetahuan dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
060103 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan (c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pengarah BPM dan ICTSO

0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

Objektif:
Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.

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

0603 Perancangan dan Penerimaan Sistem

Objektif:
Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

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

0604 Perisian Berbahaya

Objektif:
Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *Trojan, spyware, malware* dan sebagainya.

060401 Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan ancaman ICT seperti antivirus, *Intrusion Prevention System* (IPS) dan *Web Application Firewall* (WAF) serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; (c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; (d) Mengemas kini antivirus dengan *pattern* antivirus yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara pengendalian; (g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan (i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus dan *malware*.	Warga MITI

0605 *Housekeeping*

Objektif:
Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.

060501 *Backup*	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Salinan *backup* hendaklah direkodkan dan disimpan di *off site.* Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Membuat *backup* ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali; (b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; (c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan (d) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	BPM

0606 Pengurusan Rangkaian

Objektif:
Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

060601 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. (a) Pemantauan rangkaian dan server MITI bagi memastikan	BPM

keselamatan dari pencerobohan dan kelancaran pengoperasian; (b) Capaian kepada infrastruktur rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (c) Pemasangan *firewall* untuk mengawal capaian ke atas sistem yang telah dibangunkan dan memastikan keselamatan aset ICT dalam rangkaian dari pencerobohan; (d) Pemasangan *Content Filtering* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; (e) Menggunakan infrastruktur keselamatan ICT menyeluruh bagi mengesan sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MITI; (f) Perkhidmatan *Wireless* untuk kegunaan awam hendaklah diasingkan daripada rangkaian dalaman MITI; (g) Semua pengguna hanya dibenarkan menggunakan rangkaian MITI sahaja. Penyambungan rangkaian melalui modem/ router/ telefon/ dan lain-lain peralatan persendirian adalah dilarang sama sekali; (h) Sebarang penyambungan rangkaian yang bukan di bawah kawalan MITI hendaklah mendapat kebenaran ICTSO; (i) Larangan memuat turun perisian berbahaya bagi mengelakkan prestasi rangkaian terganggu dan mengelakkan penyebaran virus dan *malware*; dan (j) Penggunaan *Secure Socket Layer Virtual Private Network (*SSL VPN) bagi capaian aplikasi dalaman MITI.	

0607 Pengurusan Media

Objektif:
Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

060701 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media dan peralatan ICT ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu dan ia tertakluk kepada polisi ISMS PHYSICAL AND ENVIRONMENTAL CONTROLS POLICY (MITI-ISMS-SP-PECP) dan ISMS BACKUP POLICY (MITI-ISMS-SP-BP)	Semua Pengguna
060702 Prosedur Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Menyimpan semua media di tempat yang selamat; (f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat; dan (g) Pengendalian media hendaklah merujuk kepada KEW PA 2 (Penyerahan Aset).	Semua Pengguna
060703 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut:	Pentadbir Sistem ICT

(a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan (c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	

0608 Pengurusan Pertukaran Maklumat

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

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

Kerajaan" (Pekeliling MAMPU) dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: (a) Kakitangan MITI hendaklah memohon e-mel melalui Sistem Permohonan Akaun E-mel yang dapat dicapai melalui ezlinks.miti.gov.my (b) Pengguna dilarang menggunakan e-mel rasmi MITI untuk tujuan komersil, politik, perjudian, jenayah, perniagaan dan sebagainya; (c) Pengguna dilarang melaksanakan konfigurasi penerimaan e-mel dari e-mel rasmi ke e-mel peribadi tanpa justifikasi dan kelulusan pentadbir e-mel bagi mengelak penyalahgunaan e-mel urusan rasmi kerja. (d) Pengguna dilarang menyebarkan gambar-gambar lucah, e-mel berunsurkan fitnah, perkauman, gangguan seksual atau yang berkaitan dengannya; (e) Pengguna dilarang membenarkan akaun e-mel dan kata laluan digunakan oleh orang lain untuk tujuan menghantar, membaca dan menjawab e-mel bagi pihaknya; (f) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul dan sah; (g) Pengguna dilarang menggunakan akaun e-mel persendirian seperti gmail, yahoo atau mana-mana *public* e-mel untuk menghantar sebarang e-mel untuk tujuan urusan rasmi; (h) Pengguna dilarang membuat pendaftaran sistem *online* yang tidak rasmi penggunakan e-mel rasmi MITI kerana e-mel tersebut dikuatiri akan disebar dan disalahgunakan untuk tujuan aktiviti penyebaran virus, e-mel *spamming*, e-mel *phishing* dan *junk mail* seperti iklan pemasaran produk; (i) Pengguna tidak digalakkan membuka lampiran e-mel dari penghantar yang tidak dikenali, berkemungkinan mengandungi virus atau program yang boleh menceroboh komputer pengguna tanpa disedari. *Hackers* biasanya menggunakan fail berformat *.doc, *.docx, *.xls, *.xlsx & *.pdf dan sebagainya untuk memperdaya	

penerima e-mel;

(j) Pengguna dilarang menghantar dan membuka fail lampiran e-mel (attachment file) berformat seperti *.scr, *.com, *.exe, *.dll, *.pif, *.vbs, *.bat, *.asd, *.chm, *.ocx, *.hlp, *.hta, *.js, *.shb, *.shs, *.vb, *.vbe, *.wsf, *.wsh, *.reg, *.ini, *.diz, *.cpp, *.cpl, *.vxd, *.sys dan *.cmd. Ia dikhuatiri akan menyebarkan virus secara automatik apabila dibuka;

(k) Pengguna dilarang menyebarkan fail-fail yang mengandungi kod perosak (*malicious code*) seperti virus, *worm, trojan horse* dan *back door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain;

(l) Pengguna mestilah melaksanakan *encryption* atau menetapkan *password* ke atas maklumat-maklumat terperingkat terutama yang dihantar menerusi rangkaian terbuka seperti Internet. Pengguna juga dilarang menghantar *password* yang ditetapkan melalui e-mel bersama fail tetapi ianya perlu dihantar melalui penggunaan *Short Message Service* (SMS) atau lain-lain saluran seperti *Instant Messaging* (IM) atau sebagainya;

(m) Pengguna dilarang menghantar dokumen yang besar melebihi 25MB bagi memastikan sistem e-mel tidak terganggu dan berada dalam prestasi yang baik;

(n) Pengguna digalakkan untuk mencetak dan mendokumenkan semua e-mel yang penting untuk mengelakkan kehilangan maklumat penting apabila berlaku kerosakan kepada storan komputer;

(o) Pengguna hendaklah membuat salinan dan menyimpan fail kepilan ke dalam satu *folder* berasingan dari setiap e-mel yang penting bagi tujuan *backup* jika berlaku sebarang masalah kepada storan komputer;

(p) Nama pegawai dan kakitangan MITI yang bertukar atau berhenti hendaklah dimaklumkan dengan segera kepada BPM agar akaun e-mel dapat dikemaskinikan dengan segera;

(q) Pengguna mesti memaklumkan kepada pentadbir e-mel dengan segera sekiranya mengesyaki akaun telah disalahgunakan;

(r) Semua mesej-mesej elektronik yang diwujudkan atau disimpan di

dalam sistem adalah dianggap tidak peribadi. Pentadbir e-mel atau ICTSO MITI berhak untuk membuat semakan kandungan e-mel pengguna. Isi kandungan e-mel tersebut tidak akan diakses atau didedahkan selain daripada untuk tujuan keselamatan atau diperlukan oleh undang-undang; (s) Pengguna hendaklah bertanggungjawab dan sentiasa menyelenggara *mailbox* masing-masing. E-mel yang tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; (t) Pentadbir e-mel boleh menamatkan akaun e-mel pengguna atas sebab-sebab berikut: I. Bertukar ke agensi lain II. Bersara III. Ditamatkan perkhidmatan IV. Tindakan tatatertib V. Akaun tidak aktif melebihi 30 hari (kecuali cuti bersalin) VI. Meninggal dunia (u) Penutupan akaun e-mel kakitangan adalah selepas dua (2) minggu dari tarikh akhir perkhidmatan di MITI; (v) Kuota kapasiti e-mel adalah bergantung kepada penyedia perkhidmatan e-mel semasa; (w) Akaun e-mel rasmi MITI hanya dibekalkan kepada kakitangan MITI dan kakitangan kontrak sahaja. Bagi pekerja sementara/pelajar latihan industri, e-mel akan diberikan tertakluk kepada justifikasi permohonan daripada pegawai yang menyokong (Pengarah Bahagian/Penyelia).	

0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)

Objektif:

Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.

060901 E-Dagang	
Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; (b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Semua Pengguna
060902 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: (a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; (b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan (c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua Pengguna

0610 Pemantauan

Objektif:
Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

061001 Pengauditan dan Forensik ICT	
Ahli CERT mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT MITI; (b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; (g) Aktiviti penyalahgunaan akaun e-mel; dan (h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	MITI CSIRT
061002 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi;	Pentadbir Sistem ICT

(b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
061003 Sistem Log	
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada MITI CSIRT.	Pentadbir Sistem ICT
061004 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;	Pentadbir Sistem ICT

(b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau mengikut keperluan; (c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; (d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; (e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan (f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MITI atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	

BIDANG 07

KAWALAN CAPAIAN

0701 Dasar Kawalan Capaian

Objektif:
Mengawal capaian ke atas maklumat.

070101 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 dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan (d) Kawalan ke atas kemudahan pemprosesan maklumat.	BPM

0702 Pengurusan Capaian Pengguna

Objektif:
Mengawal capaian pengguna ke atas aset ICT MITI.

070201 Akaun Pengguna	
Pengguna adalah bertanggungjawab ke atas sistem ICT yang	Warga MITI

digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan oleh kementerian sahaja boleh digunakan; (b) Pemilikan akaun pengguna tertakluk kepada peraturan MITI dan bukanlah hak mutlak pengguna. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (c) Penggunaan akaun milik orang lain adalah dilarang; (d) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (e) Pentadbir Sistem ICT boleh membekukan dan menamatkan akaun pengguna atas sebab-sebab seperti berikut: i. Bertukar ke agensi lain; ii. Bersara; iii. Ditamatkan perkhidmatan; iv. Tindakan tatatertib Bagi pengguna luar yang ingin menggunakan sistem dalaman MITI yang memerlukan capaian melalui VPN/tunnel, hendaklah mematuhi langkah-langkah berikut: (a) Membuat permohonan secara bertulis atau e-mel kepada pemilik sistem; (b) User ID dan katalaluan hanya akan diberikan kepada permohonan yang telah diluluskan.	
070202 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
070203 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MITI.	Semua Pengguna

Kata nama pengguna atau User ID merupakan satu pengenalan identiti yang unik bagi setiap pengguna yang menggunakan sesuatu sistem komputer. Setiap User ID yang dibekalkan akan mempunyai kata laluan yang unik untuk membenarkan pengguna mendapat akses ke sistem-sistem tertentu.

Untuk menjamin keselamatan User ID dan kata laluan, langkah-langkah berikut mesti dipatuhi oleh setiap pengguna sistem dan rangkaian MITI:

(a) Rahsiakan kata laluan. Pendedahan kata laluan kepada yang tidak berhak adalah satu kesalahan di bawah Akta Jenayah Komputer 1997. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi;

(b) Pengguna dilarang daripada menggunakan ID pengguna atau nama sebagai kata laluan;

(c) Pengguna dilarang menggunakan perkataan yang boleh diperolehi daripada mana-mana kamus dalam sebarang bahasa;

(d) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;

(e) Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan sekurang-kurangnya satu huruf besar, satu huruf kecil, satu angka dan satu aksara khusus (*contoh: p6T*&Wo8a$!d atau RkfOmH09O8*yq3*);

(f) Kata laluan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;

(g) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama;

(h) Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;

(i) Penguatkuasaan penukaran kata laluan semasa *login* kali pertama;

(j) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

(k) Pengguna dilarang menggunakan sebarang maklumat peribadi seperti tarikh lahir dan sebagainya sebagai kata laluan; (l) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian atau mengaktifkan *Two Factor Aunthentication* (2FA); (m) Had kemasukkan kata laluan bagi capaian system aplikasi adalah maksimum 3 kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga ID capaian diaktifkan semula; (n) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna; (o) Mengelakkan penggunaan semula kata laluan yang telah digunakan; (p) Laporkan segera kepada MITI CSIRT sekiranya kata laluan disyaki telah dicerobohi, dan kata laluan sedia ada akan diubah serta-merta; dan (q) Proses kelulusan kata laluan e-mel seperti di Lampiran 4 dan proses kelulusan kata laluan aplikasi seperti di Lampiran 5.	
070204 Clear Desk dan Clear Screen	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: *(a)* Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;	Semua Pengguna

(b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	

0703 Kawalan Capaian Rangkaian

Objektif:
Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.

070301 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MITI, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya. (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; dan	Pentadbir Sistem ICT
070302 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet di MITI hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MITI; (b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; (c) Penggunaan teknologi *seperti bandwidth manager* untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; (d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;	Semua Pengguna

(e) Segala maklumat yang diperolehi daripada Internet dan e-mel mestilah dikira tidak sahih selagi kesahihannya belum lagi dibuktikan; (f) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; (g) Bahan rasmi adalah dilarang dari dimuat naik ke Internet tanpa kebenaran pihak pengurusan; (h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; (i) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MITI; (j) Kakitangan MITI dilarang daripada memuat naik sebarang dokumen, perisian berlesen, e-mel dan sebagainya ke server atau ruang storan yang dipunyai oleh pihak luar tanpa sebarang kebenaran daripada pihak Pengurusan; (k) Kakitangan MITI yang menggunakan akaun MITI (miti.gov.my) merupakan wakil MITI. Oleh itu, setiap kakitangan diingatkan supaya tidak menggunakan akaun tersebut untuk tujuan komersial, politik, perjudian, jenayah dan sebagainya; (l) Fail yang dimuat turun dari Internet mestilah diimbas dengan menggunakan perisian antivirus sebelum ia diinstal atau diguna pakai. Semua langkah keselamatan perlu dilaksanakan untuk mengesan sebarang virus dan mengelakkannya daripada tersebar; (m) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CDO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; (n) Pengguna dilarang melayari laman web yang tidak beretika seperti laman web pornografi, *online games, social networking* dan sebagainya;	

(o) Pengguna dilarang menggunakan talian capaian Internet alternatif yang lain seperti modem persendirian dan Wireless Broadband untuk mengakses Internet sewaktu menggunakan aset ICT kerajaan tanpa sebarang kebenaran dan tanpa sebarang perlindungan seperti firewall; (p) Pengguna dilarang daripada memuat turun dan/atau mengubah sebarang perisian yang dimuat turun daripada Internet untuk mengelakkan berlakunya pelanggaran hak cipta terpelihara; (q) Internet tidak menjamin kerahsiaan maklumat. Maklumat sensitif yang dihantar melalui internet terdedah kepada risiko dikesan oleh pihak ketiga. Semua pekerja diminta untuk berhati-hati dan berwaspada apabila menghantar sebarang maklumat melalui Internet; (r) Setiap kakitangan MITI bertanggungjawab ke atas sebarang salah perlakuan dan tindakan yang diambil sewaktu menggunakan kemudahan Internet yang diberikan; dan (s) BPM juga berhak untuk memeriksa setiap komputer yang digunakan oleh kakitangan MITI untuk memastikan setiap arahan di dalam dasar ini dipatuhi oleh semua kakitangan.	
070303 Capaian *Public* WIFI	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Warga MITI tidak dibenarkan menggunakan capaian *public* WIFI percuma contohnya WIFI di premis makanan dan tempat awam untuk urusan rasmi MITI; dan (b) Dokumen yang hendak dihantar melalui *public* WIFI perlulah di *encrypt* dan mempunyai kata laluan.	Warga MITI

0704 Kawalan Capaian Sistem Pengoperasian

Objektif:
Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

070401 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: (a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan (b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: (a) Mengesahkan pengguna yang dibenarkan; (b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* dan (c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. 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) Mengehadkan dan mengawal penggunaan program; dan (d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	Pentadbir Sistem ICT

070402 Token Keselamatan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan token GPKI hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; (b) Token hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; (c) Perkongsian token untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Token yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; (d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Bahagian Kewangan, MITI; dan (e) Pelaksanaan hendaklah merujuk kepada Panduan Pengguna Token Portal GPKI MAMPU.	Warga MITI

0705 Kawalan Capaian Aplikasi dan Maklumat (Dalaman dan Luaran)

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

070501 Capaian Aplikasi dan Maklumat (Dalaman dan Luaran)	
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;	Pentadbir Sistem ICT

(b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); (c) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; (d) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah dibenarkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; dan (e) Semua sistem maklumat dan aplikasi (dalaman dan luaran) hendaklah dikenal pasti, direkodkan dan dikaji semula mengikut keperluan.	

0706 Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif:
Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.

070601 Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan mudah alih yang dibekalkan oleh MITI seperti telefon pintar, tablets dan yang seumpamanya hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan (b) Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih.	Warga MITI
070602 Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Capaian ke sistem dalaman MITI perlu melalui SSL VPN; (b) Kebenaran bertulis atau e-mel untuk capaian SSL VPN dan justifikasi permohonan bagi melaksanakan kerja jarak jauh hendaklah mendapat kelulusan daripada Pengarah BPM; dan	Warga MITI

(c) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	
070603 *Bring Your Own Device* (BYOD)	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna BYOD perlu memastikan keselamatan maklumat semasa menggunakan peralatan BYOD; (b) Pengguna BYOD adalah dilarang memasang perisian yang tidak dibenarkan oleh MITI; (c) Pengguna BYOD adalah dilarang memasang perisian yang mengganggu servis rangkaian MITI; (d) Mengaktifkan fungsi keselamatan katalaluan di setiap komputer riba / peranti; (e) Perkakasan BYOD hendaklah dilindungi oleh perisian Antivirus bagi mengelak penyebaran virus/malware/trogen dan lain-lain keatas pengguna MITI yang lain; (f) Pengguna BYOD perlu memastikan peranti yang digunakan menggunakan teknologi penyulitan (*encryption*), tandatangan digital atau sebarang mekanisme bagi melindungi maklumat elektronik semasa ianya digunakan; (g) Pengguna BYOD adalah dilarang menyalin dan membawa keluar maklumat organisasi dengan menggunakan peranti mudah alih dan media storan seperti USB, *external* HD dsb; (h) Pengguna BYOD perlu memadam dokumen elektronik dengan merincih secara elektronik/*'secure deletion*' selepas dokumen tidak lagi diguna pakai; dan (i) Pengguna BYOD adalah dilarang meninggalkan komputer riba / peranti di ruang pejabat yang terbuka tanpa menguncikannya dengan kabel keselamatan.	Warga MITI

BIDANG 08

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN INFRASTRUKTUR DAN SISTEM

0801 Keselamatan Dalam Proses Perolehan Untuk Pembangunan Infrastruktur dan Sistem

Objektif:
Memastikan mekanisme perolehan infrastruktur dan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian dan mematuhi peraturan dan pekeliling semasa yang berkuatkuasa.

080101 Mekanisme Perolehan Infrastruktur dan Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengenal pasti keperluan sebelum sebarang perolehan dilaksanakan sama ada perolehan daripada syarikat pembekal atau pembangunan secara dalaman. (b) Spesifikasi perolehan hendaklah mengandungi klausa tertentu berhubung keperluan keselamatan, pensijilan keselamatan produk, ketersediaan kod sumber, keperluan pelupusan data, keutamaan terhadap teknologi dan kepakaran tempatan, serta keperluan kompetensi pasukan pembangunan.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO
080102 Keperluan Keselamatan Infrastruktur dan Sistem Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujud sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (b) Ujian keselamatan hendaklah dijalankan ke atas data *input* untuk menyemak pengesahan dan integriti data yang dimasukkan;	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

(c) Memastikan data output adalah tepat berdasarkan data input yang dimasukkan; (d) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang ralat maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan (e) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan mematuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	
080103 Pengesahan Data Input dan Output	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan (b) Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem dan Pentadbir Sistem ICT

0802 Kawalan Kriptografi

Objektif:
Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

080201 Enkripsi	
Warga MITI hendaklah membuat enkripsi ke atas maklumat sensitif atau maklumat rahsia rasmi mengikut keperluan seperti penggunaan *encryption* dan kata laluan pada maklumat berkenaan (Contoh: penghantaran dokumen melalui e-mel, penggunaan SSL *certificate* (https) pada aplikasi).	Warga MITI
080202 Tandatangan Digital	
Penggunaan tandatangan digital adalah diwajibkan bagi pengurusan transaksi maklumat rahsia rasmi secara elektronik.	Warga MITI

080203 Pengurusan Infrastruktur Kunci Awam (*Public Key Infrastructure- PKI*)	
Pengurusan ke atas PKI hendaklah diuruskan dengan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Warga MITI

0803 Keselamatan Fail Sistem

Objektif:
Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.

080301 Kawalan Fail Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; (b) Kod sumber atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; (c) Mengawal capaian ke atas kod sumber atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan (e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem dan Pentadbir Sistem ICT

0804 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif:
Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

080401 Prosedur Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi pra-syarat pentauliahan sistem. Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan. (b) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (c) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggung jawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pihak ketiga; (d) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (e) Akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada pengguna yang diberi kebenaran; dan (f) Menghalang sebarang peluang kebocoran maklumat.	Pemilik Sistem dan Pentadbir Sistem ICT
080402 Pembangunan Perisian Secara *Outsource*	
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pentadbir/pemilik sistem. Kod sumber (*source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik MITI.	BPM dan Pentadbir Sistem ICT

0805 Kawalan Teknikal Keterdedahan (*Vulnerability*)

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

080501 Kawalan dari Ancaman Teknikal	
Kawalan teknikal dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memperoleh maklumat teknikal yang digunakan; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT

BIDANG 09

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:
Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

090101 Mekanisme Pelaporan	**Tanggungjawab**
Pusat Kawalan dan Koordinasi Siber Negara (NC4) menyediakan platform bagi perkongsian maklumat dan sistem pelaporan berkaitan insiden siber untuk seluruh Prasarana Maklumat Kritikal Negara (CNII). Insiden keselamatan ICT seperti di bawah hendaklah dilaporkan kepada ICTSO dan kumpulan MITI CSIRT dengan kadar segera: (a) Maklumat yang disyaki atau didapati hilang; atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat diguna atau disyaki digunakan tanpa kebenaran; (c) Kata laluan atau mekanisme kawalan akses yang hilang, dicuri atau disyaki hilang; (d) Berlaku insiden yang luar biasa seperti kehilangan fail, kegagalan sistem dan serangan luar jangka e-mel; dan (e) Berlaku percubaan pencerobohan, penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di MITI seperti di **Lampiran 2**. Prosedur pelaporan insiden keselamatan ICT berdasarkan: (a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan	Warga MITI

(b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	

0902 Pengurusan Maklumat Insiden Keselamatan ICT

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

090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada MITI. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; (d) Menyediakan tindakan pemulihan segera; dan (e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO

BIDANG 10

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 Dasar Kesinambungan Perkhidmatan

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

100101 Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan* - BCP) dan Pelan Pemulihan Bencana (*Disaster Recovery Plan* - DRP)	**Tanggungjawab**
BCP adalah di bawah tanggungjawab Bahagian Khidmat Pengurusan (BKP) dan DRP adalah di bawah tanggungjawab BPM. BCP dan DRP hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT MITI dan perkara-perkara berikut perlu diberi perhatian: (a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan dalam jangka masa yang ditetapkan; (c) Mendokumentasikan proses dan prosedur yang telah dipersetujui; dan (d) Mengadakan program latihan/simulasi kepada pengguna mengenai prosedur kecemasan sekurang-kurangnya setahun sekali. BCP dan DRP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:	ICTSO dan BPM

(a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai personel MITI/wakil dan vendor/wakil berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel); (c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan (e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan. Salinan BCP dan DRP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. BCP dan DRP hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian BCP dan DRP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. MITI hendaklah memastikan salinan BCP dan DRP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

BIDANG 11

PEMATUHAN

1101 Pematuhan dan Keperluan Perundangan

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

110101 Pematuhan Dasar	**Tanggungjawab**
Warga MITI hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MITI dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Sebarang pelanggaran terhadap Dasar Keselamatan ICT MITI akan dikenakan tindakan sewajarnya. Semua aset ICT di MITI termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna bagi mengesan penggunaan selain dari tujuan rasmi. Sebarang penggunaan aset ICT MITI selain daripada maksud dan tujuan adalah merupakan satu penyalahgunaan sumber MITI.	Warga MITI
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi piawaian pelaksanaan keselamatan ICT.	ICTSO

110103 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia supaya tidak berlaku penyalahgunaan.	Warga MITI
110104 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh Warga MITI adalah seperti di **Lampiran 3**.	Warga MITI
110105 Penguatkuasaan Dan Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT MITI boleh dikenakan tindakan tatatertib.	Warga MITI
110106 Pelaksanaan Audit Dalam dan Audit Luar	
Audit Dalam Semakan audit dalam adalah perlu bagi memastikan pematuhan terhadap peraturan dan polisi yang berkuat kuasa. Pasukan Audit Dalam yang terlatih hendaklah ditubuhkan bagi melaksanakan audit dalam. Audit Pematuhan ICT yang dikendalikan oleh Pasukan Audit Dalam yang dilantik hendaklah dilaksanakan setiap tahun. Skop pematuhan ICT hendaklah meliputi pematuhan terhadap DKICT MITI. **Audit Luar** Semakan audit luar adalah perlu bagi memastikan pematuhan kepada peraturan dan polisi yang sedang berkuat kuasa dan hasil semakan semula audit dalam.	BPM

Audit luar hendaklah dilaksanakan oleh pihak yang tiada kepentingan terhadap MITI dan sistem yang diaudit. Pensijilan khas audit luar seperti ISMS dan Pengurusan Kesinambungan Perkhidmatan, hendaklah dilaksanakan oleh badan yang diiktiraf oleh Kerajaan.	

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses sandaran sesuatu dokumen atau maklumat.
Bandwidth	Jalur Lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan
BCP	*Business Continuity Planning*
CDO	*Chief Digital Officer (*Ketua Pegawai Digital) yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
CNII	*Critical National Information Infrastructure* Infrastruktur Maklumat Kritikal Negara
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
DRP	*Disaster Recovery Planning*
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.

Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
Hard disk	Cakera keras Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
LAN *Local Area Network*	Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out* computer. Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *Trojan horse, worm, spyware* dan sebagainya.
MITI CSIRT	MITI *Computer Security Incident Response Team* bertanggungjawab ke atas pengurusan insiden dan keselamatan siber agensi.

Modem	Modulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari computer.
NC4	National Cyber Coordination and Command Centre Pusat Kawalan dan Penyelarasan Siber Negara
NACSA	National Cyber Security Agency Agensi Keselamatan Cyber Negara
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsifungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pekerja Sambilan	Personel Short-Term Employment Program (MySTEP)
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.
Pegawai Keselamatan MITI	Menyelaras urusan keselamatan MITI dengan teratur, cekap dan berkesan mengikut tatacara dan peraturan yang ditetapkan.
Pihak Ketiga	Pembekal perkhidmatan/Vendor/Agensi luar
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan computer

Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Warga MITI	Pegawai/Kakitangan yang berkhidmat di MITI.
Wireless	LAN Jaringan komputer yang terhubung tanpa melalui kabel.
URKI	Unit Rangkaian dan Keselamatan ICT

Lampiran 1

MITI-ISMS-DKICT-01

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT MITI

Nama (Huruf Besar) : ……..

No. Kad Pengenalan : ……..

Jawatan : ...……..

Bahagian : ……..

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa: -

Saya telah membaca, memahami dan akur akan peraturan-peraturan yang terkandung di dalam Dasar Keselamatan ICT MITI; dan

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

Tandatangan : ……

Tarikh : ……

Pengesahan Pegawai Keselamatan ICT

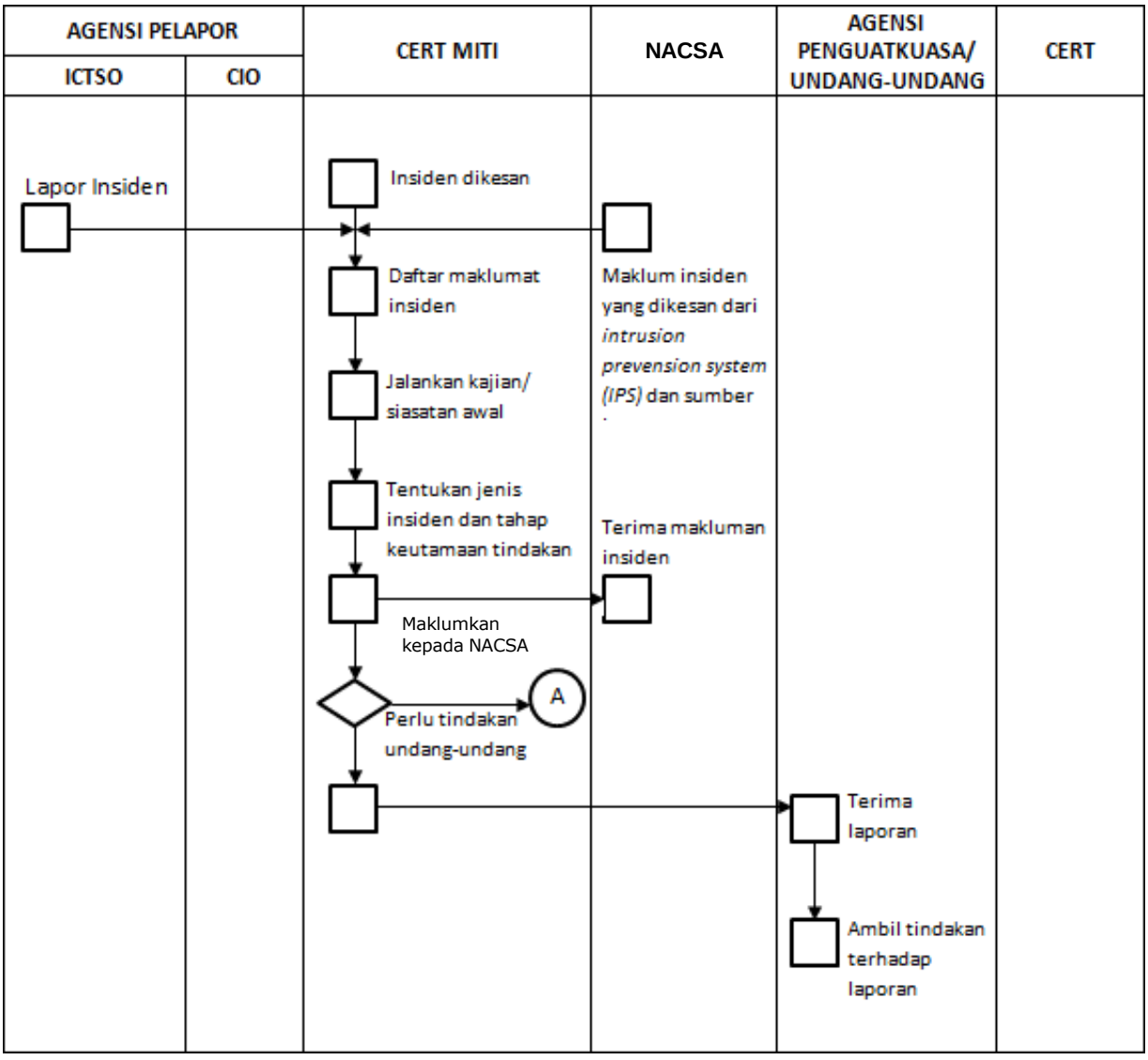
……
(Nama Pegawai Keselamatan ICT)

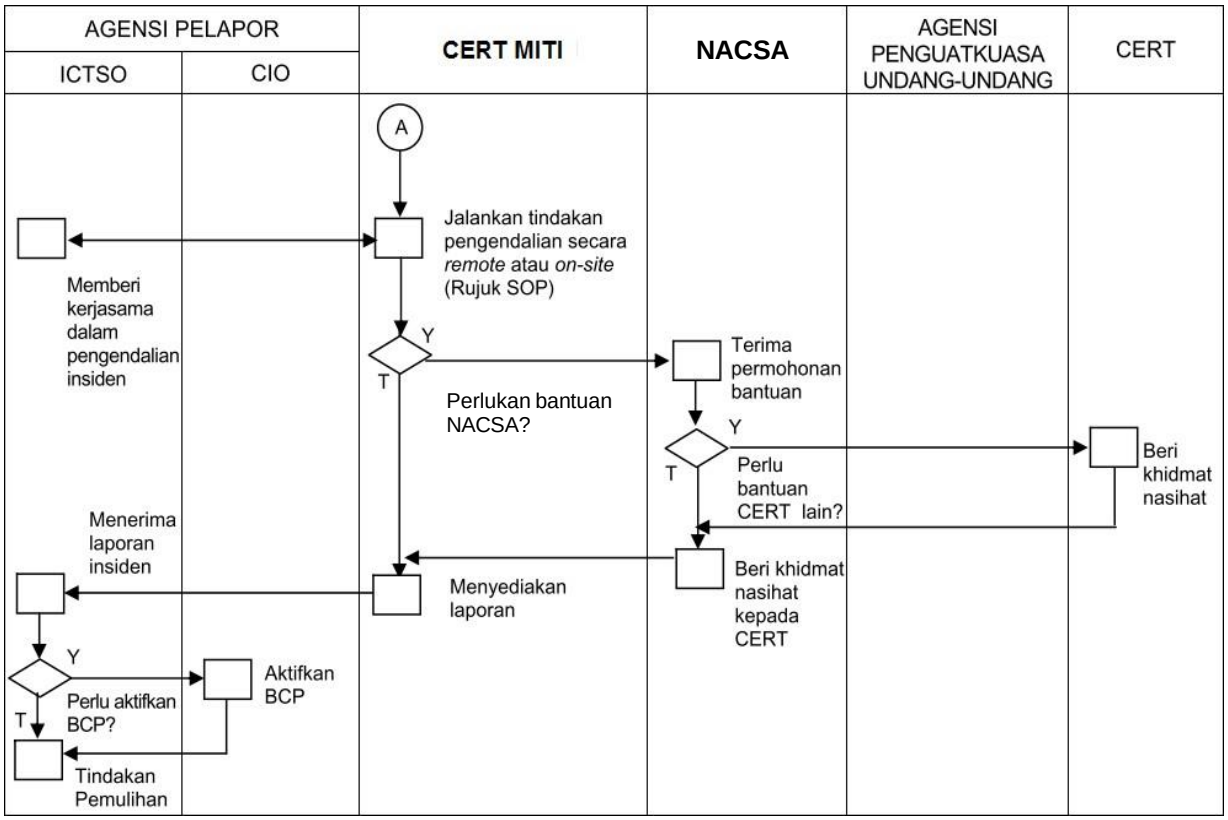
Tarikh : ……..

Nota : Semua warga MITI perlu membaca DKICT secara keseluruhan sebelum menandatangani Surat Akuan Pematuhan DKICT. DKICT boleh di capai di Portal MITI pada pautan *Our Services > Guidelines > ICT Security Policy*

Lampiran 2

PROSES KERJA PELAPORAN PENGENDALIAN INSIDEN ICT




AGENSI PELAPOR
ICTSO
CIO
CERT MITI
NACSA
AGENSI PENGUATKUASA UNDANG-UNDANG
CERT
A
Jalankan tindakan pengendalian secara remote atau on-site (Rujuk SOP)
Memberi kerjasama dalam pengendalian insiden
Y
T
Perlukan bantuan NACSA?
Terima permohonan bantuan
Y
T
Perlu bantuan CERT lain?
Beri khidmat nasihat
Menerima laporan insiden
Menyediakan laporan
Beri khidmat nasihat kepada CERT
Y
T
Perlu aktifkan BCP?
Aktifkan BCP
Tindakan Pemulihan

Lampiran 3

SENARAI PERUNDANGAN DAN PERATURAN

1. PEKELILING AM

A. PEKELILING AM BILANGAN 6 TAHUN 1999, PELAKSANAAN PERKONGSIAN PINTAR ANTARA AGENSI-AGENSI KERAJAAN DALAM BIDANG TEKNOLOGI MAKLUMAT

B. PEKELILING AM BIL. 3 TAHUN 2000 RANGKA DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI KERAJAAN (ICT)

C. PEKELILING AM BIL.1 TAHUN 2001 MEKANISME PELAPORAN INSIDEN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

D. PEKELILING AM BIL. 2 TAHUN 2002, PENGGUNAAN DAN PEMAKAIAN DATA DICTIONARY SEKTOR AWAM (DDSA) SEBAGAI STANDARD DI AGENSI-AGENSI KERAJAAN.

E. PEKELILING AM BILANGAN 2 TAHUN 2006, PENGUKUHAN TADBIR URUS JAWATANKUASA IT DAN INTERNET KERAJAAN

F. PEKELILING AM BIL. 1 TAHUN 2015, PELAKSANAAN DATA TERBUKA SEKTOR AWAM

2. SURAT PEKELILING AM

A. SURAT PEKELILING AM BIL. 6 TAHUN 2005, GARIS PANDUAN PENILAIAN RISIKO KESELAMATAN MAKLUMAT SEKTOR AWAM

B. SURAT PEKELILING AM BIL. 4 TAHUN 2006, PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT) SEKTOR AWAM

C. SURAT PEKELILING AM BIL. 3 TAHUN 2009, GARIS PANDUAN PENILAIAN TAHAP KESELAMATAN RANGKAIAN DAN SISTEM ICT SEKTOR AWAM

D. SURAT PEKELILING AM BILANGAN 3 TAHUN 2015, GARIS PANDUAN PERMOHONAN KELULUSAN TEKNIKAL DAN PEMANTAUAN PROJEK TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT) AGENSI SEKTOR AWAM

E. SURAT PEKELILING AM BIL. 4 TAHUN 2022: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT) SEKTOR AWAM.

3. <u>PEKELILING KEMAJUAN PENTADBIRAN AWAM (PKPA)</u>

A. PEKELILING KEMAJUAN PENTADBIRAN AWAM BIL. 1 TAHUN 2003, GARIS PANDUAN MENGENAI TATACARA PENGGUNAAN INTERNET DAN MEL ELEKTRONIK DI AGENSI-AGENSI KERAJAAN

B. PEKELILING KEMAJUAN PENTADBIRAN AWAM BIL. 2 TAHUN 2015, PENGURUSAN LAMAN WEB AGENSI SEKTOR AWAM

C. PEKELILING TRANSFORMASI PENTADBIRAN AWAM, BIL. 3 TAHUN 2017
PENGURUSAN PERKHIDMATAN KOMUNIKASI BERSEPADU KERAJAAN
(GOVERNMENT UNIFIED COMMUNICATION (1GOVUC))

D. PEKELILING TRANSFORMASI PENTADBIRAN AWAM BIL. 4 TAHUN 2017, PELAKSANAAN KUMPULAN WANG AMANAH PEMBANGUNAN PROJEK ICT SEKTOR AWAM (KWAICT)

E. PEKELILING TRANSFORMASI PENTADBIRAN AWAM BIL. 3 TAHUN 2018, PANDUAN PENGURUSAN PROJEK ICT SEKTOR AWAM (PPRISA)

4. SURAT ARAHAN KETUA PENGARAH MAMPU

A. LANGKAH-LANGKAH MENGENAI PENGGUNAAN MEL ELEKTRONIK DI AGENSI-AGENSI KERAJAAN (JUN 2007)

B. LANGKAH-LANGKAH PEMANTAPAN PELAKSANAAN SISTEM MEL ELEKTRONIK DI AGENSI-AGENSI KERAJAAN (NOVEMBER 2007)

C. GARIS PANDUAN PELAKSANAAN BLOG BAGI AGENSI SEKTOR AWAM (JULAI 2009)

D. PANDUAN PENYEDIAAN BERITA ONLINE DAN PENYIARAN BERITA ONLINE DI LAMAN WEBPORTAL AGENSI-AGENSI KERAJAAN (SEPTEMBER 2009)

E. PENGGUNAAN MEDIA JARINGAN SOSIAL DI SEKTOR AWAM (NOVEMBER 2009)

F. GARIS PANDUAN PENGGUNAAN ICT KE ARAH ICT HIJAU DALAM PERKHIDMATAN AWAM (2010)

G. GARIS PANDUAN TRANSISI PROTOKOL INTERNET VERSI 6 (IPV6) SEKTOR AWAM (JANUARI 2010)

H. PEMANTAPAN PENGGUNAAN DAN PENGURUSAN E-MEL DI AGENSI-AGENSI KERAJAAN (2010)

I. AMALAN TERBAIK PENGGUNAAN MEDIA JARINGAN SOSIAL (TARIKH 8 APRIL 2011)

J. PELAN STRATEGIK ICT SEKTOR AWAM 2016-2020 (DISEMBER 2016)

5. PERATURAN-PERATURAN PERKHIDMATAN DAN PENTADBIRAN

A. PERINTAH-PERINTAH AM

B. PERATURAN-PERATURAN PEGAWAI AWAM (PERLANTIKAN, KENAIKAN PANGKAT PENAMATAN PERKHIDMATAN) 2005

C. PERATURAN-PERATURAN PEGAWAI AWAM (KELAKUAN DAN TATATERTIB) 1993

D. PANDUAN PENGURUSAN PEJABAT (PP 5 TAHUN 2007)

E. PEKELILING KEMAJUAN PENTADBIRAN AWAM (PKPA)

F. PEKELILING PERKHIDMATAN DAN SURAT PEKELILING PERKHIDMATAN

G. PEKELILING AM DAN SURAT PEKELILING AM

H. 1PEKELILING PERBENDAHARAAN (1PP)

I. GARISAN PANDUAN PELAPORAN KEHADIRAN WARGA MITI BERDASARKAN SISTEM KAD AKSES (PEKELILING DALAMAN 1 TAHUN 2018)

J. GARISAN PANDUAN PELAKSANAAN EKOSISTEM KONDUSIF SEKTOR AWAM (EKSA)

K. AKTA ARKIB NEGARA MALAYSIA (AKTA 629)

L. ARAHAN PERBENDAHARAAN

M. AKTA PROSEDUR KEWANGAN 1957

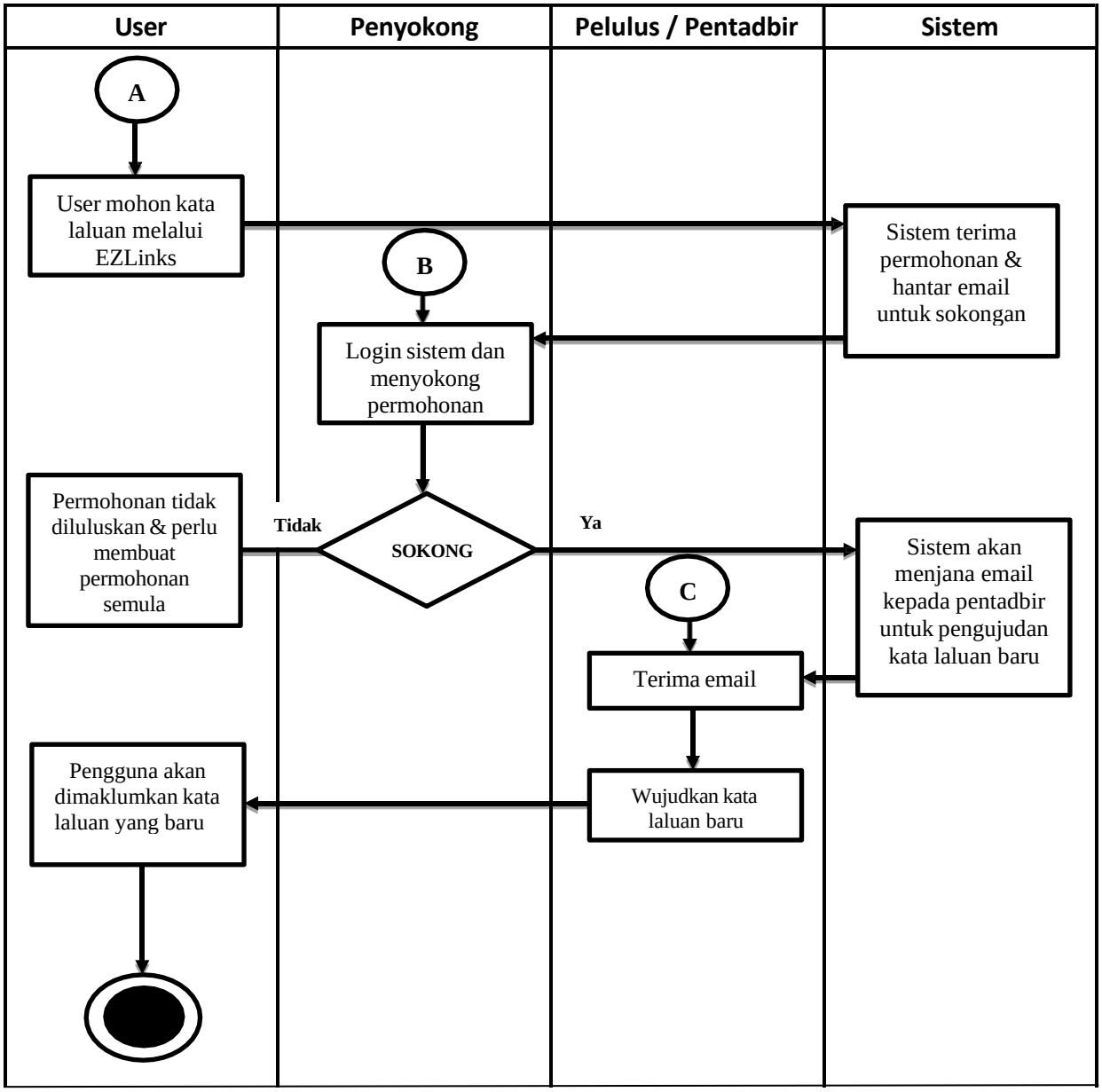
N. ARAHAN KESELAMATAN

O. DASAR KESELAMATAN ICT MITI

P. PELAN STRATEGIK ICT MITI

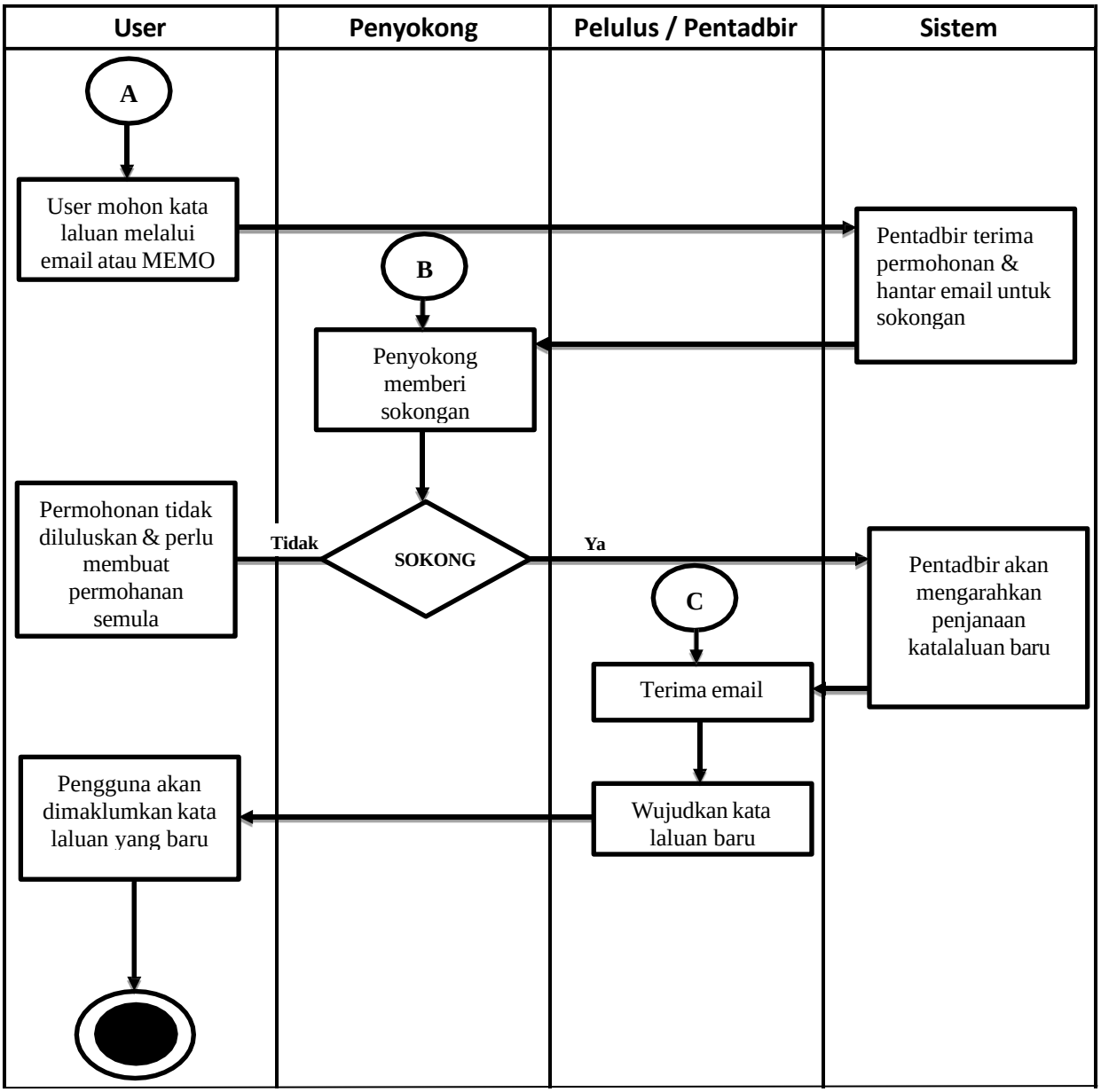
Lampiran 4

PROSES KELULUSAN KATA LALUAN E-MEL



Lampiran 5

PROSES KELULUSAN KATA LALUAN PENGGUNA SISTEM APLIKASI



Lampiran 6

BUTIRAN PINDAAN DASAR KESELAMATAN ICT MITI

BIL.	TARIKH	VERSI	BUTIR PINDAAN
1.	**30.3.2021**	**4.6**	1. Perkara 020107 Jawatankuasa Pemandu ICT MITI i. Mengeluarkan frasa "Urus Setia : BPM" kepada "Urus Setia : Unit EKP BPM" 2. Perkara 020108 Computer Security Incident ResponseTeam (MITI CSIRT). Kemaskini agensi MITI i. Personel ICT Malaysian Investment Development Authority (MIDA) ii. Personel ICT Malaysian External Trade Development Corporation (MATRADE) iii. Personel ICT Malaysia Productivity Corporation (MPC) iv. Personel ICT Malaysian Industrial Development Finance (MIDF) v. Personel ICT Malaysia Automotive Robotics and IoT Institute (MARii) vi. Personel ICT Malaysia Steel Institute (MSI) vii. Personel ICT Standard and Industrial Research Institute of Malaysia (SIRIM) viii. Personel ICT EXIM Bank ix. Personel ICT Jabatan Standard Malaysia x. Personel ICT InvestKL xi. Personel ICT Halal Development Corporation (HDC) xii. Personel ICT Majlis Rekabentuk Malaysia (MRM) xiii. Personel ICT National Metrology Institute of Malaysia (NMIM) 3. Perkara 020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga i. Penambahan (b) rujukan "MITI-ISMS- SP-SSMP-01"

BIL	TARIKH	VERSI	BUTIR PINDAAN
			4. Perkara 030201 Kategori Maklumat Kemaskini Merujuk kepada Akta Rahsia Rasmi 1972 [Akta 88], maklumat Rahsia Rasmi adalah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 [Akta 88] dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972. 5. Perkara 030203 Pengendalian Maklumat i. Mengemaskini (h) “Menjaga maklumat pengenalan peribadi (PII atau Personally Identifiable Information) daripada disebar dan disalahguna oleh pihak yang tidak bertanggungjawab” dan menggantikan kepada “Menjaga maklumat pengenalan peribadi PII daripada disebar dan disalahguna oleh pihak yang tidak bertanggungjawab.” 6. Kemaskini perkara 050201 Peralatan ICT i. Mengeluarkan frasa pada (x) “dicabut” kepada “ditanggalkan”. 7. Kemaskini perkara 060601 Kawalan Infrastruktur Rangkaian i. Mengeluarkan frasa pada (j) “dari Pejabat MITI Luar Negara 8. Perkara 060701 Penghantaran dan Pemindahan i. Penambahan frasa “dan peralatan” dan “ISMS BACKUP POLICY (MITI-ISMS- SP-BP)”

BIL	TARIKH	VERSI	BUTIR PINDAAN
			9. Perkara 060802 Pengurusan Mel Elektronik (E-mel) i. Mengeluarkan frasa pada (w) “adalah diberi mengikut gred seperti berikut:” dan diganti “kapasiti e-mel adalah 8GB”. ii. Mengeluarkan (x) iaitu “Penambahan kuota adalah berdasarkan sokongan pengarah bahagian masing-masing serta kelulusan pengarah BPM” iii. Penambahan frasa “pelajar latihan industri” dan “Pengarah Bahagian/Penyelia” 10. Kemaskini perkara 080201 Enkripsi i. Mengeluarkan frasa “pada setiap masa” diganti “mengikut keperluan” dan penambahan pada (Contoh: penghantaran dokumen melalui e-mel). 11. Kemaskini perkara 080203 Pengurusan Infrastruktur Kunci Awam (Public Key Infrastructure- PKI) i. Mengeluarkan frasa “dilakukan dengan berkesan dan” diganti “diuruskan dengan”. 12. Kemaskini perkara 090101 Mekanisme Pelaporan i. Mengeluarkan frasa pada (e) “menceroboh” diganti “pencerobohan”. 13. Penambahan pada Glosari i. NACSA - National Cyber Security Agency / Agensi Keselamatan Cyber Negara ii. Pekerja Sambilan - Personel Short-Term Employment Program (MySTEP)

BIL.	TARIKH	VERSI	BUTIR PINDAAN
2.	**30.7.2021**	**4.7**	Pindaan Klausa 061004 Pemantauan Log.
3.	**25.2.2022**	**4.8**	1. Perkara 020103 Pegawai Keselamatan ICT (ICTSO) i. Kemaskini Pengurus URKI kepada Pengurus Kanan Operasi 2. Perkara 050203 Media Tandatangan Digital i. Penambahan "Media Tandatangan Digital adalah teknologi yang digunakan untuk mengesahkan identiti penghantar/penandatangan sesuatu mesej dan digunakan bagi memastikan sesuatu maklumat adalah betul dan sah di dalam transaksi elektronik. Ia bukanlah imej tandatangan individu yang diimbas/softcopy." 3. Perkara 050402 Simpanan Data atas Talian (cloud storage) i. Mengeluarkan item "(c) Setiap dokumen yang disimpan di atas talian perlu ditetapkan kata laluan untuk membuka dokumen." 4. Perkara 060802 Pengurusan Mel Elektronik (E-mel) i. Mengeluarkan item "(c) Penggunaan e-mel rasmi MITI (@miti.gov.my) adalah untuk kegunaan urusan rasmi sahaja." ii. Mengeluarkan item "(n) Penghantaran e-mel bergambar (grafik) bagi jemputan/hebahan mesyuarat atau seminar perlulah menggunakan saiz yang kecil tidak melebihi 150KB bagi mengawal storan/quota dan prestasi server e-mel." iii. Kemaskini item (m) "10MB" kepada "25MB"

BIL.	TARIKH	VERSI	BUTIR PINDAAN
			iv. Kemaskini item (w) "Kuota kapasiti e-mel adalah 8GB" kepada "bergantung kepada penyedia perkhidmatan e-mel semasa" 5. Perkara 080201 Enkripsi i. Penambahan ayat "(Contoh: penghantaran dokumen melalui e-mel, penggunaan SSL certificate (https) pada aplikasi)." 6. Lampiran 2: Kemaskini perkataan "GCERT MAMPU" kepada "NACSA"
4.	**9.3.2023**	**4.9**	1. Kemaskini MITI CERT kepada MITI CSIRT. 2. Kemaskini kesemua dokumen yang mengandungi perkataan Pasukan Pengendali Insiden Keselamatan ICT (CERT) kepada Computer Security Incident Response Team (CSIRT). 3. Kemaskini kesemua dokumen yang mengandungi perkataan Chief Information Officer (CIO) kepada Chief Digital Officer (CDO). 4. Perkara 030201 Kategori Maklumat, Kemaskini Personal Identifiable Information (PII) kepada Maklumat Pengenalan Peribadi (Personal Identifiable Information (PII)). 5. Perkara 020108 Computer Security Incident Response Team (MITI CSIRT) i. menambah klausa (f) menyebarkan makluman berkaitan peranan dan tanggungjawab warga MITI dan agensi di dalam MITI CSIRT. 6. Pekara 060401 Perlindungan dari Perisian Berbahaya

BIL.	TARIKH	VERSI	BUTIR PINDAAN
			i. Menggantikan frasa pada item (f) 'mengendalikannya' kepada 'pengendalian' 7. Perkara 060501 Backup. i. Kemaskini item (a) 'Membuat backup keselamatan ke atas semua sistem perisian dan aplikasi sekurang- kurangnya sekali atau setelah mendapat versi terkini;' kepada 'Membuat backup ke atas semua sistem perisian dan aplikasi sekurang- kurangnya sekali;' 8. Perkara 060601 Kawalan Infrastruktur Rangkaian i. Menggantikan frasa pada item (d) 'proxy dan Web Content Filter' kepada 'content filtering' ii. Menggantikan frasa pada item (e) 'menceroboh' kepada 'pencerobohan' 9. Perkara 060802 Pengurusan Mel Elektronik (E-mel) i. Menggantikan frasa pada item (n) dan (o) 'cakera keras' kepada 'storan' 10. Perkara 061003 Sistem Log i. Menggantikan frasa pada item (c) 'ICTSO dan CIO' kepada 'MITI CSIRT' 11. Perkara 070201 Akaun Pengguna i. Mengeluarkan frasa pada item (b) 'bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan MITI' ii. Menambah frasa pada item (a) 'atau e-mel' Mengeluarkan item (b) 'Setiap permohonan mestilah dilengkapi dengan salinan Kad Pengenalan untuk individu atau salinan sijil pendaftaran syarikat dan penyata bank untuk syarikat;'

BIL.	TARIKH	VERSI	BUTIR PINDAAN
			12. Perkara 070203 Pengurusan Kata Laluan i. Mengeluarkan frasa pada item (a) 'dengan sesiapa pun' ii. Menambah item (e) 'sekurang- kurangnya satu huruf besar, satu huruf kecil, satu angka dan satu aksara khusus' dan mengeluarkan frasa 'dan mudah ditaip' iii. Mengelurkan frasa 'hendaklah diingat dan' iv. Penambahan item (l), (m) dan (n) 13. Perkara 070602 Kerja Jarak Jauh i. Menambah frasa pada item (b) 'atau e-mel' 14. Perkara 080401 Prodesur Kawalan Perubahan i. Mengeluarkan frasa pada item (e) 'diizinkan' dan menggantikan dengan frasa 'diberi kebenaran'
5.	**14.5.2024**	**4.10**	1. Perubahan logo dan nama kementerian dari Kementerian Perdagangan Antarabangsa dan Industri kepada Kementerian Pelaburan, Perdagangan dan Industri. 2. Perkara 020103 Pegawai Keselamatan ICT (ICTSO) ditukar dari Pengurus Kanan Operasi kepada Pengurus URKI BPM 3. Perkara 020108 Computer Security Incident Response Team (MITI CSIRT) - Kemaskini agensi MITI i. Personel ICT Malaysian Investment Development Authority (MIDA) ii. Personel ICT Malaysian External Trade Development Corporation (MATRADE) iii. Personel ICT Malaysia Productivity Corporation (MPC) iv. Personel ICT Malaysian Industrial Development Finance (MIDF) v. Personel ICT Malaysia Automotive Robotics and IoT Institute (MARii)

			vi. Personel ICT Malaysia Steel Institute (MSI) vii. Personel ICT Standard and Industrial Research Institute of Malaysia (SIRIM) viii. Personel ICT EXIM Bank ix. Personel ICT Jabatan Standard Malaysia x. Personel ICT InvestKL xi. Personel ICT Halal Development Corporation (HDC) xii. Personel ICT Majlis Rekabentuk Malaysia (MRM) xiii. Personel ICT National Metrology Institute of Malaysia (NMIM) xiv. National Aerospace Industry Coordinating Office (NAICO) xv. Collaborative Research in Engineering, Science and Technology (CREST)