KEMENTERIAN PELABURAN, PERDAGANGAN DAN INDUSTRI

POLISI KESELAMATAN SIBER

Versi 1.0

SEPTEMBER 9, 2025

KANDUNGAN

SEJARAH DOKUMEN

Versi	Kelulusan	Tarikh Kuatkuasa
1.0	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) MITI Bil 3 Tahun 2025	9 September 2025

GLOSARI

	ISTILAH	PENERANGAN
1.	Ancaman	Kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian.
2.	Antivirus	Perisian yang mengimbas virus pada media storan.
3.	APEG	Unit Automasi Pejabat & Electronic Government (EG)
4.	Aset ICT	Segala yang mempunyai nilai kepada Jabatan – perkakasan, perisian, perkhidmatan, data, maklumat dan manusia.
5.	Backup	Proses penduaan dokumen atau maklumat.
6.	Bandwidth	Jumlah data yang boleh dipindahkan melalui komunikasi dalam jangka masa tertentu.
7.	BPM	Bahagian Pengurusan Maklumat Kementerian Pelaburan, Perdagangan dan Industri
8.	CDO	Chief Digital Officer (Ketua Pegawai Digital)
9.	Clear Desk	Tidak meninggalkan dokumen sensitif di atas meja.
10.	Clear Screen	Tidak memaparkan maklumat sensitif apabila komputer ditinggalkan.
11.	CSIRT	Computer Security Incident Response Team membantu agensi menangani insiden keselamatan ICT.
12.	Denial of Service	Halangan pemberian perkhidmatan.

	ISTILAH	PENERANGAN
13.	Downloading	Aktiviti memuat turun perisian.
14.	DRT	Pasukan Pemulihan Bencana (Disaster Recovery Team).
15.	EKP	Unit Aplikasi EKP
16.	Encryption	Penyulitan data oleh pengirim supaya tidak difahami kecuali oleh penerima yang sah.
17.	Firewall	Sistem untuk menghalang capaian tidak sah ke rangkaian.
18.	Forgery	Pemalsuan dan penyamaran identiti, biasanya dalam e-mel.
19.	Hard Disk	Cakera keras untuk menyimpan dan mengakses data.
20.	Hub	Peranti yang menghubungkan stesen kerja dan menyiarkan data.
21.	ICT	Teknologi Maklumat dan Komunikasi (Information and Communication Technology).
22.	ICTSO	Pegawai Keselamatan ICT.
23.	IDS	Sistem Pengesan Pencerobohan – mengesan aktiviti tidak berkaitan atau berbahaya.
24.	Insiden Keselamatan	Musibah yang berlaku ke atas sistem maklumat.
25.	Internet	Sistem rangkaian global untuk capaian maklumat.
26.	Internet Gateway	Titik masuk ke rangkaian lain, memandu dan mengekalkan trafik.

	ISTILAH	PENERANGAN
27.	IP	Protokol Internet (Internet Protocol) merujuk kepada set peraturan yang mengawal cara data dihantar melalui internet, memastikan peranti boleh berkomunikasi antara satu sama lain.
28.	IPS	Sistem Pencegah Pencerobohan – menyekat atau menghalang aktiviti serangan.
29.	JPM	Jabatan Perdana Menteri
30.	Kriptografi	Sains penulisan kod rahsia untuk storan dan penghantaran data selamat.
31.	LAN	Local Area Network – rangkaian kawasan setempat.
32.	Logout	Keluar dari sistem atau aplikasi komputer.
33.	Malicious Code	Perisian/perkakasan yang dimasukkan tanpa kebenaran seperti virus, trojan, spyware.
34.	MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
35.	Mobile Code	Kod perisian yang berpindah antara komputer dan melaksanakan fungsi secara automatik.
36.	Outsource	Guna perkhidmatan luar untuk fungsi ICT tertentu.
37.	Penilaian Risiko	Penilaian kemungkinan bahaya, kerosakan atau kehilangan aset.
38.	Perisian Aplikasi	Perisian seperti pemproses kata, spreadsheet atau sistem aplikasi jabatan.
39.	Phising	Pancingan Data - sejenis penipuan dalam talian di mana penyerang cuba memperdaya

	ISTILAH	PENERANGAN
		individu supaya mendedahkan maklumat sensitif
40.	Pihak Ketiga	Kontraktor, Pembekal atau Perunding
41.	PKI	Public-Key Infrastructure – sistem keselamatan komunikasi dan transaksi internet.
42.	PKS	Polisi Keselamatan Siber
43.	Risiko	Kemungkinan berlakunya bahaya, kerosakan dan kerugian.
44.	Router	Penghala – menghantar data antara dua rangkaian.
45.	Screen Saver	Imej yang diaktifkan selepas komputer tidak digunakan seketika.
46.	Server	Pelayan komputer.
47.	Switches	Suis – gabungan hab dan titi untuk prestasi rangkaian yang lebih baik.
48.	Threat	Gangguan atau ancaman
49.	UAI	Unit Aplikasi Industri
50.	UO	Unit Operasi
51.	UPS	Uninterruptible Power Supply – bekalan kuasa berterusan semasa ketiadaan elektrik.
52.	URKI	Unit Rangkaian & Keselamatan ICT
53.	UTEK	Unit Khidmat Sokongan Teknikal
54.	Video Conference	Media paparan multimedia masa nyata kepada pengguna.

	ISTILAH	PENERANGAN
55.	Video Streaming	Komunikasi video dan audio serentak dari dua lokasi.
56.	Virus	Atur cara yang merosakkan data atau sistem.
57.	Vulnerability	Sebarang kelemahan aset yang boleh dieksploitasi oleh ancaman.
58.	Warga MITI	Meliputi keseluruhan kakitangan MITI
59.	Wireless LAN	Rangkaian komputer tanpa kabel.

1 TUJUAN

1.1 Polisi Keselamatan Siber (PKS) Kementerian Pelaburan, Perdagangan dan Industri (MITI) merupakan dokumen yang menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga MITI dan pihak ketiga yang mempunyai urusan dengan perkhidmatan digital MITI dalam melindungi maklumat di ruang siber.

2 LATAR BELAKANG

2.1 Polisi ini dibangunkan untuk menjamin kesinambungan perkhidmatan MITI dengan meminimumkan kesan insiden keselamatan siber. Polisi ini akan memudahkan perkongsian maklumat sesuai dengan keperluan operasi MITI bagi memastikan semua maklumat dilindungi.

3 OBJEKTIF

3.1 Objektif dokumen PKS ini dibangunkan adalah seperti berikut:

3.1.1 Menerangkan kepada semua pengguna yang merangkumi warga MITI dan pihak ketiga yang mempunyai urusan dengan perkhidmatan digital MITI mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber serta meningkatkan tahap kesedaran mengenai keselamatan siber;

3.1.2 Memastikan keselamatan penyampaian perkhidmatan MITI di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak-pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;

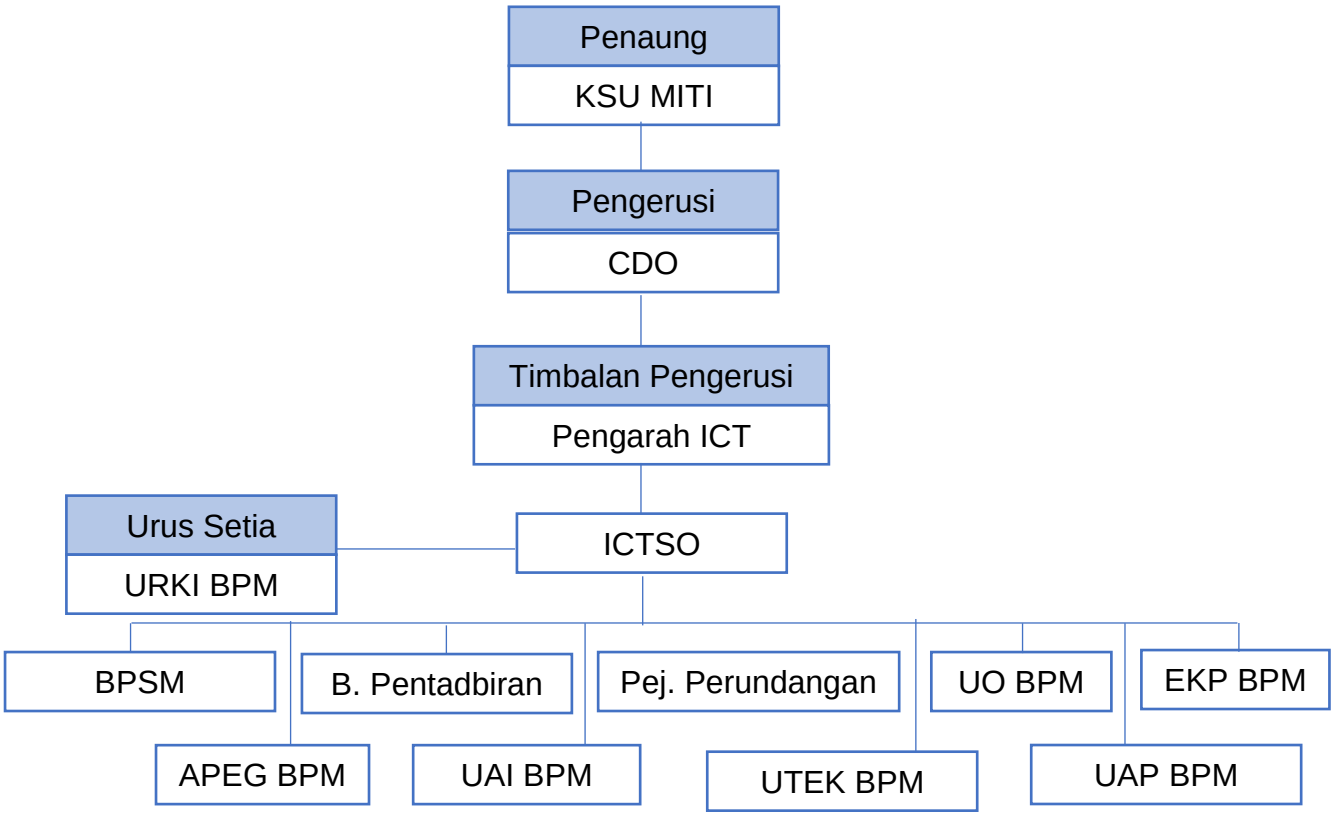
3.1.3 Memastikan kelancaran operasi MITI yang berlandaskan perkhidmatan digital dengan mencegah serta meminimumkan risiko kerosakan atau kemusnahan aset ICT;

3.1.4 Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, ketersediaan, kesahihan maklumat dan komunikasi; dan

3.1.5 Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

4 TADBIR URUS

4.1 Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKS MITI, satu (1) tadbir urus PKS telah diwujudkan seperti berikut:



Rajah 1: Struktur Tadbir Urus PKS MITI

4.2 Keahlian pasukan tadbir urus PKS MITI adalah seperti berikut:

Penaung:	Ketua Setiausaha (KSU)
Pengerusi:	Ketua Pegawai Digital (CDO)
Timbalan Pengerusi:	Pengarah ICT
Ketua Urus Setia:	ICTSO
Urus Setia:	Unit Rangkaian dan Keselamatan ICT (URKI)
Ahli:	i. Bahagian Pengurusan Sumber Manusia ii. Bahagian Pentadbiran

	iii. Pejabat Perundangan iv. Unit Operasi (UO) v. Unit Enterprise Knowledge Portal (EKP) vi. Unit Automasi pejabat & EG (APEG) vii. Unit Aplikasi Industri (UAI) viii. Unit Aplikasi Perdagangan (UAP) ix. Unit Khidmat Sokongan Teknikal (UTEK)

5 ASET ICT MITI

5.1 Aset ICT MITI merangkumi Maklumat, Aliran Data, Platform Aplikasi dan Perisian, Peranti Fizikal dan Sistem, Sistem Luaran serta Sumber Luaran seperti berikut:

5.1.1 Maklumat

Semua penyedia perkhidmatan dalam MITI hendaklah mengenal pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori berikut:

i. Maklumat Rahsia Rasmi

Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud Maklumat Rahsia Rasmi ialah 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 28 Akta Rahsia Rasmi 1972.

ii. Maklumat Rasmi

Maklumat rasmi ialah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh MITI semasa menjalankan urusan rasmi. Maklumat rasmi ini juga merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

iii. Maklumat Pengenalan Peribadi

Maklumat Pengenalan Peribadi (PII atau *Personally Identifiable Information*) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

iv. Data Terbuka

Data terbuka merujuk kepada data kerajaan yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan. PII dikecualikan daripada data terbuka.

5.1.2 Aliran Data

Aliran data merujuk kepada laluan lengkap data tertentu semasa transaksi. Aliran data dan komunikasi dalam MITI hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Saluran komunikasi termasuk:

i. Saluran komunikasi dan aliran data antara sistem di MITI;
ii. Saluran komunikasi dan aliran data ke sistem luar; dan
iii. Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

5.1.3 Platform Aplikasi dan Perisian

Semua platform aplikasi dan perisian hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

5.1.4 Peranti Fizikal dan Sistem

Semua peranti fizikal dan sistem hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Peranti fizikal termasuk:

i. Pelayan;
ii. Peranti/peralatan rangkaian;
iii. Workstation, komputer desktop/komputer riba;

iv. Telefon/peranti pintar;
v. Media storan;
vi. Peranti dengan sambungan ke rangkaian, contohnya mesin pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV);
vii. Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi Kerajaan; dan
viii. Peranti pengesahan (authentication devices), contohnya token keselamatan, dongle dan alat pengimbas biometrik.

5.1.5 Sistem Luaran

Sistem luaran adalah sistem bukan milik MITI yang dihubungkan dengan sistem MITI. Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dinilai tahap keselamatannya secara berkala.

5.1.6 Sumber Luaran

Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dinilai tahap keselamatannya secara berkala. Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi MITI. Contoh perkhidmatan sumber luaran ialah:

i. Perisian Sebagai Satu Perkhidmatan (SaaS);
ii. Platform Sebagai Satu Perkhidmatan (PaaS);
iii. Infrastruktur Sebagai Satu Perkhidmatan (IaaS);
iv. Storan Pengkomputeran Awan (*Cloud Storage*); dan
v. Pemantauan Keselamatan.

Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan, dikaji semula dan dipastikan keselamatannya secara berkala.

6 RISIKO

6.1 MITI hendaklah mengenal pasti risiko yang berkaitan dengan maklumat yang terlibat. Risiko ialah kebarangkalian sesuatu kecelakaan atau bencana berlaku yang menyebabkan kerosakan sehingga terjejas fungsi perkhidmatan sesuatu jabatan. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber MITI.

6.2 Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber MITI.

6.3 Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

6.3.1 Kerentanan (*Vulnerability*)

Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasi dan mengakibatkan pelanggaran keselamatan. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

6.3.2 Ancaman (*Threat*)

MITI hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

6.3.3 Impak (*Impact*)

MITI hendaklah menganggarkan impak insiden yang mungkin terjadi. lmpak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi MITI.

6.3.4 Tahap Risiko (*Risk Level*)

Tahap risiko ditentukan daripada ancaman, kebarangkalian dan impak risiko. Kaedah penentuan hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.

6.3.5 Penguraian Risiko (*Risk Mitigation*)

i. Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya.

ii. Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

a. Teknologi

Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, *firewall* digunakan untuk menghadkan capaian logikal kepada sistem tertentu.

b. Proses

Perekayasaan proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

c. Manusia

Mengenal pasti sumber manusia berkelayakan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.

6.3.6 Pengurusan Risiko (*Risk Management*)

i. Penyedia perkhidmatan digital di MITI hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:

a. mengenal pasti kerentanan;
b. mengenal pasti ancaman;
c. menilai risiko;
d. menentukan penguraian risiko;
e. memantau keberkesanan penguraian risiko; dan
f. memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

ii. Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya sekali setahun oleh Bahagian/Jabatan masing-masing dan dimaklumkan kepada Ketua Jabatan atau Jawatankuasa yang ditentukan oleh Ketua Jabatan.

7 PRINSIP KESELAMATAN

7.1 Prinsip keselamatan hendaklah dipilih berdasarkan penilaian risiko dan kategori maklumat yang dikendalikan oleh sistem. Bagi mencapai objektif keselamatan maklumat, MITI hendaklah melaksanakan prinsip keselamatan seperti yang berikut:

7.1.1 Prinsip “Perlu-Tahu” (*Need-to-Know*)

MITI hendaklah melaksanakan mekanisme bagi memberikan kebenaran kepada capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah berdasarkan prinsip “Perlu-Tahu” yang membenarkan capaian maklumat yang diperlukan untuk melaksanakan tugasnya sahaja.

Bagi capaian spesifik Maklumat Rahsia Rasmi, penggunaan yang dibenarkan hendaklah dihadkan kepada masa, lokasi, peranan dan fungsi pengguna tersebut.

7.1.2 Hak Keistimewaan Minimum (*Minimum Privilege*)

Pengguna hendaklah diberikan hak keistimewaan minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat.

Prinsip ini digunakan untuk menyekat hak akses kepada aplikasi, sistem, proses dan peranti kepada pengguna yang dibenarkan untuk melaksanakan aktiviti. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

7.1.3 Pengasingan Tugas (*Segregation of Duty*)

Bagi mengekalkan prinsip semak-dan-imbang (check and balance), MITI hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

7.1.4 Kawalan Capaian Berdasarkan Peranan (*Role Based Access Control*)

Capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut.

7.1.5 Peminimuman Data

Menghadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

8 TEKNOLOGI

8.1 Teknologi untuk melindungi data hendaklah dikenal pasti di semua peringkat pemprosesan data di setiap elemen pengkomputeran seperti berikut:

8.1.1 Peringkat Pemprosesan Data

i. Data-dalam-simpanan (*Data-at-Rest*)

MITI hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-simpanan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-simpanan.

Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

ii. Data-dalam-pergerakan (*Data-in-Motion*)

MITI hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-pergerakan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam pergerakan.

iii. Data-dalam-penggunaan (*Data-in-Use*)

MITI hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-penggunaan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Di samping itu, teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam penggunaan.

Teknologi yang bersesuaian boleh digunakan oleh MITI untuk memastikan asal data dan data/transaksi tanpa-sangkal.

iv. Perlindungan Ketirisan Data (*Data Leakage Protection*)

Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.

Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

8.1.2 Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, MITI hendaklah menggunakan kaedah teknologi dan kawalan keselamatan (*countermeasure and control measure*) yang dapat melindungi data di semua peringkat saluran pemprosesan bagi semua elemen dalam persekitaran pengkomputeran.

Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam persekitaran pengkomputeran mengikut Arahan Keselamatan yang dikeluarkan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) atau mendapat pengesahan daripada CGSO.

Setiap projek ICT yang dibangunkan di MITI hendaklah mempunyai Pelan Pengurusan Keselamatan Maklumat tersendiri yang mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

i. Peranti Pengkomputeran Peribadi
ii. Peranti Rangkaian
iii. Aplikasi

iv. Pelayan
v. Persekitaran Fizikal

9 PROSES

9.1 Warga MITI hendaklah melindungi keselamatan siber dengan melaksanakan perkara-perkara berikut:

9.1.1 Konfigurasi Asas

i. Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem.
ii. Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

9.1.2 Kawalan Perubahan Konfigurasi

i. Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.
ii. Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.
iii. Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

9.1.3 Sandaran

i. Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan.
ii. Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

9.1.4 Kitaran Pengurusan Aset

i. Pindah

a. Pemindahan hak milik aset berlaku dalam keadaan berikut:

- Warga MITI meninggalkan agensi disebabkan oleh persaraan, perletakkan jawatan atau penugasan semula;
- Aset yang dikongsi untuk kegunaan sementara;
- Pemberian aset kepada agensi lain; dan
- Aset dikembalikan setelah tamat tempoh sewaan

b. Data dalam peranti tersebut hendaklah diuruskan mengikut tatacara pelupusan di perkara (ii).

ii. Pelupusan

a. Pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya.
b. Berdasarkan keputusan CGSO, pelupusan perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara 2003 (Akta 629) dan Warta Kerajaan P.U.(A)377. Peraturan-Peraturan Arkib Negara (Penetapan Borang-Borang bagi Pelupusan Rekod Awam) 2008.
c. Pelupusan boleh dalam bentuk pemusnahan fizikal dan/atau sanitasi data.
d. Sanitasi data hendaklah mengikut garis panduan yang sedang berkuat kuasa.

9.1.5 Kitaran Hayat

i. Kitaran hayat data hendaklah diuruskan Akta Arkib Negara 2003 (Akta 629).
ii. Akta Arkib Negara 2003 (Akta 629) memberikan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

10 MANUSIA

10.1 Warga MITI, pembekal, pakar runding dan pihak-pihak berkepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

10.2 Sistem penyampaian perkhidmatan Kerajaan hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan. Kakitangan hendaklah dilatih dalam bidang pengkhususan yang diperlukan. Asas kecekapan pengguna hendaklah dibangunkan bagi semua warga MITI.

10.3 Kompetensi Pengguna

10.3.1 Kompetensi pengguna termasuk:

i. Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan siber dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan siber.
ii. Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga MITI berhubung alat-alat keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.

10.3.2 Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan pengguna selaras dengan arahan/pekeliling semasa adalah diharapkan.

10.4 Kompetensi Pelaksana

10.4.1 Warga MITI yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

10.4.2 Pegawai Keselamatan ICT hendaklah memenuhi syarat-syarat berikut:

i. Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.
ii. Memenuhi keperluan pembelajaran berterusan.
iii. Menimba pengalaman yang mencukupi dalam bidang keselamatan siber.

iv. Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.

10.4.3 Pegawai Keselamatan ICT yang dilantik oleh MITI hendaklah memenuhi keperluan kompetensi di atas. Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di MITI.

10.5 Peranan

10.5.1 Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.

10.5.2 Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani *Non-disclosure Agreement* (NDA) seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.

10.5.3 Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.

10.5.4 Warga MITI yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Jabatan dikembalikan sekiranya berlaku perubahan peranan.

10.5.5 Warga MITI yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan yang berkaitan seperti tersenarai dalam senarai aset Nota Serah Tugas.

10.5.6 Warga MITI lain yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Jabatan.

11 PELAN PENGURUSAN KESELAMATAN MAKLUMAT

11.1 Setiap projek yang berimpak tinggi di MITI hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain.

11.1.1 Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), Polisi Keselamatan Siber Kementerian Pelaburan, Perdagangan dan Industri (PKS MITI) dan surat pekeliling/arahan terkini untuk menangani isu-isu operasi projek.

11.2 Pelan ini hendaklah mengenal pasti perlindungan data-dalam-penggunaan, data-dalam pergerakan, data-dalam-simpanan dan menghalang ketirisan data.

11.3 Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

11.3.1 Peranti Pengkomputeran Peribadi

i. Peranti pengkomputeran merujuk kepada peranti komputer yang digunakan untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi adalah seperti komputer riba, workstation, telefon pintar, tablet dan peranti storan.

ii. Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran dari MITI. Walau bagaimanapun, peranti pengkomputeran peribadi milik persendirian adalah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang dibawa masuk ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

11.3.2 Peranti Rangkaian

i. Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti suis, penghala (*router*), *firewall* dan kabel.

ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

11.3.3 Aplikasi

i. Perian aplikasi yang digunakan untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi adalah pelayan web, pelayan aplikasi dan sistem pengoperasian.
ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi dalam-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

11.3.4 Pelayan

i. Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah ditempatkan di lokasi yang selamat.
ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi dalam-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

11.3.5 Persekitaran Fizikal

i. Persekitaran fizikal merujuk kepada lokasi yang menempatkan sistem ICT.
ii. MITI hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia untuk mendapatkan khidmat nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.
iii. Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip defence-in-depth.
iv. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi dalam-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

12 PERNYATAAN POLISI KESELAMATAN SIBER MITI

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

12.2 Pernyataan ini merangkumi perlindungan semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bagi memelihara keselamatan ruang siber dan ketersediaan maklumat kepada semua pengguna yang dibenarkan. Ciri-ciri Utama keselamatan maklumat adalah seperti berikut:

12.2.1 Kerahsiaan

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

12.2.2 Integriti

Data dan maklumat hendaklah tepat, lengkap dan kemas kini dan hanya boleh diubah dengan cara yang dibenarkan.

12.2.3 Tidak Boleh Disangkal

Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal.

12.2.4 Kesahihan

Data dan maklumat hendaklah dipastikan kesahihannya.

12.2.5 Ketersediaan

Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

12.3 Selain itu, langkah-langkah ke arah memelihara keselamatan siber hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan ICT MITI, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan.

12.4 Terdapat 14 bidang keselamatan dalam Polisi Keselamatan Siber MITI. 14 bidang tersebut adalah seperti berikut:

Bidang 01 – Polisi Keselamatan Maklumat

Bidang 02 – Organisasi Keselamatan Maklumat

Bidang 03 – Keselamatan Sumber Manusia

Bidang 04 – Pengurusan Aset

Bidang 05 – Kawalan Akses

Bidang 06 – Kriptografi

Bidang 07 – Keselamatan Fizikal dan Persekitaran

Bidang 08 – Keselamatan Operasi

Bidang 09 – Keselamatan Komunikasi

Bidang 10 – Pemerolehan, Pembangunan dan Penyenggaraan Sistem

Bidang 11 – Hubungan dengan Pembekal

Bidang 12 – Pengurusan Insiden Keselamatan ICT

Bidang 13 – Pengurusan Kesinambungan Perkhidmatan

Bidang 14 – Pematuhan

13 BIDANG 01 – POLISI KESELAMATAN MAKLUMAT

13.1 Hala Tuju Pengurusan Untuk Keselamatan Maklumat

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

13.2 Polisi Keselamatan Maklumat

13.2.1 Pelaksanaan Polisi

Pelaksanaan polisi 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 ICT.

Peranan: KSU/ CDO/ Pengarah ICT/ ICTSO/ Pengarah Kanan/ Pengarah ICT

13.2.2 Penyebaran Polisi

PKS MITI perlu disebarkan dan dihebahkan kepada warga MITI dan pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT MITI.

Peranan: ICTSO

13.2.3 Pematuhan Polisi

PKS MITI mestilah dipatuhi oleh semua warga MITI dan pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT MITI.

Peranan: Warga MITI dan Pihak Ketiga

13.3 Kajian Semula Polisi

PKS MITI adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur penyelenggaraan PKS MITI:

i. Kenal pasti dan tentukan perubahan yang diperlukan;
ii. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan dimaklumkan dalam Mesyuarat Jawatan Kuasa Pemandu ICT (JPICT);
iii. Maklum kepada semua pengguna akan perubahan terkini PKS MITI; dan

iv. Kaji semula polisi sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.

Peranan: ICTSO

14 BIDANG 02 – ORGANISASI KESELAMATAN MAKLUMAT

14.1 Perancangan Dalaman

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS MITI.

14.1.1 Peranan dan Tanggungjawab Keselamatan Maklumat

i. Ketua Setiausaha (KSU)

Peranan dan tanggungjawab KSU adalah seperti berikut:

a. Memastikan semua pengguna memahami peruntukan- peruntukan di bawah PKS MITI;
b. Memastikan semua pengguna mematuhi PKS 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.

ii. Ketua Pegawai Digital (Chief Digital Officer-CDO) – Timbalan Ketua Setiausaha (TKSU) Pelaburan dan Pengurusan (PP)

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 PKS MITI;
b. Menentukan keperluan keselamatan ICT; dan
c. Membangun dan menyelaraskan pelaksanaan pelan latihan dan program kesedaran keselamatan ICT.

iii. Pengarah ICT

Pengarah Bahagian Pengurusan Maklumat (BPM) merupakan Pengarah ICT MITI. Peranan dan tanggungjawab beliau adalah seperti berikut:

a. Memastikan semua pengguna memahami dan mematuhi PKS 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.

iv. Pegawai Keselamatan ICT (ICTSO)

Pengurus URKI BPM merupakan ICTSO MITI. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

a. Menyedia dan melaksanakan program-program kesedaran keselamatan ICT MITI;
b. Menguatkuasakan PKS MITI;
c. Memberi penerangan dan pendedahan berkenaan PKS MITI kepada semua pengguna;
d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS 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 marabahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
h. Melaporkan insiden keselamatan ICT kepada National Cyber Security Agency (NACSA), 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 pengguna yang melanggar PKS MITI; dan
m. Memberikan kebenaran hak akses yang berkaitan keselamatan ICT kepada pengguna ICT MITI.

v. 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;
c. Memantau aktiviti capaian harian pengguna;
d. Mengenal pasti dan mengambil tindakan serta-merta terhadap aktiviti-aktiviti yang meragukan seperti 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 bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.

vi. Jawatankuasa Pemandu ICT (JPICT)

Peranan dan tanggungjawab JPICT seperti yang terkandung dalam Surat Pekeliling Am Bil 3 Tahun 2015 iaitu merancang dan menentukan langkah-langkah keselamatan siber.

vii. MITI Computer Security Incident Response Team (MITI CSIRT)

Peranan dan tanggungjawab adalah merujuk kepada dokumen MITI CSIRT.

viii. Pengguna

Peranan dan tanggungjawab pengguna adalah seperti berikut:

a. Membaca, memahami dan mematuhi PKS MITI;
b. Mengetahui dan memahami implikasi keselamatan ICT serta kesan daripada tindakan ketidakpatuhan terhadap PKS MITI;
c. Melaksanakan prinsip-prinsip PKS dan menjaga kerahsiaan maklumat MITI;
d. Melaksanakan langkah-langkah perlindungan seperti berikut:
e. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
f. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
g. Menentukan maklumat sedia untuk digunakan;
h. Menjaga kerahsiaan kata laluan;
i. Mematuhi standard, prosedur, langkah garis panduan keselamatan yang ditetapkan;
j. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
k. Menjaga kerahsiaan maklumat-maklumat terperingkat berkaitan keselamatan ICT.
l. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;
m. menghadiri program-program kesedaran keselamatan ICT; dan
n. menandatangani Surat Akuan Pematuhan PKS MITI sebagaimana di Lampiran 1.

ix. 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; dan
i. Menyelaras Mesyuarat Jawatankuasa Keselamatan.

14.1.2 Pengasingan Tugas

Seseorang yang dilantik perlu mempunyai pengetahuan atau pengalaman dalam bidang ICT.

Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;
ii. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi;
iii. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan di dalam production environment. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan
iv. Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

Peranan: Pengarah ICT

14.1.3 Hubungan Dengan Pihak Berkuasa

Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara- perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab MITI;
ii. Mewujud dan mengemas kini prosedur / senarai pihak yang mempunyai kuasa penyiasatan dan penguatkuasaan atau pihak yang dihubungi semasa kecemasan. Pihak yang mempunyai kuasa penyiasatan dan penguatkuasaan adalah seperti Polis Diraja Malaysia, Suruhanjaya Komunikasi Dan Multimedia dan NACSA. Pihak yang dihubungi semasa kecemasan adalah termasuk pihak pembekal utiliti, perkhidmatan kecemasan, keselamatan dan kesihatan pekerjaan, *fire and rescue*; dan
iii. Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden dan tidak berkompromi kepada sebarang aktiviti pelanggaran.

Peranan: MITI CSIRT dan Warga MITI

14.1.4 Hubungan Dengan Kumpulan Berkepentingan Khusus

Hubungan baik dengan kumpulan berkepentingan khusus dan kumpulan pakar/profesional keselamatan maklumat hendaklah dikekalkan melalui amalan berikut:

i. Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat;
ii. Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat yang terkini;
iii. Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan
iv. Berhubung dengan kumpulan pakar/profesional keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.

Peranan: BPM

14.1.5 Keselamatan Maklumat Dalam Pengurusan Projek

Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Keselamatan maklumat perlu diintegrasikan dalam setiap pengurusan projek MITI;
ii. Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;
iii. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan;
iv. Dokumen kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam PKS MITI; dan
v. Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai kelayakan dan pengalaman yang berkaitan.

Peranan: Pemilik Projek

14.2 Peranti Mudah Alih dan Telekerja

Memastikan keselamatan maklumat dan aset MITI terpelihara ketika menggunakan peranti mudah alih aset MITI atau milik persendirian dan semasa bekerja secara jarak jauh (telekerja).

14.2.1 Peranti Mudah Alih

i. Mengawal peranti mudah alih milik persendirian daripada mencapai maklumat Rahsia Rasmi dan hendaklah mematuhi polisi serta prosedur yang ditetapkan untuk dibawa masuk ke Pejabat MITI;
ii. Mematuhi piawaian keselamatan minimum yang ditetapkan bagi semua peranti mudah alih yang digunakan untuk mengakses maklumat MITI;
iii. Melindungi peranti dengan kata laluan yang kuat, penyulitan data, dan perisian keselamatan terkini (*antivirus, anti-malware*);
iv. Mengawal pemasangan aplikasi dan tidak memasang aplikasi dari sumber yang tidak dipercayai;
v. Menyimpan peranti di tempat yang selamat apabila tidak digunakan; dan

vi. Menanggung kos utiliti seperti bil telefon, bil elektrik, sewaan jalur lebar, pembaikan kerosakan peranti mudah alih dan sebagainya.

Peranan: Warga MITI dan Pihak Ketiga

14.2.2 Telekerja

Melaksanakan dasar dan langkah-langkah keselamatan sokongan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja.

Peranan: Warga MITI

15 BIDANG 03 – KESELAMATAN SUMBER MANUSIA

15.1 Keselamatan Sumber Manusia Dalam Tugas Harian

Memastikan warga MITI dan pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT MITI dapat memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.

15.1.1 Tapisan Keselamatan

Tapisan keselamatan hendaklah dijalankan terhadap warga MITI dan pihak ketiga selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga MITI dan pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan
ii. Menjalankan tapisan keselamatan untuk warga MITI dan 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.

Peranan: Warga MITI dan Pihak Ketiga

15.1.2 Perakuan Akta Rahsia Rasmi

Selaras dengan Akta Rahsia Rasmi 1972 (Akta 88) dan Arahan Keselamatan (Semakan dan Pindaan 2017), perkara-perkara berikut perlu dipatuhi:

i. Warga MITI wajib menandatangani borang Lampiran C: Perakuan Rahsia Rasmi setiap tahun; dan Lampiran D: Perakuan apabila meninggalkan perkhidmatan kerajaan.
ii. Pihak ketiga termasuk komuniti keselamatan atau mana-mana pihak lain yang berurusan dengan perkhidmatan awam atau yang berkhidmat di kediaman rasmi kerajaan wajib menandatangani borang:
iii. Lampiran E: Perakuan Rahsia Rasmi; dan
iv. Lampiran F: Perakuan apabila tamat kontrak perkhidmatan dengan kerajaan.

Peranan: Warga MITI dan Pihak Ketiga

15.1.3 Terma dan Syarat Perkhidmatan

Persetujuan berkontrak dengan warga MITI dan pihak ketiga hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:

i. Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga MITI dan pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT MITI yang terlibat dalam menjamin keselamatan aset ICT; dan
ii. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

Peranan: Warga MITI dan Pihak Ketiga

15.2 Dalam Tempoh Perkhidmatan

Memastikan warga MITI dan pihak ketiga mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

15.2.1 Tanggungjawab Pengurusan

Memastikan pegawai dan kakitangan MITI serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MITI.

Peranan: Warga MITI dan Pihak Ketiga

15.2.2 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat

Warga MITI dan pihak ketiga perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Memastikan kesedaran, pendidikan dan latihan yang berkaitan PKS MITI, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/ fungsi/ aplikasi/ sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka;
ii. Memastikan kesedaran yang berkaitan PKS MITI perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan
iii. Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.

Peranan: Warga MITI dan Pihak Ketiga

15.2.3 Proses Tatatertib

Proses tatatertib yang formal dan disampaikan kepada warga MITI hendaklah tersedia bagi membolehkan tindakan diambil terhadap warga MITI yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Memastikan adanya proses tindakan disiplin dan/ atau undang-undang ke atas warga MITI sekiranya berlaku pelanggaran terhadap perundangan dan peraturan yang ditetapkan oleh MITI; dan
ii. Warga MITI yang melanggar polisi ini akan dikenakan tindakan tatatertib atau boleh ditarik semula kemudahan ICT MITI yang dibekalkan.

Peranan: Pengarah ICT dan Ketua Unit Integriti

15.3 Penamatan dan Pertukaran Perkhidmatan

Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas warga MITI diurus dengan teratur.

15.3.1 Penamatan atau Pertukaran Perkhidmatan

Warga MITI yang telah tamat perkhidmatan perlu mematuhi perkara-perkara berikut:

i. Memastikan semua aset ICT dikembalikan kepada MITI mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan;
ii. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan pemprosesan maklumat mengikut peraturan yang ditetapkan MITI dan/atau terma perkhidmatan yang ditetapkan;
iii. Melaksanakan sandaran e-mel; dan
iv. Maklumat rasmi MITI terperingkat dalam peranti tidak dibenarkan dibawa keluar dari MITI.
v. Warga MITI yang bertukar keluar hendaklah:

a. Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada MITI mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan;
b. Melaksanakan sandaran e-mel;
c. Menyedia dan menyerahkan nota serah tugas dan MyPortfolio kepada penyelia yang berkaitan;

Peranan: BPM dan Warga MITI

16 BIDANG 04 – PENGURUSAN ASET

16.1 Tanggungjawab Terhadap Aset

Untuk mengenal pasti aset bagi memberikan dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MITI.

16.1.1 Inventori Aset

Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT MITI. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara

Peranan: Pegawai Penerima Aset,
Pegawai Aset dan Warga MITI

16.1.2 Pemilikan Aset

Aset yang boleh diselenggara hanyalah aset hak milik MITI. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut:

i. Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori serta sentiasa dikemaskini;
ii. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;
iii. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MITI;
iv. Mengenal pasti, mendokumenkan dan melaksanakan peraturan bagi pengendalian aset ICT;
v. Mengenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan;
vi. Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan
vii. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.

Peranan: Pegawai Aset dan Warga MITI

16.1.3 Penggunaan Aset yang Dibenarkan

Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.

i. Peminjaman

Langkah-langkah yang perlu diambil termasuklah seperti yang berikut:

a. Mendapatkan kelulusan bagi tujuan peminjaman aset;
b. Melindungi dan mengawal peralatan sepanjang masa;
c. Merekodkan aktiviti peminjaman dan pemulangan peralatan; dan
d. Menyemak peralatan ketika peminjaman dan pemulangan dilakukan.

ii. Pemulangan

Memastikan semua aset ICT dikembalikan mengikut peraturan dan/atau status perkhidmatan pegawai yang:

a. Bertukar keluar;
b. Bersara;
c. Ditamatkan perkhidmatan; dan

d. Diarahkan oleh Ketua Jabatan.

Membatalkan atau menarik balik semua kebenaran pemilikan ke atas aset ICT mengikut peraturan yang ditetapkan.

Peranan: Pegawai Aset ICT, Pengguna

16.2 Pengelasan Maklumat

Memastikan maklumat dan aset ICT MITI diberikan tahap perlindungan yang bersesuaian.

16.2.1 Pengelasan Maklumat

Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan.

Peranan: Pegawai Pengelas

16.2.2 Pelabelan Maklumat

Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.

Peranan: Warga MITI

16.2.3 Pengendalian Aset

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa dan menentukan maklumat adalah 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. Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan;

vii. Memastikan maklumat terperingkat yang disimpan di dalam storan dalaman atau luaran (*internal* atau *external hard disk*) diberi perlindungan melalui kaedah enkripsi yang bersesuaian; dan

viii. Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.

Peranan: Warga MITI

16.3 Pengendalian Media

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

16.3.1 Pengurusan Media Boleh Alih

Media boleh alih merujuk kepada peranti storan yang mudah dialihkan daripada sistem komputer dan direka sebagai mudah alih (*portable*) seperti pemacu kilat USB, pemacu cakera keras luaran, CD, DVD dan kad memori.

Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh MITI. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut:

i. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;
ii. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;
iii. Mengehadkan kemasukan ke kawasan pemprosesan/penyimpanan media kepada Pegawai yang dibenarkan sahaja;
iv. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;
v. Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan;
vi. Menyimpan semua jenis media di tempat yang selamat dan terhad kepada Pegawai yang dibenarkan sahaja; dan
vii. Kehilangan media storan hendaklah dilaporkan mengikut prosedur pelaporan insiden.

Peranan: Pentadbir Sistem dan Pengguna

16.3.2 Pelupusan Media

Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.

Peranan: Pentadbir Sistem dan Jawatankuasa Pelupusan Aset.

16.3.3 Pemindahan Media Fizikal

Media yang mengandungi maklumat perlu dilindungi daripada akses tanpa izin, penyalahgunaan atau kerosakan semasa dipindahkan. Media yang dimaksudkan juga adalah termasuk dokumen dalam bentuk fizikal.

Perkara-perkara berikut perlu dipertimbangkan semasa pemindahan dilakukan seperti berikut:

i. Melantik perkhidmatan pengangkutan atau kurier yang melalui tatacara perolehan semasa;
ii. Pembungkusan perlu bersesuaian bagi melindungi aset daripada kerosakan fizikal yang mungkin berlaku semasa proses pemindahan; dan
iii. Rekod atau log perlu disimpan untuk mengenalpasti kandungan media, perlindungan yang digunakan serta rakaman semasa pemindahan kepada penjaga transit dan penerimaan di destinasi.

Peranan: Warga MITI

17 BIDANG 05 – KAWALAN AKSES

Menghadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas aset ICT.

17.1 Dasar Kawalan Akses

17.1.1 Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong kawalan capaian pengguna sedia ada.

Peranan: Pentadbir Sistem

17.2 Pengurusan Capaian Pengguna

17.2.1 Pendaftaran Pengguna

Pengguna dan pentadbir sistem perlu memastikan proses pendaftaran dilakukan secara selamat, teratur dan mematuhi prosedur yang ditetapkan.

Peranan: Pentadbir Sistem dan Warga MITI

17.2.2 Hak Capaian

Penetapan dan penggunaan hak capaian perlu diberi kawalan dan penyeliaan yang ketat, atas prinsip perlu mengetahui (need-to-know-basis). Keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pegawai MITI yang dibenarkan sahaja.

Peranan: Pentadbir Sistem

17.2.3 Pengurusan Kata Laluan

Kawalan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah dipastikan selamat dan kukuh.

Peranan: Pentadbir Sistem dan Warga MITI

17.3 Capaian Sistem Pengoperasian

17.3.1 Kawalan Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem pengoperasian perlu digunakan untuk menghalang capaian terhadap sistem komputer. Kemudahan ini juga perlu bagi :

i. Mengenal pasti identiti/terminal/lokasi bagi setiap pengguna yang dibenarkan;
ii. Merekodkan capaian yang berjaya dan gagal; dan
iii. Membolehkan pengesahan kata laluan dilaksanakan berdasarkan kriteria kata laluan yang kukuh.

Peranan: Pentadbir Sistem

17.3.2 Token/ Sijil Digital

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Penggunaan token Kerajaan Elektronik (Token EG) atau sijil digital hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan;
ii. Token hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain;
iii. Perkongsian penggunaan token adalah tidak dibenarkan sama sekali; dan
iv. Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pihak yang mengeluarkan token.

Peranan: Warga MITI

17.4 Capaian Aplikasi dan Maklumat

Capaian sistem dan aplikasi di MITI adalah terhad kepada pengguna bagi tujuan melindungi sistem maklumat dan aplikasi sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan.

Peranan: Pentadbir Sistem

17.5 Capaian Jarak Jauh

Kawalan capaian jarak jauh bertujuan memastikan akses rangkaian luar ke sistem dalaman MITI terlindung dari sebarang bentuk pelanggaran keselamatan yang boleh menjejaskan privasi dan integriti data.

i. Capaian jarak jauh yang dimaksudkan merangkumi:

a. Capaian daripada sistem rangkaian dalaman; dan
b. Capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan *teleworking*.

ii. Penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (*encryption*);
iii. Lokasi bagi capaian ke sistem ICT MITI hendaklah dipastikan selamat;

iv. Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada ICTSO. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini; dan
v. Capaian jarak jauh hendaklah menggunakan kemudahan yang disediakan oleh MITI.

Peranan: ICTSO, Pentadbir Sistem, Warga MITI

17.6 Kawalan Capaian Rangkaian

17.6.1 Capaian Rangkaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

i. Mewujudkan segmen rangkaian yang bersesuaian bagi membezakan di antara rangkaian MITI dan rangkaian awam;
ii. Mewujudkan dan menguatkuasakan mekanisma untuk pengesahan pengguna dengan peralatan yang menepati kesesuaian penggunaannya;
iii. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT;
iv. Capaian pengguna jarak jauh (*remote user*) tidak dibenarkan;
v. Capaian fizikal dan logikal ke atas peralatan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal.

Penggunaan Internet MITI hendaklah dipantau secara berterusan oleh pentadbir rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kawalan ini akan dapat melindungi daripada sebarang bentuk ancaman ke atas rangkaian MITI.

Peranan: Pentadbir Rangkaian

17.7 Peralatan Mudah Alih

Kawalan keselamatan peralatan mudah alih adalah penting untuk melindungi data dan sistem dalam era kerja mudah alih dengan mengurangkan risiko keselamatan, meningkatkan produktiviti serta piawaian keselamatan. Peralatan mudah alih yang

dibekalkan oleh MITI hendaklah dilindungi dan perkara yang perlu dipatuhi adalah seperti berikut:

i. Merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan pergerakan peralatan tersebut daripada kehilangan atau kerosakan;
ii. Peralatan mudah alih hendaklah disimpan atau dikunci di tempat yang selamat apabila tidak digunakan; dan
iii. Memastikan peralatan mudah alih yang dibawa keluar dari pejabat perlu disimpan dan dijaga dengan baik bagi mengelakkan daripada kecurian.

Peranan: Pegawai Aset ICT dan Warga MITI

17.8 *Bring Your Own Device* (BYOD)

Kawalan penggunaan BYOD perlu dikawal menggunakan borang kebenaran penggunaan peralatan BYOD serta tertakluk kepada SOP MITI.

Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD.

Peranan: Warga MITI

17.9 Perkhidmatan E-Dagang

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

Peranan : Warga MITI

17.10 Kawalan Perwujudan Domain

Kawalan perwujudan domain yang teratur melibatkan perancangan nama, pendaftaran, konfigurasi DNS dan penyelenggaraan. Dengan langkah yang betul domain dapat berfungsi dengan lancar dan selamat bagi membolehkan penggunaanya untuk laman web , email serta aplikasi lain.

Peranan: Pengarah ICT / ICTSO

18 BIDANG 06 – KRIPTOGRAFI

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

18.1 Enkripsi

Warga MITI hendaklah membuat enkripsi ke atas maklumat sensitif atau maklumat rahsia rasmi mengikut keperluan.

Peranan: Warga MITI

18.2 Tandatangan Digital

Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan.

Peranan: Warga MITI

18.3 Pengurusan Infrastruktur Kunci Awam (*Public Key Infrastructure - PKI*)

Pengurusan ke atas PKI hendaklah diuruskan dengan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.

Peranan: Warga MITI

18.4 Data Masking

Tujuan data masking adalah untuk mengehadkan keterdedahan perkongsian paparan data-data peribadi dalam pelbagai medium yang boleh mengundang penyalahgunaan data individu.

Data yang perlu dilindungi ialah data sensitif seperti data peribadi (*Personally Identifiable Information - PII*) dan data ini tidak boleh dipaparkan dalam paparan pengguna sistem dan sekiranya dikeluarkan daripada sistem, data tersebut perlu digantikan dengan nilai yang tidak dapat dikenalpasti atau dihubungkan kembali ke data asal.

Peranan: Pentadbir Sistem dan Pihak Ketiga

19 BIDANG 07 – KESELAMATAN FIZIKAL DAN PERSEKITARAN

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

19.1 Keselamatan Kawasan

19.1.1 Kawalan Kawasan

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi.Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan tahap keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;
ii. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
iii. Memasang alat penggera dan pemantauan persekitaran melalui Sistem CCTV atau peralatan-peralatan lain yang sesuai;
iv. Mengehadkan jalan keluar masuk dan memastikan butiran pelawat direkodkan;
v. Mengadakan kaunter kawalan;
vi. Menyediakan tempat menunggu atau bilik khas untuk pelawat-pelawat;
vii. Mewujudkan perkhidmatan kawalan keselamatan;
viii. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;
ix. Mereka bentuk dan melaksanakan keselamatan fizikal berdasarkan kepada Arahan Keselamatan (CGSO) di dalam pejabat, bilik dan kemudahan kawasan umum;
x. Mereka bentuk dan melaksanakan perlindungan fizikal berdasarkan kepada Arahan Keselamatan (CGSO) daripada kecurian, kebakaran, banjir, letupan, rusuhan serta bencana alam seperti banjir dan gempa bumi;
xi. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad yang diwartakan seperti Bilik Fail dan Pusat Data; dan
xii. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.

Peranan: Pegawai Keselamatan MITI

19.1.2 Kawalan Masuk Fizikal

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

i. Setiap warga MITI termasuk pekerja sementara hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;
ii. Semua pas keselamatan hendaklah diserahkan semula kepada Bahagian Pentadbiran MITI apabila warga MITI termasuk pekerja sementara berhenti, bertukar keluar atau bersara;
iii. Pihak ketiga hendaklah mendapatkan Pas Keselamatan Pelawat di Kaunter Pelawat di pintu masuk Bangunan MITI. Pas ini hendaklah dikembalikan semula selepas tamat lawatan;
iv. Pihak ketiga perlu mendapatkan permit kerja daripada Pengurus Bangunan/Bahagian Pentadbiran untuk melaksanakan tugas di MITI; dan
v. Kehilangan pas mestilah dilaporkan dengan segera seperti yang ditetapkan dalam garis panduan yang dikeluarkan oleh Pejabat Ketua Pegawai Keselamatan Malaysia (CGSO).

Peranan: Warga MITI dan Pihak Ketiga

19.1.3 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.

i. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan
ii. 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.

Peranan: Warga MITI dan Pihak Ketiga

19.1.4 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:

i. Pemantauan dan pengawalan keluar masuk pengguna ke Pusat Data melalui sistem *Security Access Door* dan CCTV;
ii. Hanya personel yang mempunyai kebenaran sahaja yang dibenarkan memasuki Pusat Data;
iii. Memastikan Pusat Data sentiasa bersih dan perkakasan ICT bebas daripada habuk;
iv. Penyaman udara mestilah berfungsi dengan baik di mana suhunya adalah bersesuaian dengan Pusat Data; dan
v. Semua peralatan keselamatan, sistem pencegahan dan penggera kebakaran, UPS dan penyaman udara mestilah diselenggarakan secara berkala. ; dan
vi. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan.

Peranan: Pentadbir Pusat Data, Pihak Ketiga

19.2 Keselamatan Peralatan

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

19.2.1 Peralatan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Penggunaan Peralatan: Perkakasan, perisian, dan maklumat di bawah jagaannya hendaklah digunakan untuk urusan rasmi sahaja;
ii. Penggunaan dan Keselamatan Kata Laluan: Penggunaan kata laluan untuk akses sistem komputer adalah wajib, dan kata laluan pentadbir tidak boleh diubah tanpa kebenaran BPM;

iii. Pemantauan Peralatan ICT: Warga MITI bertanggungjawab memastikan semua peralatan ICT berfungsi dengan baik dan tidak dibenarkan menambah atau mengganti perkakasan tanpa kebenaran;

iv. Pemasangan Perisian , Penambahan perisian atau pemasangan perisian tidak berlesen tanpa kebenaran BPM adalah dilarang;

v. Kerosakan dan Kehilangan Peralatan: Warga MITI bertanggungjawab atas kerosakan atau kehilangan peralatan ICT dan perlu melaporkannya dengan segera serta hendaklah diganti dengan aksesori peralatan ICT yang sama atau setara;

vi. Perlindungan Peralatan ICT: Peralatan ICT harus dilindungi daripada kecurian, kerosakan, dan penyalahgunaan, serta disimpan di tempat yang teratur dan bersih dengan ciri keselamatan;

vii. Penyimpanan dan Pengurusan Peralatan: Peralatan ICT yang digunakan secara berterusan perlu diletakkan di kawasan berhawa dingin dan peralatan rangkaian harus diletakkan di rak khas yang berkunci;

viii. Pengurusan Aset: Peralatan ICT yang dipinjam atau hilang perlu mendapat kelulusan dan dilaporkan kepada Pengarah ICT dan ICTSO;

ix. Insiden Keselamatan Siber: Sebarang bentuk insiden, penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO dan boleh diambil tindakan tatatertib;

x. Pengendalian dan Konfigurasi: Warga MITI tidak dibenarkan mengubah lokasi, konfigurasi alamat IP, atau kata laluan pentadbir tanpa kebenaran BPM;

xi. Pendaftaran dan Pelekat Aset: Semua peralatan ICT mesti didaftarkan dalam Sistem Pengurusan Aset (SPA) dengan pelekat aset rasmi; pelekat selain daripada itu tidak dibenarkan;

xii. Daftar *Active Directory*: Semua komputer dan komputer riba yang dibekalkan oleh MITI mesti didaftarkan dengan *Active Directory* (AD);

xiii. Keselamatan Bekalan Kuasa: Pastikan semua peralatan dimatikan apabila meninggalkan pejabat dan plug ditanggalkan untuk mengelakkan kerosakan akibat lonjakan kuasa (*power surge*).

xiv. Fungsi Rangkaian: Fungsi rangkaian tanpa wayar seperti *Wi-Fi, bluetooth*, dan *infrared* perlu dimatikan apabila tidak digunakan di tempat awam.

xv. Keselamatan Penggunaan Pencetak: Warga MITI dilarang menyalahgunakan pencetak yang dibekalkan dan perlu mematuhi garis panduan penggunaan komputer sewaan di MITI.

Peranan: Warga MITI

19.2.2 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 storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
ii. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja;
iii. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;
iv. 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;
v. Permohonan dan pergerakan media storan hendaklah direkodkan;
vi. Perkakasan backup hendaklah diletakkan di tempat yang terkawal;
vii. Membuat salinan atau pendua (*backup*) bagi tujuan keselamatan dan bagi mengelakkan kehilangan data;
viii. Semua data di dalam media storan yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan
ix. Penghapusan maklumat atau kandungan media storan mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan
x. Warga MITI hendaklah bertanggungjawab ke atas sebarang kerosakan atau kehilangan maklumat dalam media storan yang dibekalkan.

Peranan: Pentadbir Sistem ICT, Warga MITI

19.2.3 Tandatangan Digital

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:

i. Warga MITI termasuk pekerja sementara hendaklah bertanggungjawab sepenuhnya ke atas tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;
ii. Tandatangan digital tidak boleh dipindah milik atau dipinjamkan; dan
iii. Sebarang penyalahgunaan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO.

Peranan: Warga MITI

19.2.4 Perisian dan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Hanya perisian yang mempunyai lesen yang sah sahaja dibenarkan bagi kegunaan di MITI;
ii. Sistem aplikasi dalaman tidak dibenarkan dibentang, diagih atau dikongsi kepada pihak lain kecuali dengan kebenaran Pengarah ICT; dan
iii. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan menjadi hak milik MITI. Sebarang pindaan mestilah mengikut prosedur yang ditetapkan.

Peranan: Warga MITI dan Pentadbir Sistem

19.2.5 Penyelenggaraan Perkakasan

Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.

i. Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar atau seperti yang termaktub dalam kontrak;
ii. Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;
iii. Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah tamat tempoh jaminan;
iv. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan;
v. Membuat pendua (*backup*) bagi konfigurasi atau data dalam perkakasan sebelum melaksanakan penyelenggaraan;
vi. Memaklumkan kepada pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan
vii. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengarah ICT/Pengurus BPM yang berkenaan.

Peranan: Semua Pentadbir ICT

19.2.6 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:

i. Peralatan ICT perlu dilindungi dan dikawal sepanjang masa;
ii. Penyimpanan atau penempatan peralatan ICT mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian seperti tempat berkunci dan terlindung;
iii. Peralatan ICT yang hendak dibawa ke luar premis, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan;
iv. Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan; dan
v. Sebarang kerosakan ke atas komputer riba yang berlaku di luar negara, perlu dilaporkan kepada Pengarah ICT dan tidak boleh dibaikpulih di pusat sokongan perkhidmatan pengeluar di luar negara.

Peranan: Warga MITI

19.2.7 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.

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

i. Semua kandungan dalam peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui shredding, grinding, atau pembakaran;
ii. Sekiranya maklumat perlu disimpan, maka pengguna hendaklah membuat salinan pendua;
iii. Data yang terdapat di dalam storan peralatan ICT hendaklah dihapuskan mengikut pekeliling yang berkuatkuasa sebelum peralatan ICT tersebut dilupuskan;
iv. Pegawai Aset ICT hendaklah mengenal pasti sama ada peralatan ICT boleh dilupuskan atau sebaliknya;
v. Peralatan ICT yang hendak dilupuskan perlu disimpan di tempat yang telah dikhaskan bagi menjamin keselamatan peralatan tersebut;
vi. Pegawai Aset ICT bertanggungjawab merekodkan maklumat pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset;
vii. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;
viii. Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut:

a. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk dijadikan hak milik peribadi.
b. Mencabut, menanggal dan menyimpan komponen dalaman CPU seperti SSD, RAM, *hard disk, motherboard* dan sebagainya;
c. Memindah keluar dari premis MITI mana-mana peralatan ICT yang hendak dilupuskan;
d. Melupuskan sendiri peralatan ICT;dan
e. Maklumat lanjut pelupusan hendaklah merujuk kepada Tatacara Pengurusan Aset

Alih Kerajaan (AM 2.7) dan Tatacara Pelupusan Rekod Awam Arkib Negara Malaysia yang terkini.

Peranan: Warga MITI

19.2.8 Peminjaman Peralatan ICT

Semua peralatan ICT termasuklah komputer riba, komputer, tablet, pencetak, projektor, perakam suara, laser pointer dan aksesori yang berkaitan seperti kabel komputer dan sebagainya, adalah hak milik MITI.

Peralatan ICT gunasama yang hendak dibawa keluar dari premis MITI untuk tujuan rasmi, perlulah mendapat kelulusan daripada pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan.

Oleh itu, setiap peralatan yang dipinjam atau dibawa keluar perlulah mengikut prosedur berikut:

i. Pengguna dikehendaki memohon dengan mengisi dan menandatangani borang KEW .PA-9 yang disediakan oleh BPM;
ii. Peralatan yang dipinjam perlulah dikembalikan setelah selesai menggunakannya untuk semakan dan simpanan pihak BPM serta menandatangani borang KEW .PA-9 yang disediakan oleh BPM;
iii. Peminjam adalah bertanggungjawab untuk memastikan semua peralatan dikembalikan dengan sempurna, lengkap dan selamat; dan
iv. Sebarang kerosakan dan kegagalan peralatan berfungsi dengan baik hendaklah dilaporkan kepada Unit Khidmat Sokongan Teknikal BPM dengan segera.

Peranan: Warga MITI

19.2.9 Mekanisma Kawalan Ujicuba Peralatan ICT (*Proof of Concept - POC*)

i. Penerimaan

a. POC mestilah mendapat persetujuan bertulis antara pihak pembekal dan MITI serta sebarang kos adalah ditanggung sepenuhnya oleh pihak pembekal; dan
b. Peralatan yang diterima bebas daripada virus, *backdoor, worm* dan perkara-perkara yang boleh memberi ancaman keselamatan kepada perkhidmatan ICT

MITI.

ii. Penyelenggaraan

a. Capaian melalui rangkaian luar MITI adalah tidak dibenarkan;
b. Sebarang kos adalah ditanggung sepenuhnya oleh pihak pembekal; dan
c. Aktiviti penyelenggaraan adalah di bawah pengawasan pegawai BPM.

iii. Pemulangan

a. Maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (*permanent deletion*); dan
b. Memastikan tiada maklumat MITI yang tertinggal pada peralatan dan perlu disahkan oleh pegawai BPM.

Peranan: BPM dan Pihak ketiga

19.2.10 *Clear Screen* and *Clear Desk*

Clear Desk and 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:

i. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;
ii. Menyimpan bahan-bahan rahsia dan sulit di dalam laci atau kabinet fail yang berkunci; dan
iii. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.

Peranan: Warga MITI

19.3 Keselamatan Persekitaran

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

19.3.1 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:

i. Merancang dan menyediakan pelan keseluruhan susun atur pejabat (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;
ii. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi seperti alat pencegah kebakaran dan pintu kecemasan;
iii. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
iv. Semua bahan cecair dan mudah terbakar dilarang disimpan berhampiran tempat penyimpanan peralatan ICT;
v. Semua peralatan perlindungan keselamatan hendaklah disemak dan diuji sekurang-kurangnya satu (1) kali dalam setahun oleh Jabatan Bomba dan Penyelamat Malaysia. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu;
vi. Akses kepada saluran riser hendaklah sentiasa dikunci;
vii. Melaksanakan latihan keselamatan secara berkala kepada warga MITI;
viii. Melaksanakan pemeriksaan keselamatan persekitaran di setiap aras bangunan oleh Bahagian Pentadbiran dan pihak ketiga; dan
ix. Memastikan penggunaan peralatan elektrik digunakan secara berhemah dan mengikut piawaian keselamatan yang telah ditetapkan.

Peranan: Warga MITI dan Pihak Ketiga

19.3.2 Bekalan Kuasa

Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan kuasa yang sesuai hendaklah disalurkan kepada peralatan ICT;
ii. Peralatan sokongan seperti UPS dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan
iii. Semua peralatan sokongan bekalan kuasa hendaklah diperiksa, diselenggara dan diuji secara berjadual oleh pihak penyelenggara bangunan.

Peranan: BPM dan Pihak Ketiga

19.3.3 Kabel Rangkaian

Port dan Kabel rangkaian komputer hendaklah dilindungi supaya ianya tidak disalahgunakan oleh pengguna yang tidak bertanggungjawab. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:

i. Melindungi port dan kabel daripada kerosakan yang disengajakan atau tidak disengajakan;
ii. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*;
iii. Semua port dan kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat; dan
iv. Port rangkaian yang tidak digunakan hendaklah dinyahaktifkan.

Peranan: BPM dan Pihak Ketiga

19.3.4 Prosedur Kecemasan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Langkah-Langkah Keselamatan sekiranya berlaku kebakaran yang dipaparkan di setiap aras; dan
ii. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada *Floor Safety Manager* (FSM) yang dilantik.

Peranan: Warga MITI

19.4 Keselamatan Dokumen

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

19.4.1 Dokumen

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Setiap dokumen hendaklah di failkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;
ii. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur Arahan Keselamatan;
iii. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan;
iv. Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa berdasarkan Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan Akta Arkib Negara Malaysia;
v. Dokumen terperingkat yang dihantar secara elektronik hendaklah menggunakan kaedah encryption seperti menetapkan kata laluan pada setiap dokumen;
vi. Semua dokumen yang disimpan di dalam peralatan ICT seperti komputer, komputer riba dan tablet perlu dipadamkan sebelum dipulangkan semula kepada BPM; dan
vii. Semua dokumen adalah di bawah tanggungjawab pemilik dokumen.

Peranan: Warga MITI

19.4.2 Penyimpanan Maklumat Di Storan Awan

Setiap dokumen rasmi hanya dibenarkan disimpan di storan awan (*cloud storage*) yang diiktiraf oleh Kerajaan Malaysia seperti yang termaktub dalam surat arahan dan pekeliling yang sedang berkuat kuasa.

Peranan: Warga MITI

20 BIDANG 08 – KESELAMATAN OPERASI

20.1 Pengurusan Prosedur Operasi

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.

20.1.1 Pengendalian Prosedur Tanggungjawab

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal;
ii. 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
iii. Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.

Peranan: Warga MITI

20.1.2 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;
ii. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan dengan aset ICT berkenaan;
iii. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
iv. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

Peranan: Warga MITI

20.1.3 Pengasingan Tugas dan Tanggungjawab

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

Peranan: Pengarah ICT dan ICTSO

20.2 Perancangan dan Penerimaan Sistem

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

20.2.1 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.

Peranan: BPM

20.2.2 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi

Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada

persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan daripada perkakasan yang digunakan dalam pengoperasian sebenar (*production environment*).
ii. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan
iii. Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.

Peranan: Pengarah ICT, Pentadbir Sistem

20.2.3 Penerimaan Sistem

Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.

Peranan: Pentadbir Sistem dan ICTSO

20.3 Perisian Berbahaya

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

20.3.1 Perlindungan dari Perisian Berbahaya

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. 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;
ii. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;
iii. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;

iv. Mengemas kini antivirus dengan pattern antivirus yang terkini;
v. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;
vi. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara pengendalian;
vii. 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;
viii. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan
ix. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus dan malware.

Peranan: Warga MITI

20.3.2 Perlindungan dari *Mobile Code*

Penggunaan mobile code yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.

Peranan: Warga MITI

20.4 Housekeeping

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

20.4.1 *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:

i. Membuat *backup* ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali;
ii. Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat;

iii. 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
iv. Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat.

Peranan: BPM

20.5 Pengurusan Media

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

20.5.1 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 penghantaran dan pemindahan media yang sedang berkuat kuasa.

Peranan: Semua Pengguna

20.5.2 Prosedur Pengendalian Media

Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut:

i. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;
ii. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;
iii. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;
iv. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;
v. Menyimpan semua media di tempat yang selamat;
vi. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat; dan
vii. Pengendalian media hendaklah merujuk kepada KEW PA 2 (Penyerahan Aset).

Peranan: Semua Pengguna

20.5.3 Keselamatan Sistem Dokumentasi

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut:

i. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;
ii. Menyedia dan memantapkan keselamatan sistem dokumentasi; dan
iii. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.

Peranan: Pentadbir Sistem

20.6 Maklumat Umum

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut:

i. Memastikan perisian,data dan maklumat dilindungi dengan mekanisme yang bersesuaian;
ii. Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan
iii. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.

Peranan: Semua Pengguna

20.7 Pemantauan

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

20.7.1 Pengauditan dan Forensik ICT

Ahli CSIRT mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut:

i. Sebarang percubaan pencerobohan kepada sistem ICT MITI;
ii. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery, phishing*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*);
iii. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;
iv. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;
v. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;
vi. Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian;
vii. Aktiviti penyalahgunaan akaun e-mel; dan

viii. Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.

Peranan: MITI CSIRT

20.7.2 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:

i. Rekod setiap aktiviti transaksi;
ii. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;
iii. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan
iv. 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.

Peranan: Pentadbir Sistem

20.7.3 Sistem Log

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:

i. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;

ii. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan
iii. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada MITI CSIRT.

Peranan: Pentadbir Sistem

20.7.4 Pemantauan Log

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;
ii. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau mengikut keperluan;
iii. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;
iv. Aktiviti pentadbiran dan operator sistem perlu direkodkan;
v. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan
vi. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MITI atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.

Peranan: Pentadbir Sistem

20.7.5 Penyeragaman Waktu

Waktu bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut *Malaysian Standard Time*.

Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MITI atau domain keselamatan perlu diseragamkan dengan waktu yang ditetapkan oleh SIRIM.

Peranan: Pentadbir Sistem

20.7.6 Kawalan Pengoperasian Perisian

Pemasangan perisian pada sistem operasi perlu dikawal bagi menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian. Kawalan yang perlu dipatuhi adalah seperti yang berikut:

i. Strategi sandaran (backup) perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian;
ii. Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; dan
iii. Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.

Peranan: Pentadbir Sistem

20.7.7 Pengurusan Kerentanan Teknikal

Sistem maklumat yang digunakan perlu dinilai secara berkala untuk mengenal pasti sebarang kerentanan teknikal yang wujud. Penilaian terhadap kerentanan ini hendaklah dilaksanakan bagi memastikan organisasi sentiasa peka terhadap potensi risiko yang akan wujud dan kawalan yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Perkara yang perlu dipatuhi adalah seperti berikut:

i. Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;
ii. Menganalisis tahap risiko kerentanan; dan
iii. Mengambil tindakan pengukuhan dan kawalan risiko.

Peranan: Pentadbir Sistem

20.7.8 Sekatan ke atas Pemasangan Perisian

Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga MITI; dan
ii. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi berdasarkan pekeliling dan garis panduan yang berkuat kuasa.
iii. Mengimbas semua perisian atau sistem dengan antivirus atau antimalware sebelum menggunakannya.

Peranan: Warga MITI

20.8 Kawalan Keselamatan Siber

Mengawal ancaman siber ke atas infrastruktur ICT, aplikasi dan sistem pengoperasian.

20.8.1 Keselamatan Maklumat bagi Penggunaan Perkhidmatan Awan

Pelaksanaan pengkomputeran awan perlu mematuhi aspek keselamatan kerana menyerahkan ketersediaan keselamatan data aplikasi dan infrastruktur ICT kepada pihak ketiga. MITI perlulah memastikan perkhidmatan ini dilindungi dengan kehendak dasar dan garis panduan pengkomputeran awan yang berkuat kuasa.

Peranan: CDO, Pengarah ICT dan ICTSO

20.8.2 Threat Intelligence

Operasi rangkaian dan infrastruktur ICT MITI dipantau menggunakan perkakasan dan perisian tertentu. Rekod aktiviti dan log dikumpulkan dan dianalisa bagi mengenalpasti ancaman serangan siber bagi membolehkan tindakan mitigasi diambil secara tepat dan berkesan.

Analisa yang dikenalpasti dikategorikan kepada tiga jenis maklumat ancaman iaitu kaedah serangan, metodologi serangan dan perincian maklumat penyerang.

Peranan: Pentadbir Sistem

20.8.3 Pengurusan Konfigurasi

Konfigurasi perkakasan, perisian dan rangkaian perlu dikawal dan tidak diubah sewenang-wenangnya oleh pihak yang tidak mempunyai hak capaian akses.

Setiap konfigurasi yang dilaksanakan perlu direkod dan salinan pendua perlu dibuat sebelum dan selepas aktiviti konfigurasi dilaksanakan. Dokumentasi dan manual pentadbir hendaklah disimpan secara dalam talian atau fizikal. Sekiranya disimpan secara fizikal, dokumen tersebut mestilah disimpan di ruangan yang selamat.

Peranan: Pentadbir Sistem

20.8.4 Aktiviti Pemantauan

Pemantauan ke atas infrastruktur ICT, aplikasi dan sistem pengoperasian perlu dilaksanakan bagi mengelak insiden keselamatan siber.

Peranan: Pentadbir Sistem

20.8.5 Web Filtering

MITI perlu bertanggungjawab melindungi sistem daripada perisian berbahaya dan menghalang akses ke laman web yang tidak dibenarkan. Ini termasuk mengurangkan risiko kakitangan mengakses laman web yang mengandungi maklumat tidak sahih, virus, atau percubaan penipuan seperti phishing untuk mendapatkan maklumat peribadi.

MITI perlu mengesan dan menyekat alamat IP dan domain laman web yang diragui untuk mengawal akses kepada kandungan yang mungkin tidak sesuai atau berpotensi membahayakan pengguna terutamanya dalam persekitaran organisasi kerajaan.

Peranan: Pentadbir Sistem

20.8.6 Pelupusan Maklumat

MITI perlu melaksanakan pelupusan maklumat dengan menggunakan kaedah hapus kekal (*secure permanently erase*) bagi memastikan maklumat yang dilupuskan tidak boleh dicapai oleh mana-mana pihak.

21 BIDANG 09 – KESELAMATAN KOMUNIKASI

Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan serta melindungi integriti maklumat.

21.1 Kawalan Rangkaian

Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:

i. Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi sistem rangkaian;
ii. Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti kecurian, banjir, gegaran dan habuk;
iii. Peranti keselamatan seperti firewall, Web Application Firewall (WAF) dan Intrusion Prevention System (IPS) hendaklah dipasang mengikut kesesuaian keperluan;
iv. Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja;
v. Sebarang kerja pengubahsuaian, atau naik taraf peranti rangkaian perlulah mendapat kelulusan Pengarah ICT dan diselia oleh Pentadbir Rangkaian;
vi. Semua pengguna hanya dibenarkan menggunakan fasiliti rangkaian sedia ada di MITI sahaja dan penggunaan peranti rangkaian luar seperti switch, hub, access point (AP) dan lain-lain perkakasan rangkaian tanpa kelulusan BPM adalah dilarang sama sekali;
vii. Capaian pengguna jarak jauh (remote user) adalah tidak dibenarkan;
viii. Sebarang penggunaan perkhidmatan Internet mestilah menggunakan perkhidmatan rangkaian Internet rasmi yang disediakan MITI. Bagaimanapun, sebarang langganan talian Internet selain yang disediakan MITI akan dipertimbangkan tetapi tertakluk kepada kriteria berikut:
ix. Terdapat keperluan kritikal dengan kelulusan khas pihak pengurusan tertinggi MITI; atauTiada liputan perkhidmatan Internet MITI di kawasan berkenaan; dan

x. MITI mempunyai peruntukan bagi membiayai langganan khidmat Internet tersebut.

xi. Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi Service Level Agreement/ Assurance (SLA) yang telah ditetapkan; dan

xii. Semua perisian berkaitan rangkaian dan keselamatan seperti sniffer, network analyser atau perisian seperti proxy avoidance dan unauthorized VPN software adalah dilarang dipasang pada komputer pengguna atau sistem rangkaian MITI kecuali mendapat kebenaran Pengarah ICT/ ICTSO.

Peranan: ICTSO / Pengurus URKI / Pentadbir Rangkaian

21.1.1 Keselamatan Perkhidmatan Rangkaian

Perkhidmatan rangkaian hendaklah dipastikan sentiasa selamat serta dipantau bagi memastikan kerahsiaan, integriti dan ketersediaan maklumat terjamin.

Mekanisme keselamatan, tahap ketersediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan disediakan secara in-house ataupun outsource.

Peranan:ICTSO / Pentadbir Sistem / Pentadbir Rangkaian / Warga MITI

21.1.2 Pengasingan Rangkaian

Pengasingan perkhidmatan rangkaian bertujuan meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan.

Peranan: Pentadbir Rangkaian

21.2 Pemindahan Maklumat

Memastikan maklumat yang dipindah selamat dan dilindungi.

21.2.1 Polisi dan Prosedur Pemindahan Data dan Maklumat

Prosedur ini bertujuan untuk mengendali, menyimpan, memindah serta melindungi maklumat daripada terdedah tanpa kebenaran atau salah guna serta memastikan keselamatan pemindahan maklumat dengan entiti luar terjamin.

Peranan: ICTSO / Pentadbir Sistem / Warga MITI

21.2.2 Perjanjian Mengenai Pemindahan Data dan Maklumat

MITI perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara MITI dengan pihak ketiga. Perkara yang perlu dipertimbangkan ialah:

i. Penghantaran dan penerimaan maklumat MITI hendaklah dalam keadaan terkawal;
ii. Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat MITI;
iii. Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan
iv. MITI hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan mencegah ketirisan data.

Peranan: Pengarah ICT/ ICTSO

21.2.3 Pengurusan Pesanan Elektronik

Maklumat yang dihantar, diterima dan disimpan melalui mel elektronik MITI perlu dilindungi bagi menghindari capaian atau sebaran maklumat yang tidak dibenarkan. Pengguna layak menerima kemudahan perkhidmatan e-mel dengan sokongan dari Penyelia.

Perkara yang perlu dipatuhi adalah seperti di Garis Panduan Penggunaan E-mel yang sedang berkuat kuasa

Peranan: Warga MITI

21.2.4 Perjanjian Kerahsiaan

Syarat-syarat perjanjian kerahsiaan atau Non-Disclosure Agreements (NDA) perlu mengambil kira keperluan organisasi dan hendaklah disemak, dikemaskini dan didokumentasikan.

Pembekal / agensi luar hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat.

Peranan: Pengarah ICT/ ICTSO/ Pentadbir Sistem ICT

22 BIDANG 10 – PEMEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM

22.1 Keperluan Keselamatan Sistem Maklumat

Memastikan keperluan keselamatan diambil kira dalam setiap fasa kitar hayat pembangunan sistem maklumat.

22.1.1 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat

Pembangunan sistem baharu atau penambahbaikan sistem sedia ada hendaklah mematuhi perkara-perkara berikut:

i. Semua sistem yang dibangunkan sama ada secara dalaman atau khidmat sumber luaran hendaklah dikaji supaya mengikut keperluan pengguna dan selaras dengan dasar atau peraturan semasa yang berkuat kuasa;
ii. Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang ditetapkan; dan
iii. Ujian keselamatan hendaklah dilakukan di setiap peringkat pembangunan sistem bagi memastikan integriti data.

Peranan: Pentadbir Sistem ICT dan Pihak Ketiga

22.1.2 Melindungi Perkhidmatan Aplikasi Dalam Rangkaian Awam

Maklumat aplikasi yang melalui rangkaian awam hendaklah dilindungi daripada aktiviti tidak sah seperti penipuan, pendedahan maklumat, pengubahsuaian maklumat yang tidak dibenarkan dan pertikaian kontrak. Perkara-perkara yang perlu dipatuhi adalah:

i. Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala;
ii. Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala;
iii. Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan MFA (Multi Factor Authentication);

iv. Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi;
v. Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan
vi. Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.

Peranan: Pengarah ICT, Pentadbir Sistem dan Pihak Ketiga

22.1.3 Melindungi Transaksi Perkhidmatan Aplikasi

Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

i. Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi;
ii. Memastikan semua aspek transaksi dipatuhi:

a. Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan;
b. Mengekalkan kerahsiaan maklumat;
c. Mengekalkan privasi pihak yang terlibat;
d. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi; dan.
e. Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh pihak kerajaan.

Peranan: Pengarah ICT, Pentadbir Sistem

22.2 Keselamatan Dalam Proses Pembangunan Dan Sokongan

Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan siber yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.

22.2.1 Polisi Keselamatan Dalam Pembangunan Sistem

Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

i. Keselamatan persekitaran pembangunan;
ii. Keselamatan pangkalan data;
iii. Keperluan keselamatan dalam fasa reka bentuk;
iv. Keperluan check point keselamatan dalam carta perbatuan projek;
v. Keperluan pengetahuan ke atas keselamatan aplikasi;
vi. Keselamatan dalam kawalan versi; dan
vii. Bagi pembangunan melalui khidmat sumber luaran (outsource), pembekal yang dilantik hendaklah berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.

Peranan: Pengarah ICT, ICTSO dan Pentadbir Sistem

22.2.2 Polisi Keselamatan Dalam Pembangunan Sistem

Prosedur kawalan perubahan sistem hendaklah diwujudkan bagi mengawal sebarang perubahan ke atas sistem maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, didokumenkan dan disahkan sebelum diguna pakai;
ii. Setiap aplikasi perlu dikaji semula dan diuji apabila terdapat perubahan/naiktaraf sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. lndividu atau kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pihak ketiga;
iii. Kawalan perlu dibuat terhadap sebarang perubahan ke atas sistem aplikasi atau pakej perisian bagi memastikan ianya terhad mengikut keperluan sahaja; dan
iv. Capaian kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.

Peranan: Pengarah ICT

22.2.3 Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi

Sebarang cadangan perubahan platform hendaklah berasaskan kepada kajian teknikal bagi memastikan pengoperasian sistem tidak terjejas. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Memastikan sistem aplikasi dan integriti data disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilakukan;
ii. Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan
iii. Sebarang perubahan hendaklah selari dengan Pelan Kesinambungan Perkhidmatan MITI.

Peranan: Pentadbir Sistem

22.2.4 Prinsip Kejuruteraan Sistem Yang Selamat

Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggarakan dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat.

Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat.

Semua peringkat pembangunan sistem hendaklah mengambil kira prinsip kejuruteraan sistem berikut:

i. Asas Keselamatan merujuk kepada PKS MITI dan pekeliling semasa yang berkuat kuasa dalam reka bentuk sesuatu sistem.
ii. Berasaskan risiko
iii. Mengurangkan risiko ke tahap boleh terima.
iv. Mudah diguna
v. Mempunyai ciri-ciri open standard untuk portability dan interoperability.
vi. Meningkatkan daya tahan
vii. Memastikan tiada sebarang kelemahan melalui pelaksanaan keselamatan.
viii. Mengurang kelemahan
ix. Meminimumkan kelemahan disebabkan reka bentuk yang kompleks supaya penyenggaraan sistem mudah dilaksanakan.

x. Mengambil kira keperluan rangkaian dalam reka bentuk sistem
xi. Pelaksanaan keselamatan hendaklah mengambil kira capaian sistem daripada dalam dan luar premis.

Peranan: Pentadbir Sistem

22.2.5 Persekitaran Pembangunan Sistem Yang Selamat

Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.

Adalah perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira:

i. Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem;
ii. Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran;
iii. Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem;
iv. Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem;
v. Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan
vi. Kawalan ke atas capaian kepada persekitaran pembangunan sistem.

Peranan: Pentadbir Sistem

22.2.6 Pembangunan Sistem Secara Khidmat Sumber Luaran

Pembangunan perisian secara khidmat sumber luaran (*outsource*) perlu diselia dan dipantau oleh pentadbir/pemilik sistem. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik MITI. Semasa fasa pembangunan sistem oleh pihak ketiga, kod sumber (*source code*) yang dibangunkan perlu diakses dan disemak oleh MITI.

Pembangunan perisian aplikasi secara *outsource* hendaklah mematuhi perkara-perkara berikut:

i. Setiap projek perlu dipantau oleh Pengarah ICT;
ii. Kontrak perbekalan hendaklah memasukkan klausa kod sumber menjadi hak milik MITI;

iii. Kod sumber yang diserahkan kepada MITI mesti bebas daripada sebarang ralat dan kerentanan;
iv. Mengutamakan kepakaran teknologi tempatan;
v. Pembangunan aplikasi hendaklah dijalankan dalam persekitaran MITI mengikut situasi;
vi. Penggunaan data masking/ dummy data semasa pembangunan dan pengujian;
vii. Data ujian hendaklah dilupuskan secara kekal (secured delete) selepas projek disiapkan/ tamat kontrak; dan
viii. Aktiviti sandaran penuh (full backup) ke atas keseluruhan sistem hendaklah berjaya dilakukan sebelum projek tamat.

Peranan: Pengarah ICT dan Pentadbir Sistem

22.2.7 Ujian Keselamatan Sistem

Ujian keselamatan sistem hendaklah dijalankan ke atas tiga (3) peringkat pemprosesan maklumat iaitu peringkat kemasukan data (*input*), peringkat pemprosesan data (*process*), dan peringkat penjanaan laporan (*output*). Perkara–perkara yang perlu dipatuhi oleh pentadbir sistem adalah:

i. Merancang dan melaksanakan penilaian risiko mengikut keperluan bagi mengenal pasti dan melaksana kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam aplikasi;
ii. Merancang dan melaksana ujian keselamatan yang bersesuaian mengikut fasa di dalam kitar hayat pembangunan sistem (Software Development Life Cycle atau SDLC) bagi mengenal pasti kelemahan sistem; dan
iii. Membuat semakan pengesahan sistem aplikasi untuk mengenal pasti sebarang pencemaran maklumat sama ada disebabkan oleh kesilapan atau disengajakan.

Peranan: Pentadbir Sistem

22.2.8 Pengujian Penerimaan Sistem

Program Pengujian Penerimaan Sistem (Ujian Penerimaan Pengguna dan Ujian Penerimaan Akhir) hendaklah dilaksana berdasarkan kriteria yang telah ditetapkan sebelum sistem diguna pakai.

Amalan pengujian mestilah menurut standard semasa serta menepati amalan terbaik dalam industri.

Peranan: Pentadbir Sistem ICT, Warga MITI dan Pihak Ketiga

22.3 Keselamatan Sistem Fail

Memastikan supaya sistem fail dikawal dan dikendali dengan baik dan selamat.

22.3.1 Kawalan Sistem Fail

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Proses pengemaskinian sistem fail hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;
ii. Kod sumber yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji;
iii. Mengawal capaian ke atas kod sumber bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;
iv. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan
v. Mengaktifkan log audit bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.

Peranan: Pemilik Sistem dan Pentadbir Sistem

22.4 Kawalan Teknikal Keterdedahan

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

22.4.1 Kawalan dari Ancaman Teknikal

Kawalan teknikal dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut:

i. Memperoleh maklumat teknikal yang digunakan;
ii. Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan
iii. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.

Peranan: Pentadbir Sistem

22.5 Pembangunan Aplikasi Mudah Alih

Menerangkan perkara yang mesti dipatuhi dalam membangunkan aplikasi mudah alih bagi menjamin keselamatan aplikasi dan data.

Peranan: Pentadbir Sistem

22.5.1 Prosedur Integrasi Pembangunan Aplikasi Mudah Alih

Pembangunan aplikasi mudah alih yang melibatkan integrasi dengan sistem induk mesti menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang mengurangkan risiko ancaman keselamatan.

Peranan: Pentadbir Sistem, Pembangun Sistem

22.6 Data Ujian

22.6.1 Perlindungan Data Ujian

Data ujian hendaklah disediakan dengan secukupnya sebelum ujian dilaksanakan. Kaedah menjana data ujian adalah seperti berikut:

i. Menyediakan secara manual;
ii. Salin data daripada persekitaran produksi (production) kepada persekitaran pengujian;
iii. Salin data ujian daripada sistem aplikasi terdahulu (legacy);
iv. Menyediakan secara automatik seperti web service atau sebarang tools yang menjana data; atau
v. Back-end Data Injection.
vi. Perkara–perkara yang perlu dipatuhi adalah:
vii. Sebarang prosedur kawalan persekitaran produksi (production environment) hendaklah juga dilaksanakan dalam persekitaran pengujian;
viii. Pengguna ICT yang mempunyai hak capaian persekitaran produksi (production) sebenar sahaja dibenarkan untuk menyalin data dari persekitaran produksi ke persekitaran pengujian;
ix. Data yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan

x. Mengaktifkan log audit bagi merekodkan semua aktiviti pengujian dan pengemaskinian untuk tujuan statistik, pemulihan, keselamatan dan pengesahan data.

Peranan: Pentadbir Sistem, Warga MITI dan Pihak Ketiga

23 BIDANG 11 – HUBUNGAN DENGAN PEMBEKAL

Memastikan keselamatan aset ICT MITI yang diberi kebenaran capaian dilindungi dari ancaman keselamatan.

23.1 Keselamatan Maklumat Dalam Hubungan Pembekal

Memastikan aset ICT MITI yang boleh diakses pembekal dilindungi.

23.1.1 Polisi Keselamatan Maklumat Untuk Hubungan Pembekal

Semua syarikat pembekal adalah tertakluk kepada Dasar Keselamatan Kerajaan yang berkuat kuasa. Perkara–perkara yang perlu dipatuhi adalah seperti berikut:

i. Membaca, memahami dan mematuhi PKS MITI;
ii. Perlu menandatangani Non-Disclosure Agreement (NDA) MITI yang sedang berkuat kuasa dan Surat Akuan Pematuhan Polisi Keselamatan Siber MITI seperti di Lampiran 1;
iii. Syarikat pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas; dan
iv. Akses syarikat pembekal ke atas aset ICT MITI hendaklah sentiasa dikawal dan dipantau.

Peranan: Pemilik Projek, Pihak Ketiga

23.1.2 Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pembekal

Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi.

Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap

masa dalam memberikan perkhidmatan kepada pihak MITI selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.

Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i. MITI hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan;
ii. Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan;
iii. Semua wakil syarikat pembekal hendaklah melepasi tapisan keselamatan daripada CGSO;
iv. Semua wakil syarikat pembekal hendaklah menandatangani Perakuan Akta Rahsia Rasmi 1972 seperti di Lampiran E dan F, Arahan Keselamatan (Semakan dan Pindaan 2017);
v. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi;
vi. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan MITI; dan
vii. Syarikat pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh MITI.

Peranan: Pihak Ketiga

23.1.3 Rantaian Bekalan Produk ICT

Perjanjian dengan syarikat pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira adalah seperti berikut:

i. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan;

ii. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal lain yang memberikan perkhidmatan atau pembekalan produk;
iii. Memastikan jaminan daripada syarikat pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik serta memenuhi obligasi kontrak; dan
iv. Pembekal utama hendaklah memastikan produk atau perkhidmatan yang diberikan adalah selamat daripada unsur-unsur yang boleh mengganggu kelancaran perkhidmatan ICT di MITI.

Peranan: Pihak Ketiga dan Pemilik Projek

23.2 Pengurusan Penyampaian Perkhidmatan Pembekal

Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.

23.2.1 Pemantauan dan Kajian Perkhidmatan Pembekal

Prestasi perkhidmatan pembekal hendaklah sentiasa dipantau, diaudit dan dikaji semula secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti berikut:

i. Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan;
ii. Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan
iii. Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.

Peranan: Pemilik projek, Pihak Ketiga

23.2.2 Pengurusan Perubahan Perkhidmatan Pembekal

Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan dengan mengambil kira kepentingan

maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti berikut:

i. Perubahan dalam perjanjian dengan pembekal;
ii. Perubahan yang dilakukan oleh MITI bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan
iii. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.

Peranan: Pemilik Projek dan Pihak Ketiga

24 BIDANG 12 – PENGURUSAN INSIDEN KESELAMATAN ICT

Untuk memastikan semua insiden dikendalikan dengan konsisten, cepat, tepat dan berkesan termasuk saluran komunikasi keselamatan dan *security events* bagi memastikan sistem ICT MITI dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej MITI dan sistem penyampaian perkhidmatan.

24.1 Mekanisma Pelaporan Insiden Keselamatan Siber

i. Pelaporan kepada NC4 (*National Cyber Coordination and Command Centre*)
Semua insiden keselamatan siber yang berlaku mesti dilaporkan segera kepada NC4 (*National Cyber Coordination and Command Centre*). Dengan prosedur pelaporan yang teratur, NC4 dapat memastikan tindakan balas pantas , melindungi data penting dan memperkukuhkan keselamatan negara secara keseluruhan.

ii. NCII (*National Critical Information Infrastructure*)
Merupakan inisiatif penting kerajaan untuk melindungi infrastruktur maklumat kritikal negara . Infrastruktur ini melibatkan sistem dan aset yang amat penting kepada kelangsungan ekonomi, keselamatan negara, kesihatan awam, kestabilan sosial dan memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

iii. Pelaporan kepada CSIRT MITI.
Pentadbir sistem dan pengguna yang terlibat mesti melaporkan sebarang insiden yang melibatkan keselamatan siber kepada CSIRT MITI.

iv. Tindakan Dalam Keadaan Berisiko Tinggi

Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak.

Peranan: Warga MITI, CSIRT MITI, ICTSO

24.2 Prosedur Pengurusan dan Pengendalian Insiden Keselamatan Siber

Pengurusan pengendalian insiden keselamatan siber dilaksanakan oleh Pasukan CSIRT MITI yang diketuai oleh ICTSO. Pengendalian ini dilaksana berpandukan prosedur pengurusan pelaporan dan pengendalian insiden keselamatan siber berkuat kuasa.

Pengendalian insiden keselamatan siber perlu diuruskan dengan cepat, teratur dan berkesan, mengikut prosedur yang ditetapkan. Pasukan CSIRT MITI perlu membaca dan memahami dokumen Terma Rujukan Cyber Security Incident Response Team (CSIRT) MITI.

Peranan: CSIRT MITI, ICTSO

25 BIDANG 13 – PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Menjamin operasi perkhidmatan agar tidak tergendala dan meminimumkan gangguan penyampaian perkhidmatan yang berterusan kepada pelanggan MITI.

25.1 Perancangan Pengurusan Kesinambungan Perkhidmatan

Pengurusan Kesinambungan Perkhidmatan (PKP) ialah mekanisma bagi mengurus dan memastikan kepentingan pemegang taruh sistem penyampaian perkhidmatan dilindungi dan imej MITI terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan MITI di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan. Pelan PKP perlu dibangunkan dan mengandungi perkara-perkara berikut:

i. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
ii. Senarai pengguna berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan pegawai yang tidak dapat hadir untuk menangani insiden;

iii. Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;
iv. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan
v. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan.

CDO adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT MITI.

Salinan pelan PKP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama.

Peranan: CDO, Pengarah ICT, ICTSO dan BPM

25.2 Pelaksanaan Kesinambungan Keselamatan Maklumat (Implementing Information Security Continuity)

Pelan PKP hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

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

MITI hendaklah memastikan salinan pelan PKP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

Peranan: CDO, Pengarah ICT, ICTSO dan BPM

25.3 Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat

MITI hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.

Peranan: CDO, Pengarah ICT, ICTSO dan BPM

25.4 Pelan Pemulihan Bencana

Pelan Pemulihan Bencana (DRP) merujuk kepada dokumen pelan yang menetapkan sumber, tindakan, tanggungjawab dan data yang diperlukan untuk mengurus proses pemulihan selepas berlaku gangguan terhadap perkhidmatan kritikal MITI. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh pengurusan MITI.

Peranan: CDO, Pengarah ICT, ICTSO dan BPM

25.5 Lewahan (*Redundancy*)

Semua sistem aplikasi dan peralatan yang kritikal hendaklah mempunyai kemudahan lewahan dan diuji (*failover test*) keberkesanannya mengikut keperluan dan kesesuaian semasa.

Peranan: Pentadbir Sistem

26 BIDANG 14 – PEMATUHAN

26.1 Pematuhan dan Keperluan Perundangan

Meningkat dan memantapkan tahap keselamatan siber bagi mengelak daripada pelanggaran mana-mana undang-undang, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat serta pematuhan kepada audit.

26.1.1 Pematuhan Dasar, Piawaian dan Keperluan Teknikal

Warga MITI hendaklah membaca, memahami dan mematuhi PKS MITI dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Sebarang pelanggaran terhadap PKS 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 daripada tujuan rasmi.

Sebarang penggunaan aset ICT MITI selain daripada maksud dan tujuan adalah merupakan satu penyalahgunaan sumber MITI.

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.

Peranan: ICTSO dan Pengguna ICT

26.1.2 Pelanggaran Dasar, Piawaian dan Keperluan Teknikal

Pelanggaran Pelan Keselamatan Siber MITI boleh dikenakan tindakan tatatertib.

Peranan: Pengguna ICT

26.1.3 Keperluan Perundangan

Senarai perundangan dan peraturan yang perlu dipatuhi oleh Warga MITI adalah seperti di Lampiran 2.

Peranan: Pengguna ICT

26.1.4 Pelanggaran Perundangan

Pelanggaran dasar ini boleh diambil tindakan undang-undang dan tatatertib di bawah Akta Rahsia Rasmi 1972 dan Perintah-Perintah Am Bab D - Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993.

Peranan: Pengguna ICT

26.1.5 Hak Harta Intelek

Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual.

Melaksanakan kawalan terhadap keperluan pelesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.

Peranan: Pengguna ICT

26.1.6 Perlindungan Rekod

Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.

Peranan: Pengguna ICT

26.1.7 Privasi dan Perlindungan Maklumat Peribadi

MITI hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.

Peranan: Pengguna ICT

26.1.8 Peraturan Kawalan Kriptografi

Kawalan kriptografi hendaklah dilaksanakan berdasarkan kepada dasar dan garis panduan yang berkuat kuasa.

Peranan: Pengguna ICT

26.1.9 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.

Peranan: Pentadbir Sistem

26.1.10 Pelaksanaan Audit Dalam dan Audit Luar

i. 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 PKS MITI.

ii. Audit Luar

Semakan audit luar adalah perlu bagi memastikan pematuhan kepada peraturan dan polisi yang sedang berkuat kuasa dan hasil semakan semula audit dalam.

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 bertauliah.

Peranan: Pentadbir Sistem

LAMPIRAN 1: SURAT PEMATUHAN POLISI KESELAMATAN SIBER MITI

SURAT AKUAN PEMATUHAN

POLISI KESELAMATAN SIBER (PKS)

KEMENTERIAN PELABURAN, PERDAGANGAN DAN INDUSTRI (MITI)

Nama : .....

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 Polisi Keselamatan Siber (PKS) 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: ……..

LAMPIRAN 2: RUJUKAN

Polisi Keselamatan Siber MITI ini hendaklah dibaca bersama dengan akta, warta kerajaan, pekeliling, surat pekeliling dan peraturan-peraturan berkaitan dan sedang berkuat kuasa seperti berikut:

Senarai Perundangan dan Peraturan Keselamatan ICT Malaysia

Bil	Dokumen	Tahun	Penerbit
1	Arahan Keselamatan	—	—
2	Pekeliling Am Bil. 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan	2000	Jabatan Perdana Menteri (JPM)
3	Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)	2002	MAMPU (Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia)
4	Pekeliling Am Bil. 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)	2001	JPM
5	Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agenis Kerajaan	2003	JPM
6	Surat Pekeliling Am Bil. 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam	2005	JPM
7	Surat Pekeliling Am Bil. 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam	2006	JPM
8	Surat Arahan Ketua Setiausaha Negara – Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa	2006	JPM

	Wayar (Wireless Local Area Network) di Agensi-Agenis Kerajaan		
9	Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agenis Kerajaan	2007	MAMPU
10	Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-Agenis Kerajaan	2007	MAMPU
11	Surat Pekeliling Am Bil. 2 Tahun 2000 – Peranan Jawatankuasa-Jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK)	2000	JPM
12	Pekeliling Perbendaharaan (1PP)	—	Kementerian Kewangan Malaysia (MOF)
13	Akta Tandatangan Digital 1997 (Akta 562)	1997	Parlimen Malaysia
14	Akta Rahsia Rasmi 1972 (Akta 88)	1972	Parlimen Malaysia
15	Akta Jenayah Komputer 1997 (Akta 563)	1997	Parlimen Malaysia
16	Akta Hak Cipta (Pindaan) Tahun 1997	1997	Parlimen Malaysia
17	Akta Komunikasi dan Multimedia 1998 (Akta 588)	1998	Parlimen Malaysia
18	Perintah-Perintah Am	—	JPM
19	Arahan Perbendaharaan	—	MOF
20	Arahan Teknologi Maklumat 2007	2007	JPM
21	Garis Panduan Keselamatan MAMPU 2004	2004	MAMPU
22	Surat Pekeliling Am Bil. 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam	2009	MAMPU
23	Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam	2010	MAMPU

24	Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) V1.0	2016	MAMPU
25	Surat Arahan Ketua Pengarah MAMPU – Penggunaan Media Jaringan Sosial di Sektor Awam	2009	MAMPU
26	Dasar Pengurusan Rekod dan Arkib Elektronik 2003	2003	Arkib Negara Malaysia
27	Surat Pekeliling Am Bil. 3 Tahun 2015 – Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Agensi Sektor Awam	2015	MAMPU
28	Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) oleh Agensi Keselamatan Siber Negara (NACSA)	2019	MAMPU
29	Garis Panduan Pengurusan Pusat Data MAMPU	—	MAMPU
30	Dasar Perkhidmatan Pengkomputeran	—	MAMPU
31	Garis Panduan Pengurusan Keselamatan Maklumat melalui Pengkomputeran Awan (Cloud Computing) dalam Perkhidmatan Awam	—	MAMPU
32	Pekeliling Kemajuan Pentadbiran Awam Bil. 2 Tahun 2021 – Dasar Perkongsian Data Sektor Awam	2021	JPM
33	Polisi Keselamatan Siber MAMPU	—	MAMPU