DASAR KESELAMATAN ICT

JABATAN METEOROLOGI MALAYSIA

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI

VERSI 3.4

SEJARAH DOKUMEN

Tarikh Kelulusan	Versi	Kelulusan	Tarikh Kuatkuasa
24 Mac 2004	1.0	Ketua Pengarah	24 Mac 2004
29 Jun 2009	2.0	JPICT JMM Bil 2/2009	1 Julai 2009
7 Oktober 2011	2.1	JPICT JMM Bil 3/2011	1 Januari 2012
7 Februari 2014	3.0	JPICT JMM Bil. 1/2014	1 April 2014
14 Ogos 2014	3.1	JPISMS JMM Bil. 2/2014	20 Ogos 2014
20 Jun 2016	3.2	JPISMS JMM Bil. 1/2016	13 Julai 2016
5 April 2017	3.3	JPICT JMM Bil. 2/2017	2 Mei 2017
25 Mei 2018	3.4	JPICT JMM Bil. 3/2018	1 Jun 2018

JADUAL PINDAAN DASAR KESELAMATAN ICT METMALAYSIA

Tarikh Kuatkuasa	Versi	Butiran Pindaan
1 Januari 2012	2.1	i. **Tajuk baru : Penyataan Dasar**, muka surat 1 dan 2 ii. **Perkara 1.4 Skop : Pindaan pada para 1.3 Skop versi 2.0 kepada para 1.4 Skop** muka surat 3 dan 4 iii. **Perkara 1.5 Prinsip : Penambahan secara lebih lengkap bagi prinsip-prinsip DKICT**, muka surat 5, 6, 7 dan 8 iv. **Tajuk Baru : Penilaian Risiko Keselamatan ICT,** muka surat 9 v. **Tajuk Baru : Perkara 3.7 Jawatankuasa Pemandu ICT JMM (JPICT)**, muka surat 16 vi. **Perkara 3.8 Keperluan Keselamatan Kontrak dengan Pihak Ketiga : Penambahan para (a) hingga (e)**, muka surat 17 vii. **Perkara 4.1 Inventori Aset : Penambahan para (a) hingga (e)**, muka surat 18 viii. **Pertukaran Tajuk : Perkara 5.1 Sebelum Perkhidmatan**, muka surat 20 ix. **Perkara 5.2 Semasa dalam Perkhidmatan : Penambahan para (a) hingga (d),** muka surat 20 dan 21 x. **Tajuk Baru : PENGURUSAN MAKLUMAT INSIDEN KESELAMATAN ICT**, muka surat 23

Tarikh Kuatkuasa	Versi	Butiran Pindaan
		xi. **Tajuk Baru : Perkara 5.7 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT**, muka surat 23 xii. **Perkara 6.1 Perimeter Keselamatan Fizikal : Penambahan para (h) hingga (l)**, muka surat 25 dan 26 xiii. **Perkara 6.4 Peralatan ICT : Penambahan para (b), (c), (d), (f), (g), (h), (i), (k), (l), (m), (n), (o), (p), (q), (r), (s), (t), (u) dan (w)**, muka surat 27, 28 dan 29 xiv. **Perkara 6.5 Media Storan : Penambahan para (a) hingga (f)**, muka surat 29 dan 30 xv. **Perkara 6.9 Pelupusan Aset ICT : Penambahan para (c) hingga (v)**, muka surat 32 dan 33 xvi. **Tajuk baru : Perkara 7.3 Pengasingan Tugas dan Tanggungjawab,** muka surat 37 xvii. **Tajuk baru : PENGURUSAN PENYAMPAIAN PIHAK KETIGA,** muka surat 38 xviii. **Tajuk baru : Perkara 7.5 Perkhidmatan Penyampaian,** muka surat 38 xix. **Tajuk baru : PENGURUSAN PERTUKARAN MAKLUMAT** muka surat 43 xx. **Tajuk baru : Perkara 7.14 Pertukaran Maklumat**

Tarikh Kuatkuasa	Versi	Butiran Pindaan
		muka surat 43 xxi. **Tajuk baru : PERKHIDMATAN E-DAGANG (ELECTRONIC COMMERCE SERVICES)**, muka surat 46 xxii. **Tajuk baru : Perkara 7.17 E-Dagang,** muka surat 46 xxiii. **Tajuk baru : Perkara 7.18 Maklumat Umum,** muka surat 47 xxiv. **Tajuk baru : PEMANTAUAN**, muka surat 47 xxv. **Tajuk baru : Perkara 7.19 Pengauditan dan Forensik ICT,** muka surat 47 dan 48 xxvi. **Tajuk baru : Perkara 7.22 Pemantauan Log**, muka surat 49 dan 50 xxvii. **Tajuk baru : Perkara 8.3 Hak Capaian**, muka surat 52 xxviii. **Tajuk baru : Perkara 8.4 Pengurusan Katalaluan,** muka surat 52 dan 53 xxix. **Tajuk baru : KAWALAN CAPAIAN RANGKAIAN**, muka surat 55 xxx. **Tajuk baru : Perkara 8.8 Rangkaian,** muka surat 55 xxxi. **Tajuk baru : KAWALAN CAPAIAN SISTEM PENGOPERASIAN**, muka surat 55 xxxii. **Tajuk baru : Perkara 8.9 Capaian Sistem Pengoperasian,** muka surat 55 dan 56

Tarikh Kuatkuasa	Versi	Butiran Pindaan
		xxxiii. **Tajuk baru : Perkara 9.2 Pengesahan Data Input dan Output,** muka surat 57 xxxiv. **Tajuk baru : Perkara 9.4 Pengurusan Infrastruktur Kunci Awam (PKI),** muka surat 58 xxxv. **Tajuk baru: Perkara 9.7 Pembangunan Perisian Secara *Outsource***, muka surat 59 xxxvi. **Tajuk baru : KAWALAN TEKNIKAL KETERDEDAHAN (VULNERABILITY)**, muka surat 59 xxxvii. **Tajuk baru : Perkara 9.8 Kawalan dari Ancaman Teknikal**, muka surat 60 xxxviii. **Tajuk baru : Perkara 11.2 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal,** muka surat 62 xxxix. **Tajuk baru : Perkara 11.3 Pematuhan kepada Audit,** muka surat 62 xl. **Tajuk baru : Perkara 11.5 Pelanggaran Dasar,** muka surat 66

Tarikh Kuatkuasa	Versi	Butiran Pindaan	Mukasurat
1 April 2014	3.0	JPICT JMM Bil. 1/2014	Semua
20 Ogos 2014	3.1	K05/04 : Pindaan pada para c, d, e, f	49
13 Julai 2016	3.2	Pemansuhan ‘Seksyen’ dalam Bahagian Komunikasi Meteorologi dan ditukar kepada ‘Operasi’	14, 25, 26, 27, 28, 29
		Pindaan pada Nama Bahagian selepas penstrukturan dalaman Jabatan	24, 27
2 Mei 2017	3.3	Pengemaskinian semasa Bengkel Pemurnian Dokumen ISMS dan kelulusan JPICT	4, 5, 6, 14, 16, 17, 18, 19, 20, 25, 33
1 Jun 2018	3.4	Penambahbaikan semasa Bengkel Pemurnian Dokumen ISMS 2018 dan kelulusan JPICT	2, 17,19, 58, 59, 63 & 65

ISI KANDUNGAN

BIL	PERKARA	M/S
1.	**PENGENALAN**	1
2.	**OBJEKTIF**	1
3.	**PERNYATAAN DASAR**	2
4.	**SKOP**	3
5.	**PRINSIP-PRINSIP**	5
6.	**PENILAIAN RISIKO KESELAMATAN ICT**	7
7.	**KAWALAN-KAWALAN**	
	KAWALAN 01 : DASAR KESELAMATAN ICT	8
	Objektif **K01/01 Pelaksanaan Dasar** **K01/02 Penyebaran Dasar** **K01/03 Penyelenggaraan Dasar** **K01/04 Pematuhan Dasar**	 8 8 8 8
	KAWALAN 02 : KESELAMATAN ORGANISASI	9
	Objektif **K02/01 Infrastruktur Organisasi Dalaman** K02/01/01 Ketua Pengarah (KP) K02/01/02 Ketua Pegawai Maklumat (CIO) K02/01/03 Pengurus ICT K02/01/04 Pegawai Keselamatan ICT (ICTSO) K02/01/05 Ketua Pejabat K02/01/06 a) Pentadbir Sistem b) Pentadbir Rangkaian c) Pentadbir Pangkalan Data Dan Keselamatan d) Pentadbir Laman Web e) Pentadbir Pusat Data f) Pentadbir Bilik Server DRC g) Pentadbir Sistem Aplikasi h) Pentadbir Emel K02/01/07 Pengguna K02/01/08 Jawatankuasa Pemandu ICT (JPICT) K02/01/09 Jawatankuasa Pemandu Pensijilan MS ISO/IEC	 9 9 9 9 10 11 12 12 12 13 13 14 14 15 16 16 18

BIL	PERKARA	M/S
	27001 Pengurusan Sistem Keselamatan Maklumat (JPISMS) K02/01/10 Pasukan Tindak Balas Insiden Keselamatan ICT (CERT MetMalaysia) K02/01/11 Pasukan Pemulihan Bencana (DRT) MetMalaysia **K02/02 Pihak Ketiga** K02/02/01 Keperluan Keselamatan Dalam Kontrak ICT	 **19** **20** **21**
	KAWALAN 03 : PENGURUSAN ASET	**24**
	Objektif **K03/01 Akauntabiliti Aset** **K03/02 Pengelasan Maklumat** **K03/03 Pengendalian Maklumat**	 **23** **23** **23**
	KAWALAN 04 : KESELAMATAN SUMBER MANUSIA	**25**
	Objektif **K04/01 Sebelum Perkhidmatan** **K04/02 Semasa Perkhidmatan** K04/02/01 Program Kesedaran Keselamatan ICT **K04/03 Bertukar Atau Tamat Perkhidmatan**	 **25** **25** **26** **26**
	KAWALAN 05 : KESELAMATAN FIZIKAL DAN PERSEKITARAN	**27**
	Objektif **K05/01 Keselamatan Kawasan** K05/01/01 Kawalan Kawasan K05/01/02 Kawalan Masuk Fizikal K05/01/03 Kawasan Larangan K05/01/04 Kawalan Kawasan Larangan **K05/02 Keselamatan Peralatan** K05/02/01 Peralatan ICT K05/02/02 Media Storan K05/02/03 Media Tandatangan Digital K05/02/04 Media Perisian dan Aplikasi K05/02/05 Perkakasan Tanpa Penyeliaan (Unattended Equipment) K05/02/06 Peralatan di Luar Premis K05/02/07 Pelupusan K05/02/08 Penyelenggaraan	 **27** **27** **28** **28** **28** **29** **29** **30** **31** **31** **32** **32** **32** **33**

BIL	PERKARA	M/S
	K05/03 Kawalan Persekitaran	**33**
	K05/03/01 Kawalan Persekitaran	**33**
	K05/03/02 Kabel Rangkaian	**34**
	K05/03/03 Bekalan Kuasa	**34**
	K05/03/04 Prosedur Kecemasan	**34**
	K05/04 Keselamatan Sistem Dokumentasi	**35**
	KAWALAN 06 : PENGURUSAN OPERASI DAN KOMUNIKASI	**36**
	Objektif	
	K06/01 Prosedur Operasi	**36**
	K06/01/01 Pengendalian Dokumen Prosedur Operasi	**36**
	K06/01/02 Pengurusan Perubahan	**36**
	K06/01/03 Pengasingan Tugas dan Tanggungjawab	**36**
	K06/01/04 Prosedur Pengurusan Insiden	**37**
	K06/02 Perancangan, Pemasangan dan Penerimaan Sistem	**37**
	K06/02/01 Perancangan Kapasiti	**37**
	K06/02/02 Pemasangan Sistem	**38**
	K06/02/03 Penerimaan Sistem	**38**
	K06/03 Perisian Berbahaya	**38**
	K06/03/01 Perlindungan dari Perisian Berbahaya	**38**
	K06/03/02 Perlindungan dari *Mobile Code*	**39**
	K06/04 Housekeeping	**39**
	K06/04/01 Backup	**39**
	K06/05 Pengurusan Rangkaian	**39**
	K06/06 Pengurusan Media	**40**
	K06/06/01 Media Mudah Alih	**40**
	K06/06/02 Prosedur Pengendalian Media	**40**
	K06/07 Pengurusan Pertukaran Maklumat	**41**
	K06/08 Mel Elektronik (Emel)	**41**
	K06/09 Perkhidmatan e-Dagang (e-Commerce)	**42**
	K06/10 Paparan Maklumat Umum	**43**
	K06/11 Pengurusan Perkhidmatan Pihak Ketiga	**43**
	K06/12 Pemantauan	**43**
	K06/12/01 Pemantauan Log	**43**
	K06/12/02 Pengauditan dan Forensik ICT	**44**
	K06/12/03 Jejak Audit	**45**
	K06/12/04 Log Sistem	**45**

BIL	PERKARA	M/S
	KAWALAN 07 : KAWALAN AKSES	**46**
	Objektif	
	K07/01 Kawalan Akses	**46**
	K07/02 Pengurusan Akses Pengguna	**46**
	K07/02/01 Pendaftaran Pengguna	**46**
	K07/02/02 Hak Akses (Access Privilege)	**47**
	K07/02/03 Pengurusan Kata Laluan	**47**
	K07/02/04 *Clear Desk* dan *Clear Screen*	**48**
	K07/03 Akses Sistem Pengoperasian	**48**
	K07/03/01 Akses Sistem Pengoperasian	**48**
	K07/03/02 Kad Pintar	**49**
	K07/04 Akses Aplikasi dan Maklumat	**50**
	K07/05 Akses Jarak Jauh	**50**
	K07/05/01 Kerja Jarak Jauh (Teleworking)	**51**
	K07/05/02 *Cloud Networking*	**51**
	K07/06 Kawalan Akses Rangkaian	**51**
	K07/06/01 Akses Rangkaian	**51**
	K07/06/02 Akses Internet	**51**
	K07/07 Peralatan Mudah Alih	**52**
	KAWALAN 08 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	**53**
	Objektif	
	K08/01 Kawalan Prosesan Aplikasi	**53**
	K08/01/01 Pengesahan Data *Input*	**53**
	K08/01/02 Kawalan Proses	**53**
	K08/01/03 Pengesahan Data *Output*	**53**
	K08/02 Kawalan Kriptografi	**54**
	K08/03 Keselamatan Sistem Fail	**54**
	K08/04 Keselamatan Proses Pembangunan Dan Sokongan	**55**
	K08/04/01 Prosedur Perubahan	**55**
	K08/04/02 Pembangunan Secara *Outsource*	**55**
	K08/04/03 Pembocoran Maklumat	**55**
	K08/05 Kawalan Terhadap *Vulnerability*	**55**
	KAWALAN 09 : PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN	**56**

BIL	PERKARA	M/S
	Objektif K09/01 Mekanisme Pelaporan Insiden Keselamatan ICT K09/02 Prosedur Pengendalian Insiden Keselamatan ICT	 56 57
	KAWALAN 10 : PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	58
	Objektif K10/01 Pengurusan Kesinambungan Perkhidmatan (PKP) K10/02 Pelan Kesinambungan Perkhidmatan	 58 59
	KAWALAN 11 : PEMATUHAN	60
	Objektif K11/01 Pematuhan Dasar K11/02 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal K11/03 Pematuhan Kepada Keperluan Audit K11/04 Keperluan Perundangan K11/05 Pelanggaran Perundangan	 60 60 60 61 62
8.	GLOSARI	63
9.	SENARAI LAMPIRAN	67
10.	Garis Panduan Dan Etika Penggunaan Emel dan Internet MetMalaysia	
11.	Surat Akuan Pematuhan Dasar Keselamatan ICT MetMalaysia.	

PENGENALAN

Jabatan Meteorologi Malaysia (MetMalaysia) berperanan untuk membekalkan pelbagai perkhidmatan meteorologi, iklim dan geofizik yang tepat dan berkesan berteraskan profesionalisme, inovatif dan integriti. Dokumen Dasar Keselamatan ICT (DKICT) ini mengandungi peraturan-peraturan yang perlu difahami, dipatuhi dan diguna pakai oleh semua pengguna yang menyediakan perkhidmatan, mencapai dan menggunakan aset dan aplikasi Teknologi Maklumat dan Komunikasi (ICT) di MetMalaysia.

OBJEKTIF

Objektif DKICT MetMalaysia adalah seperti berikut :

1. memastikan kelancaran operasi jabatan yang berasaskan ICT dengan mencegah serta meminimumkan kerosakan atau kemusnahan aset ICT jabatan;
2. melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, tidak boleh disangkal, ketersediaan dan kesahihan *(*confidentiality, integrity, authenticity, accessibility, accountability *(CIA^3))*;
3. meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;
4. meningkatkan tahap kesedaran keselamatan ICT kepada para pengguna;
5. memperkemaskan pengurusan risiko;
6. mencegah penyalahgunaan atau kecurian aset ICT; dan
7. melindungi aset ICT daripada penyelewengan oleh pengguna.

PERNYATAAN DASAR

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

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Terdapat empat komponen asas keselamatan ICT, iaitu:

1. melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan dari capaian tanpa kuasa yang sah;
2. menjamin setiap maklumat adalah tepat dan sempurna;
3. memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
4. memastikan akses hanya kepada pengguna yang sah atau penerimaan maklumat daripada sumber yang sah.

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

1. Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau diakses tanpa kebenaran;
2. Integriti - Data dan maklumat hendaklah tepat, lengkap dan terkini. Ia hanya boleh dipinda dengan cara yang dibenarkan;
3. Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh dipertikai;
4. Kesahihan - Data dan maklumat hendaklah diakui sah; dan
5. Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

Sistem ICT MetMalaysia terdiri daripada organisasi, perkakasan, perisian, manusia, perkhidmatan ICT, premis, data dan maklumat. MetMalaysia telah menetapkan keperluan-keperluan asas adalah seperti berikut:

1. data dan maklumat dalam bentuk salinan bercetak atau/dan digital hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ia amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan serta berkualiti; dan
2. semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan MetMalaysia dan Kerajaan.

Bagi memastikan keselamatan sistem ICT sentiasa terjamin, DKICT ini merangkumi perlindungan ke atas semua bentuk maklumat Kerajaan yang dimasuk, diwujud, disimpan, dijana, dicetak, diakses, diedar, disalin dan dimusnah dalam semua aset ICT. Ini dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara berikut:

1. **Perkakasan**
   Semua perkakasan komputer dan periferal (server, workstation, komputer peribadi, pencetak, firewall dan lain-lain), peralatan multimedia (webcam, headset, projektor dan lain-lain) dan perkakasan komunikasi (*gateway*, *router*, wireless access point dan lain-lain).
2. **Perisian**
   Semua jenis perisian yang digunakan untuk mengendali, memproses, menyimpan dan menghantar data atau maklumat termasuk perisian pengoperasian.
3. **Data atau/dan Maklumat**
   Semua data atau/dan maklumat yang disimpan atau digunakan di dalam pelbagai media atau peralatan ICT.
4. **Media Storan**
   Semua media storan dan peralatan yang berkaitan, seperti kartrij, pemacu kilat, pita, cakera optik, cakera liut, cakera keras dan lain-lain.
5. **Dokumentasi**
   Semua dokumen termasuk prosedur dan manual pengguna yang berkaitan dengan aset ICT, dokumen pemasangan dan pengoperasian peralatan dan perisian.
6. **Premis Komputer**
   Semua kemudahan serta premis yang diguna untuk menempatkan perkara 1 hingga 5 di atas.

7. **Perkhidmatan Sokongan ICT**
   Perkhidmatan yang menyokong sistem ICT melaksanakan fungsi-fungsinya seperti talian LAN/WAN, bekalan elektrik, penyaman udara, pencegah kebakaran dan lain-lain.

8. **Manusia**
   Semua pengguna infrastruktur ICT MetMalaysia yang dibenarkan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT MetMalaysia adalah seperti berikut :

1. **Akses atas dasar perlu mengetahui**

   Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar perlu mengetahui sahaja. Akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut sahaja.

2. **Hak akses minimum**

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

3. **Akauntabiliti**

   Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

4. **Pengasingan**

   Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi.

5. **Pengauditan**

   Pengauditan dilaksanakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan aset ICT. Semua perkakasan dipastikan dapat menjana dan menyimpan log bagi tujuan jejak audit (audit trail).

6. **Pematuhan**

   DKICT MetMalaysia hendaklah dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

7. **Pemulihan**

   Pemulihan sistem amat perlu untuk memastikan ketersediaan dan kebolehcapaian. Pemulihan boleh dilakukan melalui proses sandaran (backup) dan mewujudkan Pelan Kesinambungan Perkhidmatan (PKP).

8. Saling Bergantung

Setiap prinsip adalah lengkap melengkapi dan saling bergantung antara satu sama lain dalam menentukan kejayaan keselamatan sistem ICT. Kepelbagaian pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

PENILAIAN RISIKO KESELAMATAN ICT

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

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

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat MetMalaysia termasuklah aplikasi, perisian, perkakasan, pelayan, rangkaian, pangkalan data, sumber manusia, proses dan prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

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

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

1. mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
2. menerima atau/dan bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan tertinggi;
3. mengelak atau/dan mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
4. memindahkan risiko ke pihak ketiga dan pihak-pihak lain yang berkepentingan.

KAWALAN 01 : DASAR KESELAMATAN ICT

Objektif	
DKICT MetMalaysia ini diwujudkan untuk melindungi sistem ICT bagi memastikan kelancaran operasi Jabatan secara berterusan, meminimumkan kerosakan atau kemusnahan aset-aset ICT melalui usaha pencegahan atau mengurangkan kesan kejadian yang tidak diingini berdasarkan kepada ciri-ciri keselamatan iaitu kerahsiaan, integriti, tidak boleh disangkal, ketersediaan dan kesahihan.	
K01/01 Pelaksanaan Dasar	**Tindakan**
Pelaksanaan dasar ini dijalankan oleh Ketua Pengarah dan dibantu oleh Jawatankuasa Pemandu ICT (JPICT) yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pengurus ICT, Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik.	Ketua Pengarah
K01/02 Penyebaran Dasar	**Tindakan**
Dasar ini perlu disebarkan kepada semua pengguna yang terlibat dengan sistem ICT MetMalaysia.	ICTSO
K01/03 Penyelenggaraan Dasar	**Tindakan**
DKICT MetMalaysia adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan DKICT MetMalaysia: a. mengenal pasti dan menentukan perubahan yang diperlukan; b. mengemukakan cadangan pindaan secara bertulis untuk tindakan dan pertimbangan JPICT; c. memaklumkan pindaan yang telah diluluskan oleh JPICT kepada semua pengguna; dan d. menyemak semula dokumen mengikut keperluan bagi memastikan dokumen terkini.	ICTSO / JPICT
K01/04 Pematuhan Dasar	**Tindakan**
DKICT MetMalaysia adalah terpakai kepada semua pengguna.	Pengguna

KAWALAN 02 : KESELAMATAN ORGANISASI

<table>
<tr><th colspan="2">Objektif</th></tr>
<tr><td colspan="2">Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT MetMalaysia.</td></tr>
<tr><td colspan="2">K02/01 Infrastruktur Organisasi Dalaman</td></tr>
<tr><td>K02/01/01 Ketua Pengarah (KP)</td><td>Tindakan</td></tr>
<tr><td>Peranan dan tanggungjawab KP MetMalaysia adalah seperti berikut:
a. memastikan semua pengguna memahami peruntukan di bawah DKICT MetMalaysia;
b. memastikan semua pengguna mematuhi DKICT MetMalaysia;
c. memastikan semua keperluan organisasi seperti sumber kewangan, sumber manusia dan perlindungan keselamatan adalah mencukupi; dan
d. memastikan penilaian risiko keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT MetMalaysia.</td><td>KP</td></tr>
<tr><td>K02/01/02 Ketua Pegawai Maklumat (CIO)</td><td>Tindakan</td></tr>
<tr><td>Jawatan CIO adalah disandang oleh Timbalan Ketua Pengarah (Strategik & Teknikal).
Peranan dan tanggungjawab CIO adalah seperti berikut:
a. membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;
b. bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MetMalaysia;
c. bertanggungjawab menyelaras dan mengurus pelan tindakan dan program keselamatan seperti penyediaan DKICT MetMalaysia, pelan latihan dan program kesedaran, pengurusan risiko dan pengauditan; dan
d. menentukan keperluan keselamatan ICT.</td><td>TKP(S)</td></tr>
<tr><td>K02/01/03 Pengurus ICT</td><td>Tindakan</td></tr>
<tr><td>Jawatan Pengurus ICT disandang oleh Pengarah Bahagian Komunikasi Meteorologi.
Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:</td><td>P(KM)</td></tr>
</table>

a. memastikan DKICT MetMalaysia difahami, dipatuhi dan dilaksanakan; b. mengkaji semula aspek-aspek keselamatan fizikal seperti kemudahan *backup* dan persekitaran bagi peralatan ICT yang perlu, dengan dibantu oleh ICTSO; c. memastikan DKICT dipatuhi dalam operasi semasa seperti berikut: i. pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; ii. pembelian atau peningkatan perisian dan sistem komputer; iii. perolehan teknologi dan perkhidmatan komunikasi baharu; iv. pelantikan dan pelaksanaan kerja-kerja pihak ketiga; dan v. memastikan tapisan keselamatan dilaksanakan terhadap pihak ketiga selaras dengan keperluan tahap perkhidmatan. d. memastikan laporan tentang ancaman keselamatan direkod; e. membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam Jabatan yang mematuhi DKICT MetMalaysia; f. membangun, mengkaji semula dan mengemas kini pelan kontingensi keselamatan ICT; dan g. merangka dan melaksanakan sistem kawalan capaian pengguna ke atas aset-aset ICT MetMalaysia.	
K02/01/04 Pegawai Keselamatan ICT (ICTSO)	**Tindakan**
Jawatan ICTSO MetMalaysia disandang oleh Penolong Pengarah Kanan Bahagian Komunikasi Meteorologi yang dilantik. Peranan dan tanggungjawab ICTSO adalah seperti berikut: a. mengurus keseluruhan program keselamatan ICT MetMalaysia; b. menguatkuasakan pelaksanaan DKICT MetMalaysia; c. menjalankan pengurusan risiko dan audit keselamatan ICT berpandukan dokumen Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) untuk mengenalpasti ketidakpatuhan kepada DKICT MetMalaysia; d. mencadangkan langkah-langkah pengukuhan bagi mematuhi dasar berkaitan keselamatan ICT MetMalaysia;	PPK(KM)

e. melaporkan insiden keselamatan ICT kepada CIO bagi insiden yang memerlukan Pelan Kesinambungan Perkhidmatan (PKP); f. melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (GCERT MAMPU) dan seterusnya membantu dalam penyiasatan atau pemulihan; g. menjalankan program-program kesedaran keselamatan ICT; h. menyedia dan menyebarkan amaran-amaran terhadap kemungkinan berlaku ancaman ke atas keselamatan ICT dan menyediakan khidmat nasihat serta langkah pemulihan yang bersesuaian; i. memastikan pematuhan DKICT MetMalaysia oleh pihak ketiga yang mengakses dan menggunakan aset-aset ICT MetMalaysia untuk tujuan penyelenggaraan, pemasangan, naik taraf dan sebagainya; j. menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu keselamatan ICT; k. memastikan DKICT MetMalaysia dikemaskini bersesuaian dengan dasar kerajaan, perubahan teknologi, arahan Jabatan dan ancaman siber dari semasa ke semasa; dan l. memastikan Pelan Strategik ICT MetMalaysia merangkumi aspek keselamatan ICT.	
K02/01/05 Ketua Pejabat	**Tindakan**
Peranan dan tanggungjawab Ketua Pejabat adalah seperti berikut: a. memastikan pengguna-pengguna di Pusat/Bahagian/Seksyen/Unit mematuhi DKICT MetMalaysia dan seterusnya melaporkan sebarang insiden berkaitan keselamatan ICT kepada ICTSO; b. memaklumkan kepada pentadbir sistem apabila kakitangan tamat perkhidmatan, bertukar, berkursus panjang atau berlaku perubahan dalam bidang tugas; c. mengenal pasti tahap capaian pengguna seperti yang ditetapkan di dalam DKICT MetMalaysia; d. memaklumkan dengan serta merta aktiviti-aktiviti tidak normal seperti pencerobohan/penggodaman dan pengubahsuaian data tanpa kebenaran; dan e. memastikan pembangunan sistem aplikasi mematuhi DKICT MetMalaysia.	Ketua Pejabat

K02/01/06 Pentadbir Sistem	Tindakan
Pentadbir-pentadbir Sistem adalah seperti berikut: a. Pentadbir Rangkaian; b. Pentadbir Pangkalan Data Dan Keselamatan; c. Pentadbir Laman Web; d. Pentadbir Pusat Data; e. Pentadbir Bilik Server DRC; f. Pentadbir Sistem Aplikasi; dan g. Pentadbir Emel.	Pentadbir Sistem
K02/01/06 (a) Pentadbir Rangkaian	**Tindakan**
Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut: a. memastikan *LAN* dan *WAN* MetMalaysia beroperasi sepanjang masa; b. memastikan semua peralatan dan perisian rangkaian diselenggara mengikut perancangan; c. merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; d. mengesan dan mengambil tindakan pembaikan segera ke atas masalah rangkaian; e. memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; f. memastikan sistem aplikasi boleh menjana dan menyimpan log bagi tujuan jejak audit (audit trail); g. memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan secara tidak sah ke rangkaian MetMalaysia; dan h. melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT (Security Posture Assessment (SPA)) serta penilaian risiko keselamatan maklumat.	Pentadbir Rangkaian
K02/01/06 (b) Pentadbir Pangkalan Data Dan Keselamatan	**Tindakan**
Peranan dan tanggungjawab Pentadbir Pangkalan Data Dan Keselamatan adalah seperti berikut: a. melaksanakan pemasangan dan penambahbaikan pangkalan data serta perisian lain yang berkaitan; b. memastikan pangkalan data boleh diakses pada setiap masa; c. melaksanakan pemantauan dan penyelenggaraan yang	Pentadbir Pangkalan Data Dan Keselamatan

berterusan ke atas pangkalan data; d. melaksanakan *backup* dan *restoration* ke atas pangkalan data; e. memastikan aktiviti pentadbiran pangkalan data seperti kawalan akses pengguna, penyelesaian masalah dan proses pengemaskinian data dilaksanakan dengan teratur; f. memastikan proses pembersihan data (housekeeping) dalam pangkalan data dilaksanakan; g. memastikan sistem aplikasi boleh menjana dan menyimpan log bagi tujuan jejak audit (audit trail); dan h. melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.	
K02/01/06 (c) Pentadbir Laman Web	**Tindakan**
Peranan dan tanggungjawab Pentadbir Laman Web adalah seperti berikut: a. menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b. memantau prestasi capaian dan memastikan akses yang lancar; c. memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka depan laman web; d. memastikan kawalan akses Pentadbir Kandungan Laman Web dilaksanakan; e. memastikan pembangunan laman web mematuhi ciri-ciri keselamatan; f. memastikan sistem aplikasi boleh menjana dan menyimpan log bagi tujuan jejak audit (audit trail). g. memastikan sistem pengoperasian dan perisian-perisian lain dalam *web server* beroperasi dengan lancar; h. melaksanakan *backup* secara berkala dan *restoration* bila perlu; dan i. melaporkan sebarang insiden atau ancaman siber ke atas laman web kepada ICTSO.	Pentadbir Laman Web
K02/01/06 (d) Pentadbir Pusat Data	**Tindakan**
Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut:	Pentadbir Pusat data

a. memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat; b. memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data; c. menyediakan penjadualan dan perancangan penghantaran *backup* ke atas data dan sistem secara berkala; dan d. memastikan Pusat Data sentiasa beroperasi mengikut prosedur yang telah ditetapkan.	
K02/01/06 (e) Pentadbir Bilik Server DRC	**Tindakan**
Peranan dan tanggungjawab Pentadbir Bilik Server DRC adalah seperti berikut: a. memastikan persekitaran fizikal dan keselamatan bilik server DRC berada dalam keadaan baik dan selamat; b. memastikan keselamatan aset-aset ICT yang berada dalam bilik server DRC; dan c. memastikan kawalan akses ke bilik server DRC mengikut prosedur yang telah ditetapkan.	Pentadbir Bilik Server DRC
K02/01/06 (f) Pentadbir Sistem Aplikasi	**Tindakan**
Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut: a. mengkaji sistem sedia ada; b. mencadangkan keperluan pembangunan sistem aplikasi bagi penambahbaikan; c. memantau dan menyelenggara sistem dari semasa ke semasa; d. bertanggungjawab dalam aspek pelaksanaan keseluruhan sistem; e. menyediakan dokumentasi sistem dan manual pengguna; f. memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan tidak terjejas; g. memastikan pembangunan sistem aplikasi mematuhi ciri-ciri keselamatan sebelum sistem beroperasi; h. memastikan sistem aplikasi boleh menjana dan menyimpan log bagi tujuan jejak audit (audit trail). i. memastikan *virus pattern*, *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemaskini bagi mengurangkan risiko	Pentadbir Sistem Aplikasi

ancaman virus dan penggodam; j. mematuhi DKICT semasa mewujudkan akaun pengguna bagi setiap sistem aplikasi; k. memastikan *backup* sistem aplikasi dan data yang berkaitan dilaksanakan secara berjadual; l. menghadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan penyalahgunaan; dan m. melaporkan kepada ICTSO jika berlaku insiden dan ancaman siber ke atas sistem aplikasi.	
K02/01/06 (g) Pentadbir Emel	**Tindakan**
Peranan dan tanggungjawab Pentadbir Emel adalah seperti berikut: a. menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (kakitangan yang tamat perkhidmatan, bertukar atau melanggar DKICT jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; b. membekukan akaun kakitangan jika perlu semasa kakitangan bercuti panjang, berkursus atau menghadapi tindakan tatatertib; c. memastikan akaun kakitangan sentiasa di dalam keadaan baik dan berfungsi; d. memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan seperti serangan virus, serangan *e-mail spamming, phishing,* pencerobohan emel dan penyalahgunaan emel. Pentadbir emel hendaklah mengurus dan menangani insiden yang berlaku dengan segera dan sistematik sehingga keadaan kembali pulih; e. menyediakan ruang *mailbox* yang mencukupi sekurang-kurangnya 500MB untuk setiap akaun emel dan jumlah ini adalah bergantung kepada keperluan pemilik akaun emel; f. menggunakan kaedah inovatif dalam penghantaran fail bersaiz besar seperti menggunakan kaedah muat-turun fail dengan memaklumkan lokasi *universal resource location* (URL) atau kaedah pemampatan untuk mengurangkan saiz fail dengan memastikan ciri-ciri keselamatan dilaksanakan; g. memastikan agar keupayaan *mail relay* hanya boleh digunakan untuk *server* atau aplikasi dalaman MetMalaysia sahaja bagi tujuan keselamatan; h. memastikan kemudahan membuat capaian emel melalui pelbagai media seperti telefon mudah alih; dan	Pentadbir Emel

i. memastikan kakitangan MetMalaysia berkemahiran menggunakan emel berpandukan dokumen tatacara penggunaan emel dan Internet MetMalaysia serta pelaksanaan Kursus Pembudayaan IT (Penggunaan Emel dan Internet) secara berterusan.	
K02/01/07 Pengguna	**Tindakan**
Pengguna mempunyai peranan dan tanggungjawab seperti berikut: a. membaca, memahami dan mematuhi DKICT MetMalaysia; b. mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; d. mematuhi prinsip-prinsip DKICT dan menjaga kerahsiaan maklumat MetMalaysia; e. melaksanakan langkah-langkah perlindungan seperti berikut: • menghindari pendedahan maklumat kepada pihak yang tidak dibenarkan; • memastikan kesahihan maklumat dari semasa ke semasa; • menjaga kerahsiaan kata laluan; • melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; f. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; g. menghadiri program-program kesedaran mengenai keselamatan ICT; dan h. menandatangani Surat Akuan Pematuhan DKICT MetMalaysia.	Pengguna
K02/01/08 Jawatankuasa Pemandu ICT (JPICT)	**Tindakan**
Keanggotaan JPICT adalah seperti berikut: **Pengerusi:** Ketua Pengarah **Timbalan Pengerusi:** Timbalan Ketua Pengarah (Strategik & Teknikal)	JPICT

Ahli: a. Timbalan Ketua Pengarah (Operasi); b. Pengarah Kanan Pusat Meteorologi Penerbangan Nasional; c. Pengarah Kanan Pusat Instrumentasi Meteorologi dan Sains Atmosfera; d. Pengarah Pusat Operasi Cuaca dan Geofizik Nasional; e. Pengarah Pusat Iklim Nasional; f. Pengarah Bahagian Sains Atmosfera dan Pembenihan Awan; g. Pengarah Bahagian Radar & Satelit Meteorologi; h. Pengarah Bahagian Penyelidikan dan Pembangunan Teknikal; i. Pengarah Bahagian Komunikasi Meteorologi; j. Pengarah Bahagian Latihan Teknikal; k. Pengarah Bahagian Perancangan Strategik dan Antarabangsa; l. Pengarah Bahagian Teknikal Cuaca dan Geofizik; m. Pengarah Bahagian Instrumentasi Meteorologi; n. Pengarah Bahagian Khidmat Pengurusan; o. Ketua Unit Komunikasi Korporat; p. Ketua Unit Integriti; q. Ketua Pen. Pengarah Bahagian Komunikasi Meteorologi; dan r. Pen. Pengarah Kanan Seksyen Data & Keselamatan ICT s. Pen. Pengarah Kanan Seksyen Multimedia & Pembangunan. **Urusetia :** a. Pegawai Teknologi Maklumat F44 (MP); b. Pegawai Meteorologi C41/44 (RN); c. Pegawai Meteorologi C41/44 (DK). **Bidang kuasa:** a. menetapkan arah tuju dan strategi untuk pembangunan dan pelaksanaan ICT Jabatan; b. Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/ strategi ICT Jabatan; c. merancang dan menyelaras pelaksanaan program/ projek ICT MetMalaysia;	

d. menyelaras dan menyeragamkan pelaksanaan ICT MetMalaysia agar selari dengan Pelan Strategik ICT Jabatan; e. meluluskan projek-projek ICT agensi berdasarkan kepada keperluan sebenar dan perbelanjaan yang berhemah serta mematuhi peraturan semasa; f. mengikuti dan memantau perkembangan program ICT Jabatan serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT; g. mengemukakan perolehan ICT yang telah diluluskan di peringkat JPICT Jabatan kepada JPICT Kementerian untuk kelulusan; h. mengemukakan laporan kemajuan projek ICT yang telah diluluskan oleh JPICT kepada JPICT Kementerian mengikut tempoh-tempoh yang telah ditetapkan; dan i. mempertimbang dan meluluskan cadangan pindaan DKICT Jabatan.	
K02/01/09 Jawatankuasa Pemandu Pengurusan Sistem Keselamatan Maklumat (MS ISO/IEC 27001) (JPISMS)	**Tindakan**
Keanggotaan JPISMS adalah seperti berikut: **Pengerusi:** CIO/ TKP(S) **Timbalan Pengerusi:** Pengarah Bahagian Komunikasi Meteorologi **Ahli:** a. Pengarah Kanan Pusat Meteorologi Penerbangan Nasional; b. Pengarah Kanan Pusat Instrumentasi Meteorologi & Sains Atmosfera; c. Pengarah Pusat Operasi Cuaca Dan Geofizik Nasional; d. Pengarah Pusat Iklim Nasional; e. Pengarah Bahagian Teknikal Cuaca & Geofizik; f. Pengarah Bahagian Instrumentasi Meteorologi; g. Pengarah Bahagian Khidmat Pengurusan; h. Pengarah Bahagian Sains Atmosfera & Pembenihan Awan; i. Pengarah Bahagian Radar & Satelit Meteorologi; j. Pengarah Bahagian Penyelidikan & Pembangunan Teknikal; k. Pengarah Bahagian Latihan Teknikal; l. Pengarah Bahagian Perancangan Strategik & Antarabangsa;	JPISMS

m. Ketua Unit Komunikasi Korporat; n. Ketua Pen. Pengarah Rangkaian; o. Pen. Pengarah Kanan Data Dan Keselamatan ICT; dan p. Pen. Pengarah Kanan Multimedia Dan Pembangunan. q. Pengarah Negeri yang terlibat dengan Skop ISMS **Urusetia:** a. Pegawai Meteorologi (C44) DK, b. Pegawai Meteorologi (C44) RN – 3 orang c. Pegawai Teknologi Maklumat (F44) MP. **Bidang kuasa adalah memperakui:** a. Skop ISMS MS ISO/IEC 27001; b. keperluan kursus kesedaran untuk melaksanakan standard piawaian MS ISO/IEC 27001; c. pelaksanaan pensijilan ISMS ke atas perkhidmatan dalam skop ISMS di MetMalaysia; meluluskan Skop ISMS; d. kriteria penerimaan risiko, tahap risiko, penemuan awal penilaian risiko dan risk treatment plan; e. struktur organisasi ISMS; f. Mesyuarat Kajian Semula Pengurusan ISMS; g. menyediakan sumber-sumber untuk melaksanakan ISMS; h. menguruskan dokumen dan rekod pelaksanaan ISMS; i. laporan audit dan laporan audit susulan; dan j. tindakan pembetulan dan pencegahan ke atas ketakakuran yang ditemui oleh pasukan audit.	
K02/01/10 Pasukan Tindak Balas Insiden Keselamatan ICT (CERT MetMalaysia)	**Tindakan**
Keanggotaan CERT MetMalaysia adalah seperti berikut: **Penasihat:** CIO **Pengarah CERT:** Pengurus ICT **Pengurus CERT:** ICTSO **Setiausaha CERT:** Penolong Pegawai Teknologi Maklumat (Data dan Keselamatan ICT)	Pasukan CERT

Setiap Pasukan CERT terdiri daripada: Ketua Pasukan dan sekurang-kurangnya 4 orang ahli pasukan. **Ketua Pasukan Bertugas:** i. Ketua Penolong Pengarah Bahagian Komunikasi Meteorologi ii. Penolong Pengarah Kanan Bahagian Komunikasi Meteorologi (Data dan Keselamatan ICT) iii. Penolong Pengarah Kanan Bahagian Komunikasi Meteorologi (Multimedia dan Pembangunan) iv. Penolong Pengarah Kanan Bahagian Komunikasi Meteorologi (Rangkaian) **Ahli Pasukan:** i. Wakil Rangkaian ii. Wakil Multimedia & Pembangunan iii. Wakil Data & Keselamatan ICT Pelaksanaan jadual tugasan secara mingguan bagi setiap pasukan akan dibuat setiap bulan yang mana setiap pasukan akan bertugas selama seminggu. Sebarang insiden akan diambil tindakan awal dan dilaporkan oleh pasukan bertugas.	
K02/01/11 Pasukan Pemulihan Bencana (DRT) MetMalaysia	**Tindakan**
Keanggotaan Pasukan DRT adalah seperti berikut: Ketua: Pengarah Bahagian Komunikasi Meteorologi Timbalan Ketua: Pengarah Bahagian Teknikal Cuaca dan Geofizik **Ahli:** a. Ketua Penolong Pengarah Pusat Operasi Cuaca dan Geofizik Nasional (Cuaca); b. Ketua Penolong Pengarah Pusat Meteorologi Penerbangan Nasional; c. Ketua Penolong Pengarah Pusat Operasi Cuaca dan Geofizik Nasional (Geofizik); d. Ketua Penolong Pengarah Bahagian Komunikasi Meteorologi; e. Ketua Penolong Pengarah Bahagian Radar dan Satelit Meteorologi; f. Penolong Pengarah Kanan Bahagian Teknikal Cuaca dan Geofizik; g. Penolong Pengarah Kanan Bahagian Penyelidikan dan Pembangunan Teknikal;	Pasukan DRT

h. Penolong Pengarah Kanan Bahagian Instrumentasi Meteorologi & Sains Atmosfera; i. Penolong Pengarah Kanan Bahagian Komunikasi Meteorologi (Multimedia dan Pembangunan); j. Penolong Pengarah Kanan Bahagian Komunikasi Meteorologi (Data dan Keselamatan ICT); dan k. Penolong Pengarah Pusat Meteorologi Penerbangan Nasional. **Urusetia DRT:** a. Pegawai Teknologi Maklumat (Data & Keselamatan ICT); b. Penolong Pegawai Teknologi Maklumat (F29) (Multimedia dan Pembangunan); dan c. Penolong Pegawai Meteorologi (C29) (Bahagian Teknikal Cuaca dan Geofizik). **Bidang kuasa:** a. mengenal pasti dan menentukan fungsi kritikal MetMalaysia; b. melaksanakan penilaian risiko dan analisis impak perkhidmatan bagi fungsi kritikal yang telah dikenalpasti; c. menyediakan dan mendokumentasikan Pelan Pemulihan Bencana (DRP) MetMalaysia; d. merancang dan menguji Pelan Simulasi DRP MetMalaysia serta menyedia laporan simulasi; e. menyelaras dan melaksanakan tanggungjawab serta peranan seperti yang telah ditetapkan; f. mengenal pasti penambahbaikan keperluan DRP bagi setiap fungsi kritikal; dan g. mengemaskini dokumen DRP dan mengedarkan semula setiap kali terdapat perubahan.	
K02/02 PIHAK KETIGA	
K02/02/01 Keperluan Keselamatan Dalam Kontrak ICT	**Tindakan**
Perkara–perkara yang perlu dipatuhi adalah: a. membaca, memahami dan mematuhi DKICT MetMalaysia; b. mengenal pasti risiko ke atas keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c. memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga;	CIO Pengurus ICT, ICTSO, Pentadbir Sistem

d. akses kepada aset ICT MetMalaysia perlu berlandaskan kepada perjanjian kontrak; e. Perjanjian yang dimeterai perlu mematuhi perkara-perkara berikut: i. DKICT MetMalaysia; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; iv. RAKKSSA; dan v. Hak Harta Intelek; f. menandatangani Surat Akuan Pematuhan DKICT MetMalaysia**;**	

KAWALAN 03 : PENGURUSAN ASET

Objektif	
Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MetMalaysia.	
K03/01 Akauntabiliti Aset	**Tindakan**
Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi: a. memastikan semua aset ICT dikenal pasti, dikelas, didokumen, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini dalam Sistem Pengurusan Aset (SPA), Kad Daftar Harta Modal dan Inventori sebagaimana mengikut Pekeliling Perbendaharaan Bil.5 Tahun 2007: Tatacara Pengurusan Aset Alih Kerajaan (TPA); b. memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c. memastikan semua pengguna mengesahkan penempatan aset ICT di MetMalaysia; d. memastikan semua peraturan pengendalian aset ICT dilaksanakan; dan e. setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pegawai Aset, Pengguna
K03/02 Pengelasan Maklumat	**Tindakan**
Maklumat hendaklah diklasifikasikan dengan sewajarnya oleh pegawai yang diberi kuasa berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada MetMalaysia. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad.	KP, TKP, Pegawai yang diturunkan kuasa
K03/03 Pengendalian Maklumat	**Tindakan**
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut:	Pengguna

a. menghindari pendedahan maklumat kepada pihak yang tidak dibenarkan; b. memastikan kesahihan maklumat dari semasa ke semasa; c. menjaga kerahsiaan kata laluan; d. melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan e. menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.	

KAWALAN 04 : KESELAMATAN SUMBER MANUSIA

Objektif	
Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan MetMalaysia, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua kakitangan MetMalaysia hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
K04/01 Sebelum Perkhidmatan	**Tindakan**
Memastikan pengguna memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan warga MetMalaysia serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. menjalankan tapisan keselamatan untuk kakitangan; c. menentukan keperluan bagi menandatangani tapisan keselamatan oleh pembekal, pakar runding dan pihak-pihak lain yang berkepentingan selaras dengan keperluan tahap dan skop perkhidmatan; dan d. mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Pengurus ICT, Seksyen Pengurusan Sumber Manusia, Ketua Pejabat
K04/02 Semasa Perkhidmatan	**Tindakan**
Memastikan pengguna sedar mengenai ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong DKICT MetMalaysia dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. memastikan pengguna menjaga keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan; b. memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna secara berterusan dari semasa ke semasa; c. memastikan adanya proses tindakan disiplin dan/atau	Pengguna

undang-undang ke atas pegawai dan kakitangan serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan yang ditetapkan oleh MetMalaysia; dan d. memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul.	
K04/02/01 Program Kesedaran Keselamatan ICT	**Tindakan**
Setiap pengguna di MetMalaysia perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT.	Pengurus ICT, ICTSO
K04/03 Bertukar Atau Tamat Perkhidmatan	**Tindakan**
Memastikan semua pengguna MetMalaysia yang tamat perkhidmatan atau bertukar diurus dengan teratur. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan semua aset ICT dikembalikan kepada MetMalaysia mengikut peraturan dan/atau terma mengikut pekeliling yang berkuatkuasa; dan b. membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh MetMalaysia dan/atau terma perkhidmatan.	Pengurus ICT, Seksyen Pengurusan Sumber Manusia, Ketua Pejabat

KAWALAN 05 : KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif	
Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
K05/01 Keselamatan Kawasan	
K05/01/01 Kawalan Kawasan	**Tindakan**
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c. memasang alat penggera atau kamera; d. menghadkan jalan keluar masuk; e. mengadakan kaunter Khidmat Pelanggan; f. menyediakan ruang khas untuk pelawat; g. mewujudkan perkhidmatan kawalan keselamatan; h. melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; i. melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; j. melaksanakan perlindungan fizikal daripada bencana, seperti kebakaran, banjir dan letupan; dan k. memastikan kawasan-kawasan penghantaran dan pemunggahan dikawal daripada pihak yang tidak diberi kebenaran memasukinya.	Jawatankuasa Keselamatan

K05/01/02 Kawalan Masuk Fizikal	Tindakan
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Kakitangan i. Semua kakitangan hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; dan ii. Semua pas keselamatan hendaklah diserahkan kembali kepada MetMalaysia apabila kakitangan berpindah, berhenti atau bersara. b. Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu masuk utama premis MetMalaysia. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan c. Kehilangan pas mestilah dilaporkan dengan segera kepada Seksyen Pentadbiran, Bahagian Khidmat Pengurusan MetMalaysia.	Seksyen Pentadbiran, Bahagian Khidmat Pengurusan, Pengguna

K05/01/03 Kawasan Larangan	Tindakan
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada kakitangan yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di MetMalaysia adalah Pusat Data dan kawasan-kawasan lain yang dikategorikan sebagai kawasan larangan oleh Jabatan. Kawasan larangan hanya boleh diakses oleh kakitangan yang dibenarkan sahaja. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan **kecuali** bagi kes tertentu, seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah mendapat kebenaran dan diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Pentadbir Pusat Data, ICTSO, Pengurus ICT, Pengguna

K05/01/04 Kawalan Kawasan Larangan	Tindakan
Kawasan ini mestilah dilindungi daripada sebarang ancaman dan risiko, seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas premis tersebut adalah seperti berikut: a. sumber data atau *server,* peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik *server* atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran;	ICTSO, Pentadbir Pusat Data

b. akses adalah terhad kepada kakitangan yang telah diberi kebenaran sahaja dan dipantau pada setiap masa; c. pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) kamera atau lain-lain peralatan yang sesuai; d. peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual; e. butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; f. pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; g. lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan dan laluan awam; h. memperkukuhkan tingkap dan pintu berkunci; i. memperkukuhkan dinding dan siling; j. menghadkan jalan keluar masuk; dan k. menyediakan ruang khas untuk pelawat.	
K05/02 Keselamatan Peralatan	
K05/02/01 Peralatan ICT	**Tindakan**
a. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan. b. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan. c. Pengguna dilarang membuat pemasangan sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem. d. Pengguna mesti memastikan perisian *antivirus* bagi semua peralatan ICT yang dibekalkan oleh Jabatan, seperti komputer peribadi, *notebook, server* termasuk alat komunikasi mudah alih berada di bawah tanggungjawab mereka sentiasa aktif dan dikemas kini di samping turut melakukan imbasan ke atas media storan yang digunakan. e. Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, disalahguna dan diubah suai tanpa kebenaran. f. Aset ICT hendaklah disimpan di tempat yang selamat dan sentiasa di bawah kawalan pegawai yang bertanggungjawab. Arahan berkaitan keselamatan yang dikeluarkan oleh Kerajaan hendaklah sentiasa dipatuhi bagi mengelak	Ketua Pejabat, Pentadbir Sistem, Pegawai Aset, Pengguna

berlakunya kerosakan atau kehilangan aset. g. Jika peralatan ICT tidak digunakan, peralatan tersebut hendaklah disimpan di dalam almari / kabinet / peti besi / stor atau bilik khas yang berkunci. h. Peralatan-peralatan kritikal perlu disokong oleh UPS. i. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian, seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam bilik atau rak berkunci. j. Semua peralatan termasuk UPS berkuasa tinggi yang digunakan secara berterusan mestilah diletakkan di kawasan yang dilengkapi penyaman udara dan mempunyai pengudaraan yang sesuai. k. Peralatan ICT yang hendak dibawa keluar dari premis MetMalaysia, perlulah mendapat kelulusan Pegawai Aset atau Ketua Pejabat bagi tujuan pemantauan dan perlu direkodkan dalam buku log. l. Aset ICT yang hilang hendaklah dikendalikan mengikut Prosedur Pengendalian Insiden Keselamatan Maklumat.	
K05/02/02 Media Storan	**Tindakan**
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat, seperti cakera padat, pita magnetik dan pemacu kilat. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan ketersediaan untuk digunakan. Bagi menjamin keselamatan, langkah-langkah berikut perlu diambil: a. semua media storan perlu dikawal bagi mencegah daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan; b. bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu; c. semua media storan hendaklah dilupuskan dengan teratur dan selamat; d. semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; e. semua media storan dan *backup* hendaklah disimpan di lokasi yang berasingan yang lebih privasi dan tidak terbuka kepada umum. Akses untuk memasuki kawasan	Pentadbir Sistem, Pegawai Aset, Ketua Pejabat

penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; f. akses dan pergerakan media storan perlu direkod; g. media storan yang hendak dibawa keluar dari premis MetMalaysia perlulah mendapat kelulusan Ketua Pejabat bagi tujuan pemantauan; h. perkakasan *backup* (CD/DVD duplicator/external hardisk) hendaklah diletakkan di tempat yang lebih privasi dan terhad kepada pengguna yang dibenarkan sahaja; dan i. sebarang kehilangan media storan yang berlaku hendaklah dilaporkan mengikut Prosedur Pengendalian Ast ICT.	
K05/02/03 Media Tandatangan Digital	**Tindakan**
Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah–langkah berikut: a. pengguna hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b. tidak boleh dipindah milik atau dipinjamkan; dan c. sebarang kehilangan yang berlaku hendaklah dilaporkan mengikut Prosedur Pengendalian Ast ICT.	Pentadbir Sistem, Pengguna
K05/02/04 Media Perisian Dan Aplikasi	**Tindakan**
Sebarang media yang digunakan sebagai media perisian dan aplikasi hendaklah mematuhi langkah-langkah berikut: a. hanya perisian yang rasmi sahaja dibenarkan bagi kegunaan jabatan; b. sistem aplikasi dalaman tidak dibenarkan diagih/di demonstrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c. lesen perisian (registration code, serial numbers, CD-keys) perlu disimpan berasingan daripada *CD-ROM*, *disk* atau media berkaitan bagi mengelakkan daripada berlakunya kecurian atau cetak rompak; dan d. *source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Pengurus ICT, Pegawai Aset, Pentadbir Sistem

<table>
<tr><th>K05/02/05 Perkakasan Tanpa Penyeliaan (Unattended Equipment)</th><th>Tindakan</th></tr>
<tr><td>Pengguna perlu memastikan mana-mana perkakasan yang ditinggalkan tanpa penyeliaan mematuhi ciri-ciri keselamatan, seperti mempunyai kata laluan, screen saver dan log off.

Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan ketersediaan, kerahsiaan dan integriti.</td><td>Pengguna</td></tr>
<tr><th>K05/02/06 Peralatan di Luar Premis</th><th>Tindakan</th></tr>
<tr><td>Perkakasan yang dibawa keluar dari premis MetMalaysia adalah terdedah kepada pelbagai risiko. Perkakasan tersebut merangkumi:
a. penggunaan perkakasan secara sementara bagi keperluan mesyuarat, latihan dan sebagainya; dan
b. penempatan perkakasan secara kekal di agensi lain.
Prosedur yang perlu dipatuhi adalah seperti berikut:
a. mendapat kelulusan Ketua Pejabat;
b. peralatan perlu dilindungi dan dikawal sepanjang masa; dan
c. penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.</td><td>Ketua Pejabat</td></tr>
<tr><th>K05/02/07 Pelupusan</th><th>Tindakan</th></tr>
<tr><td>Aset ICT yang hendak dilupuskan perlu mematuhi tatacara pelupusan semasa. Langkah-langkah berikut perlu diambil dalam memastikan peralatan ICT MetMalaysia dilupuskan dengan teratur, iaitu:
a. Pegawai Aset mengenal pasti peralatan yang boleh dilupuskan atau sebaliknya;
b. peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan;
c. data dan maklumat dalam aset ICT yang dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal;
d. pelupusan peralatan ICT boleh dilakukan secara berpusat/ tidak berpusat mengikut tatacara pelupusan semasa yang berkuat kuasa;
e. sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan;
f. maklumat lanjut berhubung pelupusan aset ICT boleh dirujuk</td><td>Pegawai Aset, Pengguna</td></tr>
</table>

kepada Pekeliling Perbendaharaan 5 Tahun 2007: Tatacara Pengurusan Aset Alih Kerajaan (TPA); dan g. pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara.	
K05/02/08 Penyelenggaraan	**Tindakan**
Peralatan hendaklah diselenggarakan dengan betul bagi memastikan ketersediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil, adalah seperti berikut: a. mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; b. memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c. menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan d. memaklumkan kepada pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pentadbir Sistem, Pengurus ICT, Pegawai Aset
K05/03 Kawalan Persekitaran	
K05/03/01 Kawalan Persekitaran	**Tindakan**
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk perolehan, menyewa dan mengubah suai hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: a. merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer, ruang atur pejabat dan sebagainya) dengan teliti; b. semua ruang pejabat khususnya yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan, seperti alat pencegah kebakaran, pintu kalis api dan pintu kecemasan; c. peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. bahan mudah terbakar hendaklah disimpan di luar kawasan penyimpanan aset ICT;	Bahagian Khidmat Pengurusan

e. semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. pengguna dilarang merokok atau menggunakan peralatan memasak berhampiran peralatan komputer; dan g. semua peralatan perlindungan keselamatan dan kebakaran hendaklah diselenggara bagi memastikan ia berfungsi dengan baik.	
K05/03/02 Kabel Rangkaian	**Tindakan**
a. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat. b. Menggunakan kabel mengikut spesifikasi yang telah ditetapkan. c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping.*	Pentadbir Rangkaian
K05/03/03 Bekalan Kuasa	**Tindakan**
Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa: a. semua peralatan ICT hendaklah dilindungi daripada kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. peralatan sokongan seperti UPS dan janakuasa boleh digunakan bagi perkhidmatan kritikal di Pusat Data dan ruang Operasi supaya mendapat bekalan kuasa berterusan; dan c. semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.	Pengurus ICT, Bahagian Khidmat Pengurusan
K05/03/04 Prosedur Kecemasan	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Pelan Kesinambungan Perkhidmatan MetMalaysia; dan b. kecemasan persekitaran, seperti kebakaran, kebocoran gas dan keruntuhan siling hendaklah dilaporkan kepada Ketua Pejabat/ Wakil Tingkat yang dilantik mengikut aras.	Ketua Pejabat/ Wakil Tingkat

K05/04 Keselamatan Sistem Dokumentasi	Tindakan
Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi: a. memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada; c. setiap dokumen hendaklah direkod dan difailkan; d. dokumen terperingkat hendaklah dikelaskan mengikut peringkat keselamatan selaras dengan Arahan Keselamatan, seperti Terhad, Sulit, Rahsia atau Rahsia Besar; e. pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut Panduan Pengendalian Fail Rasmi; f. kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut Pekeliling Perkhidmatan Bil.5 Tahun 2007 Panduan Pengurusan Pejabat; dan g. menggunakan enkripsi (encryption) ke atas dokumen rahsia rasmi yang disedia, disimpan dan dihantar secara elektronik.	Pentadbir Sistem, Pentadbir Fail

KAWALAN 06 : PENGURUSAN OPERASI DAN KOMUNIKASI

Objektif	
Memastikan pengurusan operasi dan perkhidmatan pemprosesan maklumat berfungsi dengan betul dan selamat daripada ancaman dan gangguan.	
K06/01 Prosedur Operasi	
K06/01/01 Pengendalian Dokumen Prosedur Operasi	**Tindakan**
a. Semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal. b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap, seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti. c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa.	Pentadbir Sistem
K06/01/02 Pengurusan Perubahan	**Tindakan**
a. Pengubahsuaian yang melibatkan perkakasan, sistem pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu. b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan. c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat.	Pentadbir Sistem
K06/01/03 Pengasingan Tugas dan Tanggungjawab	**Tindakan**
a. Skop tugas dan tanggungjawab perlu diasingkan bagi meminimumkan penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT.	Pengurus ICT, ICTSO,

b. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi maklumat dan data daripada kesilapan, kebocoran atau dimanipulasi. c. Perkakasan yang digunakan bagi tugas pembangunan modul baharu, pengemaskinian, penyelenggaraan dan pengujian aplikasi baharu hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*.	Pentadbir Sistem
K06/01/04 Prosedur Pengurusan Insiden	**Tindakan**
CERT MetMalaysia menerima aduan atau laporan daripada pengguna, laporan yang dikesan daripada MyGSOC atau sumber luar. Maklumat insiden tersebut akan direkodkan dan siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden. Laporan insiden akan dikemukakan kepada GCERT MOSTI dan GCERT MAMPU sebagai input untuk tindakan selanjutnya. Sekiranya insiden tersebut memerlukan tindakan undang-undang, laporan dipanjangkan kepada agensi penguatkuasa undang-undang. CERT MetMalaysia yang diketuai oleh ICTSO akan menjalankan tindakan pengendalian secara capaian jauh (remote) atau on-site. Sekiranya laporan tersebut memerlukan bantuan GCERT MOSTI atau GCERT MAMPU, permohonan akan dihantar bagi mendapatkan maklum balas. CERT MetMalaysia akan memaklumkan Pengurus ICT berkenaan insiden yang berlaku dan seterusnya Pengurus ICT memaklumkan koordinator PKP. Koordinator PKP mengesyorkan kepada KP/TKP bagi mengaktifkan PKP, jika perlu. Laporan insiden yang tidak memerlukan PKP akan diteruskan dengan melaksanakan tindakan pemulihan.	CERT MetMalaysia, ICTSO, Pengurus ICT, Pengguna
K06/02 Perancangan, Pemasangan dan Penerimaan Sistem	
K06/02/01 Perancangan Kapasiti	**Tindakan**
a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti	Pentadbir Sistem

gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	
K06/02/02 Pemasangan Sistem	**Tindakan**
a. Memantau pengurusan dan pengagihan kapasiti sesuatu komponen atau sistem ICT bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. b. Memantau dan menyelaras penalaan penggunaan peralatan bagi memenuhi keperluan kapasiti akan datang supaya sistem beroperasi di tahap optimum. c. Menetapkan kriteria penerimaan sistem baharu dan sistem yang ditingkatkan. Pengujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem. d. Mengambil kira ciri-ciri keselamatan ICT dalam perancangan keperluan kapasiti supaya dapat meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian pengubahsuaian yang tidak dirancang.	Pengurus ICT, ICTSO, Pentadbir Sistem
K06/02/03 Penerimaan Sistem	**Tindakan**
Semua sistem baharu (termasuk sistem yang dikemas kini atau diubah suai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Ketua Pejabat, Pentadbir Sistem, Pengguna
K06/03 Perisian Berbahaya	
K06/03/01 Perlindungan daripada Perisian Berbahaya	**Tindakan**
Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya: a. memasang perisian keselamatan, seperti antivirus dan *Intrusion Detection Sistem* (IDS) untuk mengesan perisian/program berbahaya serta mengikut prosedur penggunaan yang betul dan selamat; b. memasang dan menggunakan perisian tulen; c. mengimbas semua perisian, sistem, media storan dan kepilan fail dengan antivirus sebelum menggunakannya; d. memastikan paten antivirus pada peralatan ICT dikemas kini dengan versi terkini;	ICTSO, Pentadbir Sistem, Pengguna

e. menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini, seperti kehilangan dan kerosakan maklumat; f. menghadiri program-program kesedaran mengenai ancaman *malware* dan cara mengendalikannya; g. memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus; h. memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; dan i. mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.	
K06/03/02 Perlindungan dari *Mobile Code*	**Tindakan**
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pengguna
K06/04 *Housekeeping*	
K06/04/01 *Backup*	**Tindakan**
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* mestilah dilakukan setiap kali perubahan berlaku. Perkara *backup* hendaklah direkodkan dan disimpan di *off site*, di samping melaksanakan perkara-perkara berikut: a. membuat *backup* untuk keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terkini; b. membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi; c. *backup* dilaksanakan secara harian, mingguan dan bulanan dan disimpan sekurang-kurangnya dalam tempoh masa tiga bulan; dan d. menguji sistem *backup* sedia ada dan memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.	Pentadbir Sistem
K06/05 Pengurusan Rangkaian	**Tindakan**
Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.	Pengguna

Langkah-langkah bagi menangani ancaman ke atas rangkaian, adalah seperti berikut: a. semua tanggungjawab atau kerja-kerja operasi yang melibatkan rangkaian dan perkakasan ICT hendaklah diasingkan untuk mengurangkan akses dan pengubahsuaian yang tidak dibenarkan; b. capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; c. semua capaian kepada Internet dan sistem aplikasi mestilah melalui *firewall*; d. memasang perisian IDS/IPS bagi mengesan dan menghalang sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MetMalaysia; e. memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; f. sebarang penyambungan rangkaian yang bukan di bawah kawalan MetMalaysia adalah tidak dibenarkan; g. semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan MetMalaysia; h. semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali dengan kebenaran ICTSO; i. semua pengguna hanya dibenarkan menggunakan rangkaian MetMalaysia sahaja. Penggunaan peranti peribadi menggunakan akses rangkaian MetMalaysia adalah dilarang sama sekali kecuali dengan kebenaran ICTSO; dan j. kemudahan *wireless LAN* perlu dipastikan kawalan keselamatannya.	
K06/06 Pengurusan Media	
K06/06/01 Media Mudah Alih	**Tindakan**
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Pengguna
K06/06/02 Prosedur Pengendalian Media	**Tindakan**
Di antara prosedur-prosedur pengendalian media termasuk: a. melabelkan semua media storan mengikut tahap sensitiviti sesuatu maklumat; b. menghadkan dan menentukan akses media storan kepada	Pengguna

pengguna yang sah sahaja; c. menghadkan pengedaran data atau media storan untuk tujuan yang dibenarkan; d. mengawal dan merekodkan aktiviti penyelenggaraan media storan bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. media storan yang hendak dibawa keluar dari premis MetMalaysia, perlulah mendapat kelulusan Pegawai Aset atau Ketua Pejabat berkenaan; f. menyimpan semua media storan di tempat yang selamat; dan g. media storan yang mengandungi maklumat terperingkat hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	
K06/07 Pengurusan Pertukaran Maklumat	**Tindakan**
Bagi memastikan keselamatan penghantaran dan penerimaan maklumat dalam agensi dan mana-mana entiti luar adalah terjamin, maka perkara-perkara berikut perlu dipatuhi: a. dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b. perjanjian perlu diwujudkan untuk pertukaran maklumat di antara MetMalaysia dengan agensi luar; c. media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan dan penerimaan; dan d. maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Pengguna
K06/08 Mel Elektronik (Emel)	**Tindakan**
Penggunaan emel di MetMalaysia hendaklah dipantau secara berterusan oleh Pentadbir Emel untuk memenuhi keperluan etika penggunaan emel dan internet. Prosedur-prosedur pengurusan emel seperti berikut: a. menghadkan jenis dan saiz fail lampiran bagi tujuan mengelakkan jangkitan virus dan serangan emel *bombing*; b. penghantaran dokumen rasmi hendaklah menggunakan emel rasmi jabatan sahaja; c. penggunaan emel MetMalaysia bagi tujuan peribadi adalah	Pengguna

tidak dibenarkan kecuali dengan kebenaran ICTSO; d. Pentadbir Emel perlu menetapkan had maksimum kuota *mailbox* dan saiz kepilan; e. penghantaran lampiran dalam format / *extension* "*.exe, *.bat" dan "*.com" tidak dibenarkan; f. bertanggungjawab ke atas *housekeeping* dan penggunaan *mailbox* masing-masing; g. pegawai yang dipertanggungjawabkan kepada emel bahagian/seksyen/pejabat tidak dibenarkan menggunakan emel tersebut di luar premis Jabatan kecuali dengan kebenaran Ketua Pejabat berkenaan; h. Ketua Pejabat perlu memaklumkan sebarang status pengguna (bertukar jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke MetMalaysia) di bahagian masing-masing bagi tujuan pengemaskinian emel yang terlibat; i. menggunakan kaedah inovatif dalam penghantaran fail bersaiz besar, seperti menggunakan kaedah muat turun fail dengan memaklumkan lokasi *Universal Resource Location* (URL) atau kaedah pemampatan untuk mengurangkan saiz fail dengan memastikan ciri-ciri keselamatan dilaksanakan; j. emel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang bersesuaian; k. menggunakan enkripsi bagi dokumen terperingkat yang dihantar secara elektronik; dan l. penggunaan emel mestilah merujuk kepada Garis Panduan dan Etika Penggunaan Emel dan Internet MetMalaysia terkini.	
K06/09 Perkhidmatan e-Dagang (e-Commerce)	**Tindakan**
Bagi memastikan keselamatan penggunaan perkhidmatan e-dagang, maka perkara-perkara berikut perlu dipatuhi; a. maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b. maklumat yang terlibat dalam transaksi atas talian perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c. integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan	Pentadbir Sistem, Pengguna

<table>
<tr><td>yang tidak diperakukan.</td><td></td></tr>
<tr><td>K06/10 Paparan Maklumat Umum</td><td>Tindakan</td></tr>
<tr><td>Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut:
a. memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu;
b. memastikan segala maklumat yang dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web; dan
c. memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian.</td><td>Ketua Pejabat,
Pentadbir Sistem</td></tr>
<tr><td>K06/11 Pengurusan Perkhidmatan Pihak Ketiga</td><td>Tindakan</td></tr>
<tr><td>Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.
Perkara-perkara yang mesti dipatuhi adalah seperti berikut:
a. memasukkan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat;
b. perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan
c. pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyelenggara dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.</td><td>Ketua Pejabat,
Pentadbir Sistem</td></tr>
<tr><td colspan="2">K06/12 Pemantauan</td></tr>
<tr><td>K06/12/01 Pemantauan Log</td><td>Tindakan</td></tr>
<tr><td>Ia bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, di antaranya seperti berikut:
a. log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan sekurang-kurangnya 3 bulan bagi membantu siasatan dan memantau kawalan capaian;
b. prosedur untuk memantau penggunaan kemudahan</td><td>Pentadbir Sistem</td></tr>
</table>

memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; c. kemudahan merekod dan maklumat log perlu dilindungi daripada diubah suai dan sebarang capaian yang tidak dibenarkan; d. aktiviti pentadbiran dan operator sistem perlu direkodkan; e. kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan, dianalisa dan diambil tindakan pemulihan; dan f. masa yang berkaitan dengan sistem pemprosesan maklumat dalam MetMalaysia perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	
K06/12 /02 Pengauditan dan Forensik ICT	**Tindakan**
CERT MetMalaysia mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a. sebarang percubaan pencerobohan kepada sistem ICT MetMalaysia; b. serangan kod perosak (malicious code), halangan pemberian perkhidmatan (denial of service), *spam*, pemalsuan (forgery, phising), pencerobohan (intrusion), ancaman (threat) dan kehilangan fizikal (physical loss); c. pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d. aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti Kerajaan; e. aktiviti pengwujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f. aktiviti pemasangan dan penggunaan perisian yang membebankan jalur lebar (bandwidth) rangkaian; g. aktiviti penyalahgunaan akaun emel; dan h. aktiviti penukaran alamat IP selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian. Langkah-langkah pengendalian insiden di atas adalah seperti berikut: a. CERT MetMalaysia akan menentukan prosedur pengumpulan bahan bukti (hardisk/media storan) yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan; b. proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat; dan	CERT MetMalaysia, ICTSO, Pentadbir Sistem

c. sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, format laporan khas perlu disediakan di mana semua proses dan hasil siasatan adalah SULIT.	
K06/12 /03 Jejak Audit	**Tindakan**
Setiap sistem mestilah mempunyai jejak audit untuk merekodkan aktiviti-aktiviti yang berlaku secara kronologi bagi membolehkan semakan dibuat. Jejak audit hendaklah mengandungi ciri-ciri berikut: a. rekod setiap aktiviti transaksi; b. maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; c. aktiviti akses pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan d. maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Pentadbir Sistem hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan, jika perlu. Ini dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem
K06/12/04 Log Sistem	**Tindakan**
Log sistem hendaklah disimpan untuk tempoh sekurang-kurangnya tiga bulan. Jenis log sistem bagi server dan aplikasi yang perlu diaktifkan adalah seperti berikut: a. log sistem untuk sistem pengoperasian; b. log sistem untuk aplikasi; dan c. log sistem untuk rangkaian. Pentadbir Sistem hendaklah melaksanakan perkara-perkara berikut: a. mewujudkan log sistem bagi merekodkan semua aktiviti harian pengguna; b. menyemak log sistem secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan melaksanakan tindakan pemulihan dengan segera; dan c. melaporkan kepada ICTSO sekiranya wujud aktiviti-aktiviti tidak sah, seperti kecurian maklumat dan pencerobohan.	Pentadbir Sistem

KAWALAN 07 : KAWALAN AKSES

Objektif	
Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT Jabatan.	
K07/01 Kawalan Akses	**Tindakan**
Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan akses pengguna sedia ada.	Pentadbir Sistem
K07/02 Pengurusan Akses Pengguna	
K07/02/01 Pendaftaran Pengguna	**Tindakan**
Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut: a. akaun yang diperuntukkan oleh Jabatan sahaja boleh digunakan; b. ID pengguna hendaklah unik dan mencerminkan identiti pengguna; c. pemilikan akaun bukanlah hak mutlak pengguna dan tertakluk kepada peraturan Jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; d. akaun bersama hanya boleh diwujudkan setelah mendapat kelulusan bertulis daripada Pengurus ICT dengan sokongan Ketua Pejabat; e. penggunaan akaun milik orang lain atau akaun Bahagian/Seksyen/Pejabat yang tidak dipertanggungjawabkan adalah dilarang; f. akaun Bahagian/Seksyen/Pejabat atau akaun bersama hanya dibenarkan diakses di premis MetMalaysia sahaja kecuali mendapat kelulusan bertulis daripada Pengurus ICT; dan g. Pentadbir Sistem boleh menggantung dan membatalkan akaun pengguna atas sebab-sebab berikut: i. pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua minggu kecuali dengan kebenaran;	Pengurus ICT, Ketua Pejabat, Pentadbir Sistem, Pengguna

ii. bertukar bidang tugas kerja; iii. bertukar ke agensi lain; iv. bersara; atau v. ditamatkan perkhidmatan.	
K07/02/02 Hak Akses (Access Privilege)	**Tindakan**
Penetapan dan penggunaan ke atas hak akses perlu diberi kawalan dan penyeliaan yang ketat. Keperluan akses hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak akses ini diberikan kepada pegawai dan kakitangan yang dibenarkan sahaja berdasarkan keperluan skop tugas.	Pentadbir Sistem
K07/02/03 Pengurusan Kata Laluan	**Tindakan**
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MetMalaysia seperti berikut: a. dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c. panjang kata laluan mestilah sekurang-kurangnya lapan aksara dengan gabungan antara huruf dan nombor serta aksara khusus; d. kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun melainkan kata laluan tersebut direkod dan disimpan di dalam kabinet besi berkunci; e. kata laluan *windows* dan *screen saver* hendaklah diaktifkan kecuali sistem pemonitoran yang dipantau sepanjang masa; f. kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g. penguatkuasaan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula; h. kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i. had kemasukan kata laluan bagi capaian kepada sistem	Pengguna

aplikasi adalah maksimum tiga kali sahaja kecuali pada akaun bersama yang digunakan untuk sistem pemantauan. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat; j. kata laluan akses aplikasi hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; k. sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna; dan l. Sekiranya akaun bersama diwujudkan, perkara-perkara berikut perlu dilaksanakan: i. Ketua Pejabat perlu bertanggungjawab ke atas akaun tersebut; dan ii. Pentadbir Sistem perlu mendapatkan kelulusan bertulis daripada Pengurus ICT atau Ketua Pejabat sebelum akaun diwujudkan dan pemonitoran ke atas akaun tersebut perlu dibuat.	
K07/02/04 *Clear Desk* dan *Clear Screen*	**Tindakan**
Prosedur *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat disimpan dengan teratur dan selamat bagi mengelakkan kebocoran atau kehilangan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. menggunakan kemudahan *password screen saver* atau log keluar sentiasa dilaksanakan; b. menyimpan dokumen atau media simpanan di dalam laci atau kabinet fail yang berkunci; dan c. memastikan semua dokumen terperingkat diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat untuk mengelakkan kebocoran maklumat sensitif.	Pengguna
K07/03 Akses Sistem Pengoperasian	
K07/03/01 Akses Sistem Pengoperasian	**Tindakan**
Kawalan akses sistem pengoperasian perlu bagi mengelakkan sebarang akses komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang akses ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a. mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan;	Pentadbir Sistem

b. merekodkan akses yang berjaya dan gagal; dan c. membekalkan kemudahan untuk pengesahan (bagi sistem kata laluan kunci digunakan, kualiti kata kunci perlu mendapat pengesahan). Kaedah-kaedah untuk menyokong pelaksanaan kemudahan keselamatan dalam sistem operasi adalah seperti berikut: a. mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; b. mewujudkan jejak audit ke atas semua akses sistem pengoperasian terutama pengguna bertaraf *super user*; dan c. menjana amaran (alert) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi bagi melaksanakan kawalan di atas adalah seperti berikut: a. mengawal akses ke atas sistem operasi menggunakan prosedur *log on* yang terjamin; b. mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna; c. mewujudkan sistem pengurusan kata laluan secara interaktif dan mematuhi pengurusan kata laluan; dan d. menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
K07/03/02 Kad Pintar	**Tindakan**
Penggunaan kad pintar perlu mematuhi perkara-perkara berikut: a. penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi akses sistem Kerajaan Elektronik yang dikhususkan; b. kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c. perkongsian penggunaan kad pintar adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga kali cubaan akan disekat; dan d. sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pengeluar kad.	Pentadbir Sistem, Pengguna

K07/04 Akses Aplikasi dan Maklumat	**Tindakan**
Ia bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk akses yang tidak dibenarkan dan menyebabkan kerosakan. Akses sistem dan aplikasi MetMalaysia adalah terhad kepada pengguna dan tujuan yang dibenarkan sahaja. Bagi memastikan kawalan akses sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi: a. pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap akses dan sensitiviti maklumat yang telah ditentukan; b. setiap aktiviti akses sistem maklumat dan aplikasi pengguna hendaklah direkodkan bagi mengesan aktiviti-aktiviti yang tidak diingini; c. memastikan akses maklumat dilindungi dari sebarang bentuk penyalahgunaan; d. memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau akses yang tidak sah; e. akses sistem maklumat dan aplikasi melalui jarak jauh adalah terhad kepada perkhidmatan yang dibenarkan sahaja; dan e. *session timeout* hendaklah dilaksanakan kecuali bagi sistem pemantauan.	Pentadbir Sistem, Pengguna
K07/05 Akses Jarak Jauh	**Tindakan**
Akses jarak jauh adalah akses daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan *telecommuting*. Pelaksanaan pengaksesan jarak jauh hendaklah mematuhi perkara-perkara berikut: a. penghantaran maklumat terperingkat yang menggunakan akses jarak jauh mestilah menggunakan kaedah enkripsi (encryption); b. lokasi bagi akses ke sistem ICT hendaklah dipastikan selamat; c. penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pengurus ICT. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini; d. menyediakan tempoh penggunaan mengikut kesesuaian; dan e. menghadkan masa penggunaan (connection time) rangkaian bagi pengguna.	Pengguna, Pentadbir Sistem

K07/05 /01 Kerja Jarak Jauh (Teleworking)	**Tindakan**
Sebarang aktiviti *teleworking* hendaklah mendapatkan kebenaran daripada ICTSO dan hanya menggunakan kemudahan VPN yang dibekalkan oleh Jabatan.	Pengguna
K07/05 /02 *Cloud Networking*	**Tindakan**
Sebarang aktiviti *cloud networking* adalah dilarang kecuali dengan kebenaran daripada ICTSO.	Pengguna
K07/06 Kawalan Akses Rangkaian	
K07/06/01 Akses Rangkaian	**Tindakan**
Kawalan akses perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. mewujudkan segmen rangkaian yang bersesuaian bagi membezakan di antara rangkaian MetMalaysia, rangkaian agensi kerajaan dan rangkaian awam; b. mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; c. memantau dan menguatkuasakan kawalan akses pengguna terhadap perkhidmatan rangkaian ICT; d. akses pengguna jarak jauh (remote user) perlulah dikawal; e. akses fizikal dan logikal ke atas perkakasan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal; dan f. polisi perlu diwujudkan untuk mengawal akses oleh pengguna pada semua rangkaian yang dikongsi (shared networks), terutama sekali yang keluar daripada rangkaian ICT.	Pentadbir Rangkaian
K07/06/02 Akses Internet	**Tindakan**
Akses internet hendaklah dikawal dan dipantau bagi menjamin keselamatan aset, kelancaran operasi dan mengelak penyalahgunaan kemudahan internet dengan mematuhi langkah-langkah berikut: i. penggunaan internet di MetMalaysia hendaklah dipantau secara berterusan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kawalan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian	ICTSO, Pengurus ICT, Pentadbir Rangkaian, Pengguna

MetMalaysia; ii. penggunaan internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya; iii. penggunaan *proxy* di MetMalaysia telah ditetapkan untuk mengawal akses internet dan mematuhi pekeliling semasa yang dikeluarkan; iv. pengawalan aktiviti *streaming atau* muat turun adalah perlu bagi pengurangan penggunaan *bandwidth*; v. penggunaan peranti peribadi untuk tujuan sambungan ke internet dilarang sama sekali di pejabat kecuali dengan kebenaran ICTSO; dan vi. penggunaan internet mestilah merujuk kepada Garis Panduan dan Etika Penggunaan Emel dan Internet MetMalaysia terkini.	
K07/07 Peralatan Mudah Alih	**Tindakan**
Penggunaan peralatan mudah alih perlu mematuhi perkara-perkara berikut: a. merekodkan aktiviti keluar masuk peralatan bagi mengesan pergerakan perkakasan tersebut daripada kejadian kehilangan atau pun kerosakan; b. peralatan hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan c. memastikan peralatan yang dibawa keluar dari pejabat perlu disimpan dan dijaga dengan baik bagi mengelakkan daripada kecurian.	Pemilik Aset, Pengguna

KAWALAN 08 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Objektif	
Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
K08/01 Kawalan Prosesan Aplikasi	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujud sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b) ujian keselamatan hendaklah dijalankan ke atas sistem aplikasi untuk menyemak pengesahan dan integriti data; dan c) semua sistem yang dibangunkan hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	ICTSO, Pentadbir Sistem, Pengguna
K08/01/01 Pengesahan Data *Input*	**Tindakan**
Input bagi aplikasi perlu disahkan untuk memastikan data yang dimasukkan betul dan tepat.	Pemilik Sistem, Pentadbir Sistem, Pengguna
K08/01/02 Kawalan Proses	**Tindakan**
Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa pemprosesan.	Pentadbir Sistem
K08/01/03 Pengesahan Data *Output*	**Tindakan**
Output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem, Pentadbir Sistem, Pengguna

K08/02 Kawalan Kriptografi	**Tindakan**
Melindungi kerahsiaan, integriti dan kesahihan maklumat yang merangkumi data di dalam sistem rangkaian, sistem aplikasi dan pangkalan data. Kata kunci enkripsi mestilah dilindungi menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Kata kunci mestilah dihindari daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran. Kriptografi turut merangkumi kaedah-kaedah berikut: a. Enkripsi Sistem aplikasi yang melibatkan maklumat terperingkat perlu dienkripsi. b. Tandatangan Digital Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. c. Infrastruktur Kunci Awam (Public Key Infrastructure (PKI)) Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pengguna
K08/03 Keselamatan Sistem Fail	**Tindakan**
Sistem fail dikawal dan dikendalikan melalui kaedah berikut: a. proses pengemaskinian dilakukan oleh pegawai yang bertanggungjawab dan mengikut prosedur yang telah ditetapkan; b. kod sistem atau aturcara yang dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c. mengawal akses ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d. mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; dan e. data ujian perlu dikawal dan dilindungi penggunaannya.	Pentadbir Sistem

K08/04 Keselamatan Proses Pembangunan dan Sokongan	
K08/04/01 Prosedur Perubahan	**Tindakan**
Perubahan atau pengubahsuaian ke atas sistem maklumat, sistem pengoperasian dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.	Pemilik Sistem, Pentadbir Sistem
K08/04/01 Pembangunan Secara *Outsource*	**Tindakan**
Pembangunan perisian aplikasi secara *outsource* perlu dipantau dan kod sumber (source code) adalah menjadi hak milik MetMalaysia.	Pengurus ICT, Ketua Pejabat, Pentadbir Sistem
K08/04/03 Pembocoran Maklumat	**Tindakan**
Pembocoran maklumat melalui apa cara sekalipun mestilah dihalang.	Pengguna
K08/05 Kawalan Terhadap *Vulnerability*	**Tindakan**
Kawalan terhadap *vulnerability* perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a. memperoleh maklumat *vulnerability* yang tepat pada masanya ke atas sistem maklumat yang digunakan; b. menilai tahap *vulnerability* bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c. mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem, ICTSO

KAWALAN 09 : PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

Objektif	
Semua insiden perlu dikendalikan dengan cepat, tepat dan berkesan bagi memastikan sistem ICT MetMalaysia beroperasi semula dengan baik supaya tidak menjejaskan imej MetMalaysia dan sistem penyampaian perkhidmatan.	
K09/01 Mekanisme Pelaporan Insiden Keselamatan ICT	**Tindakan**
a. Pelaporan Semua insiden keselamatan ICT mesti dilaporkan kepada ICTSO dan CERT MetMalaysia untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat insiden adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. b. CERT MetMalaysia Pasukan CERT MetMalaysia akan bertindak dan melaporkan kepada ICTSO dan Pengurus ICT seterusnya ICTSO akan memaklumkan GCERT bagi mendapatkan bantuan, jika perlu. c. Tanggungjawab Pengguna Pengguna yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan bersendirian, sebaliknya perlu melaporkan segera sebarang insiden keselamatan ICT bagi mengelakkan kerosakan bahan bukti. d. Tindakan Dalam Keadaan Berisiko Tinggi Dalam keadaan atau persekitaran berisiko tinggi, CIO hendaklah memaklumkan kepada pengurusan tertinggi 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. e. Sekiranya berlaku sesuatu keadaan yang mencurigakan seperti di bawah, insiden keselamatan ICT hendaklah dilaporkan kepada CERT MetMalaysia dengan kadar segera: i. maklumat atau data didapati atau disyaki hilang atau didedahkan kepada pihak yang tidak diberi kuasa; ii. sistem maklumat digunakan tanpa kebenaran atau yang disyaki sedemikian; iii. kata laluan atau mekanisme kawalan akses yang hilang, dicuri, didedahkan atau yang disyaki sedemikian; iv. berlaku kejadian sistem yang luar biasa seperti kehilangan	CIO, ICTSO, Pengguna, CERT MetMalaysia

fail, sistem kerap kali gagal berfungsi atau dicapai, dan komunikasi tersalah hantar; dan v. berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka yang boleh menjejaskan keselamatan ICT. f. ICTSO melaporkan kepada Pasukan Tindak Balas Insiden Keselamatan ICT (GCERT) apabila berlaku sebarang insiden keselamatan ICT.	
K09/02 Prosedur Pengendalian Insiden Keselamatan ICT	**Tindakan**
Pasukan CERT MetMalaysia perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur pengurusan pelaporan dan pengendalian insiden keselamatan ICT MetMalaysia. Pengendalian insiden keselamatan ICT perlu diuruskan dengan cepat, teratur dan berkesan, mengikut prosedur dengan mengambil kira kawalan-kawalan berikut: i. mengenal pasti semua jenis insiden; ii. mematuhi DRP seperti yang telah digariskan dalam PKP; iii. menyimpan jejak audit dan memelihara bahan bukti dan rekod; iv. menyediakan tindakan pencegahan dan pengukuhan supaya insiden serupa tidak berulang; dan v. memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	CIO, ICTSO, CERT MetMalaysia

KAWALAN 10 : PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Objektif	
Menjamin operasi perkhidmatan dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
K10/01 Pengurusan Kesinambungan Perkhidmatan (PKP)	**Tindakan**
Pengurusan Kesinambungan Perkhidmatan (PKP) adalah mekanisme bagi mengurus dan memastikan kepentingan *stakeholder* sistem penyampaian perkhidmatan dilindungi dan imej MetMalaysia terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan MetMalaysia di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan. Ketua Jabatan adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT MetMalaysia. Pelan PKP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: a. senarai aktiviti teras yang kritikal mengikut susunan keutamaan; b. senarai kakitangan MetMalaysia dan pihak ketiga berserta maklumat perhubungan (faksimili, telefon dan emel). Senarai pegawai simpanan hendaklah disediakan sebagai pelapis kepada pegawai yang tidak dapat hadir untuk menangani insiden; c. senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; d. alternatif sumber pemprosesan, dan lokasi, untuk menggantikan sumber yang telah lumpuh; dan e. perjanjian dengan pihak ketiga perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan. Salinan pelan PKP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. 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	KP, Pengurus ICT

bersesuaian dan memenuhi tujuan ia diwujudkan. Ujian pelan PKP hendaklah berjadual untuk memastikan semua ahli dan pegawai yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan masing-masing apabila pelan dilaksanakan. MetMalaysia hendaklah memastikan pelan PKP dikemas kini dan dilindungi.	
K10/02 Pelan Kesinambungan Perkhidmatan	Tindakan
Pelan Kesinambungan Perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh Pengurusan Tertinggi MetMalaysia dan perkara-perkara berikut perlulah diberi perhatian: a) mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b) melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; c) mendokumentasikan proses dan prosedur; d) mengenal pasti insiden/bencana yang boleh mengakibatkan gangguan yang berkemungkinan memberi impak terhadap perkhidmatan jabatan; e) mengadakan program latihan kepada pengguna mengenai prosedur Pelan Kesinambungan Perkhidmatan; f) memastikan *backup* sedia ada dapat *restore* seperti sediakala; dan g) menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.	Pasukan Koordinator PKP, Ketua DRT, Ketua ERT dan Ketua CCT

KAWALAN 11 : PEMATUHAN

Objektif	
Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran DKICT MetMalaysia.	
K11/01 Pematuhan Dasar	**Tindakan**
Setiap pengguna di MetMalaysia hendaklah membaca, memahami dan mematuhi DKICT MetMalaysia dan undang-undang atau peraturan/arahan berkaitan yang sedang berkuat kuasa. Semua aset ICT di MetMalaysia termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Pengarah berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Pengguna
K11/02 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	**Tindakan**
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 standard pelaksanaan keselamatan ICT. Sebarang penilaian pematuhan teknikal seperti aktiviti *Security Posture Assessment* (SPA) mestilah dijalankan oleh individu yang kompeten dan dibenarkan.	ICTSO
K11/03 Pematuhan Kepada Keperluan Audit	**Tindakan**
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 sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	ICTSO

K11/04 Keperluan Perundangan	Tindakan
Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MetMalaysia; 1. Arahan Keselamatan; 2. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan; 3. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002; 4. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); 5. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan; 6. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; 7. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; 8. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006; 9. Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan (TPA)"; 10. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender; 11. Surat Pekeliling Perbendaharaan Bil. 3/1995 bertajuk “Peraturan Perolehan Perkhidmatan Perundingan”; 12. Akta Tandatangan Digital 1997; 13. Akta Rahsia Rasmi 1972; 14. Akta Jenayah Komputer 1997; 15. Akta Hak Cipta (Pindaan) Tahun 1997; 16. Akta Komunikasi dan Multimedia 1998; 17. Perintah-Perintah Am; 18. Arahan Perbendaharaan; 19. Arahan Teknologi Maklumat 2007; 20. Surat Akujanji; 21. Manual Prosedur Kerja; 22. Fail Meja Kakitangan; 23. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam; 24. Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertajuk ”Penggunaan Media Jaringan Sosial di Sektor Awam”; 25. Surat Arahan MAMPU.702-1/1/7 Jld. 3 (48) bertajuk	Pengguna

”Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan”; 26. Garis Panduan Dan Etika Penggunaan EMel dan Internet Jabatan Meteorologi Malaysia; 27. Surat Pekeliling Perbendaharaan Bil. 3 Tahun 2013 - Garis Panduan Mengenai Pengurusan Perolehan ICT Kerajaan; 28. MS ISO/IEC 27001; 29. Pekeliling Perkhidmatan Bil 5 2007 bertajuk "Panduan Pengurusan Pejabat"; dan 30. Surat Arahan Ketua Pengarah Perkhidmatan Awam bertarikh 7 Jun 2014 - Tanggungjawab Pegawai Awam dalam Memelihara Intergriti Perkhidmatan Awam Semasa Menggunakan Kemudahan Media Sosial Di Internet	
K11/05 Pelanggaran Perundangan	**Tindakan**
Pelanggaran DKICT MetMalaysia boleh dikenakan tindakan disiplin dan tatatertib berdasarkan kepada peraturan dan Pekeliling Kerajaan sedia ada.	Pengguna

GLOSARI	
Aset ICT	Peralatan ICT termasuk komputer, media storan, *server, router, firewall*, rangkaian dan lain-lain.
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM dan *thumb drive* untuk sebarang kemungkinan adanya virus
Backup	Proses penduaan sesuatu dokumen atau maklumat
Bandwidth	Jalur lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
BKM	Bahagian Komunikasi Meteorologi
CIA^3	*confidentiality, integrity, authenticity, accessibility, accountability*
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
CERT	*Computer Emergency Response Team*
Denial of service	Halangan pemberian perkhidmatan.
Dokumen	Semua himpunan atau kumpulan bahan atau dokumen yang disimpan dalam bentuk media cetak, salinan lembut (soft copy), elektronik, dalam talian, kertas lutsinar, risalah atau *slaid*.
DK	Data dan Keselamatan ICT
DKICT	Dasar Keselamatan ICT jabatan.
DRC	*Disaster Recovery Center*
DRT	Pasukan Pemulihan Bencana (Disaster Recovery Team)
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya
Forgery	Pemalsuan dan penyamaran sistem yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian sistem, pencurian maklumat (information theft/espionage), penipuan (hoaxes).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Hardisk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (hub) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu

	port kepada semua *port* yang lain.
Insiden	Musibah (adverse event) yang berlaku ke atas sistem aplikasi dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan System komputer
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau sistem lain.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan sistem yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
Infrastruktur Kunci Awam (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Kawasan larangan	Kawasan yang dihadkan kemasukan oleh pegawai-pegawai yang tertentu sahaja atau kawasan-kawasan premis atau sebahagian daripada premis di mana perkara-perkara terperingkat disimpan atau diuruskan atau di mana kerja terperingkat dijalankan.
Ketua Pejabat	KP, TKP, Pengarah Kanan, Pengarah, Ketua Seksyen, Ketua Unit dan Penyelia Pejabat.
KM	Komunikasi Meteorologi
KP	Ketua Pengarah
KPP	Ketua Penolong Pengarah
Maklumat Terperingkat	Dokumen/Maklumat Rasmi yang dikategorikan sebagai Rahsia Besar, Rahsia, Sulit dan Terhad.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia termasuklah serangan virus, *Trojan horse, worm dan spyware.*
Malware	Merujuk kepada *virus, worms, spyware, adware, trojan horses, bots* dan kod-kod lain.
Media storan	Perkakasan yang berkaitan dengan penyimpanan data dan maklumat seperti disket, kartrij, cakera padat, cakera mudah alih, pita, cakera keras dan pemacu pena.

Modem	Modulator DEModulator. Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari sistem.
MP	Multimedia dan Pembangunan
MPK	Manual Prosedur Kerja
MyGSOCS	Malaysia Government Security Operation Centre. Berfungsi sebagai IDS/IPS di MetMalaysia.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Penggodam	Penceroboh sistem komputer dengan melakukan aktiviti seperti pencurian maklumat, pengubahsuai laman web, penyebaran virus dan penyesakkan rangkaian yang merosakkan komputer.
Pengguna	Kakitangan MetMalaysia dan pihak ketiga yang menggunakan aset ICT
Pengurusan Tertinggi MetMalaysia	Ketua Pengarah, Timbalan Ketua Pengarah
Pengurusan MetMalaysia	Pengurusan tertinggi, Pengarah Kanan dan Pengarah
Pemilik Sistem	Pemilik kepada sistem yang dibangunkan dan sistem yang sedang beroperasi
Peralatan Mudah Alih	Sebarang alat mudah alih yang dilengkapi sekurang kurangnya dua ciri asas komunikasi iaitu menerima atau membuat panggilan dan sistem pesanan ringkas
Perisian aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau Jabatan.
PKP	Pengurusan Kesinambungan Perkhidmatan
Pihak Ketiga	Pihak yang membekalkan perkhidmatan kepada Jabatan seperti pembekal, kontraktor, perunding dan lain-lain.
P(KM)	Pengarah Bahagian Komunikasi Meteorologi
PPK(KM)	Penolong Pengarah Kanan Bahagian Komunikasi Meteorologi
RN	Rangkaian
RAKKSSA	Rangka Kerja Keselamatan Siber Sektor Awam
Rahsia	Dokumen, maklumat dan bahan rasmi jika didedahkan tanpa kebenaran akan membahayakan keselamatan Negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan kepada sesebuah kuasa asing.
Rahsia Besar	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.

Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Sulit	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.
SPA	Penilaian tahap keselamatan sistem rangkaian dan sistem ICT (Security Posture Assessment*)*
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Terhad	Dokumen, maklumat dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu emel dan surat yang bermotif personal dan atas sebab tertentu.
TKP	Timbalan Ketua Pengarah
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

SENARAI LAMPIRAN	
1.	Garis Panduan Dan Etika Penggunaan Emel dan Internet MetMalaysia.
2.	Surat Akuan Pematuhan Dasar Keselamatan ICT MetMalaysia.

Garis Panduan Dan Etika Penggunaan EMel dan Internet
Jabatan Meteorologi Malaysia

1.0 Tujuan

Etika ini adalah bertujuan bagi memastikan penggunaan internet dan emel jabatan yang teratur dan terkawal oleh warganya. Ianya berpandukan **Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bil 1 Tahun 2003 iaitu Garispanduan Panduan Mengenai Tatacara Pengunaan Internet Dan mel Elektronik Di Agensi-agensi Kerajaan**.

Etika ini merupakan maklumat tambahan kepada PKPA tersebut dan bagi memenuhi keperluan persekitaran khusus bagi pengguna internet dan emel di Jabatan Meteorologi Malaysia (MetMalaysia) dengan mengambil kira keperluan teknologi semasa yang telah berubah serta ancaman keselamatan ICT terkini yang bersangkutan dengan internet dan komunikasi emel serta Arahan Pegawai Pengawal.

2.0 Latarbelakang

Penggunaan emel dan internet yang semakin meningkat, digabungkan dengan teknologi yang terkini serta pengurangan masa dan kos komunikasi telah mewujudkan satu dimensi baru dalam era perkhidmatan awam terutamanya dalam memberi perkhidmatan kepada para pelanggan. Walau bagaimanapun, penggunaan yang tidak terkawal akan membawa kepada kesan negatif yang akan memudaratkan bukan sahaja kepada jabatan bahkan kepada masyarakat dan negara.

Para pengguna di MetMalaysia menggunakan emel dan internet dalam operasi harian sebagai salah satu medium untuk berkomunikasi dengan pihak luar terdiri dari agensi kerajaan, swasta, para pelajar, pesara, penjawat awam dan lain-lain. Antaranya ialah bagi penghantaran data meteorologi, ramalan dan amaran cuaca, perkhidmatan pelanggan seperti aduan dan pertanyaan, sistem HRMIS dan GOE-EGDMS, perkhidmatan *helpdesk* dan bagi mencari sebarang maklumat di internet. Di samping itu emel juga digunakan bagi berkomunikasi di antara pengguna di dalam persekitaran jabatan sendiri bagi memudahkan pengagihan maklumat atau dokumen dalam format elektronik seperti laporan, kertas kerja, minit mesyuarat dan lain-lain.

3.0 Etika Penggunaan Emel

Tatacara penggunaan emel bertujuan untuk memberikan panduan dan tatacara penggunaan emel kepada semua pengguna emel dalam melaksanakan tugas-tugas harian bagi **meningkatkan tahap keselamatan** dan **memberi perlindungan keselamatan dokumen rasmi kerajaan**. Tatacara ini juga menjelaskan **tanggungjawab pengguna** untuk menggunakan kemudahan emel dengan betul, cekap, berkesan, beretika dan berbudi bahasa sepanjang masa.

3.1 Penggunaan emel yang baik

a. Memastikan penghantaran emel rasmi menggunakan akaun emel rasmi dan alamat emel penerima yang betul;

b. Segala urusan rasmi adalah dilarang menggunakan alamat emel persendirian seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya;

c. Mengutamakan penggunaan emel sebagai media komunikasi untuk urusan dalaman agensi atau dengan pelanggan luar;

d. Memastikan sebarang mesej yang dihantar melalui emel tidak lagi disusuli menerusi media lain seperti faks dan surat;

e. Membalas emel rasmi yang diterima dengan kadar segera selewat-lewatnya 1 hari dari tarikh emel berkenaan diterima;

f. Elakkan penghantaran emel berserta fail kepilan yang bersaiz melebihi 10 megabait;

g. Mengurus dan menyelenggarakan mailbox akaun emel masing-masing. Kemudahan archive boleh digunakan untuk menyimpan emel lama yang mempunyai nilai rasmi;

h. Tidak menggunakan emel rasmi bagi tujuan peribadi;

i. Memastikan alamat emel terkini dipamerkan dalam direktori pegawai di laman web agensi;

j. Menghapuskan sebarang emel berunsurkan emel spam yang berkemungkinan mempunyai virus;

k. Memastikan setiap emel mempunyai tajuk yang sesuai dengan kandungan emel;

l. Menulis jawapan di bahagian atas mesej emel penghantar;

m. Menggunakan bahasa dan ayat yang jelas, tepat dan mudah difahami oleh penerima;

n. Menggunakan bahasa formal di dalam emel rasmi;

o. Menggunakan kemudahan ‘Reply’ untuk menjawab emel tanpa sebarang perubahan kandungan asal emel;

p. Memastikan kemudahan ‘Reply To All’ digunakan jika jawapan perlu disalinkan kepada semua penerima emel;

q. Tidak menggunakan kemudahan 'Auto-Reply' kecuali untuk memaklumkan pegawai lain yang boleh dihubungi sekiranya pegawai berkenaan berada di luar pejabat yang tiada kemudahan internet;

r. Menggunakan kemudahan ‘Forward’ untuk memanjangkan emel kepada penerima lain tanpa sebarang perubahan;

s. Memastikan kemudahan ‘salinan kepada’ (cc) jika sesuatu emel perlu dimaklumkan kepada penerima yang berkaitan sahaja;

t. Kemudahan ‘blind cc’ (bcc) digunakan bagi tujuan khusus dan terkawal (bukan sewenang-wenangnya);

u. Semua akaun emel di dalam sistem emel jabatan adalah hakmilik jabatan dan bukannya individu serta jabatan mempunyai hak untuk mengawasi dan memantau sebarang penggunaan akaun emel.

v. Semua pengguna baru diwajibkan mengisi borang permohonan emel dan perlu mendapat sokongan dari Ketua Bahagian/Seksyen masing-masing.

w. Pengguna bertanggungjawab bagi memaklumkan kepada pentadbir emel sekiranya bercuti panjang atau berkursus panjang atau akan bertukar keluar dari MetMalaysia.

x. Emel jabatan tidak boleh disalahgunakan bagi penyebaran atau memperolehi sebarang bahan berunsur fitnah, seks, perkauman dan lain-lain yang menyalahi undang-undang.

y. Pengguna tidak dibenarkan mendaftar ke *yahoo groups, google groups* dan kumpulan emel yang lain.

3.2 Pengurusan Emel yang baik

a. Pengurusan kandungan dan penyenggaraan kotak mel pada komputer masing-masing adalah menjadi tanggungjawab pengguna sendiri.

b. Periksa *mailbox* anda sekurang-kurangnya sekali sehari kecuali atas sebab-sebab yang dibenarkan atau tidak dapat dielakkan.

c. Baca semua mesej emel baru dan berilah perhatian kepada *priority* (keutamaan) mesej yang dilabelkan (sekiranya ada) oleh pengirim mesej tersebut.

d. Membalas mesej secepat mungkin terutamanya yang melibatkan para pelanggan jabatan (seperti pelajar, pesara, penjawat awam, agensi awam dan swasta) serta membuat anggaran untuk membalas mesej dalam waktu yang sepatutnya.

e. Jangan biarkan mesej bertambah di dalam *folder inbox* anda. Anda mungkin terlepas pandang mesej yang lebih utama yang tersorok di antara yang lama ataupun mesej-mesej yang sudahpun dibaca. Sebaiknya buatlah folder-folder berasingan yang khusus dan bersesuaian serta memindahkan mesej-mesej tersebut ke folder berkenaan untuk rujukan di masa depan.

f. Mesej-mesej yang tidak diperlukan hendaklah dihapuskan terutamanya yang mempunyai lampiran di mana ini dapat menjimatkan ruang storan di komputer anda.

g. Memadamkan mesej yang tidak berkaitan sebaik sahaja anda menerimanya terutamanya *spam* dan emel bervirus.

h. Membuka *folder Sent Items* sekurang-kurangnya sekali seminggu dan memadamkan salinan mesej-mesej lama yang telah berjaya dikirim sekiranya tidak lagi diperlukan.

i. Sentiasa memastikan buku alamat anda dikemaskini.

3.3 Keselamatan emel

a. Lindungi sebarang maklumat terperingkat (rahsia, sulit, terhad dan sensitif) yang dihantar melalui emel. Antara kaedahnya ialah dengan menggunakan teknik penyulitan (*encription*) atau katalaluan.

b. Simpan salinan mesej yang penting terutamanya lampiran.

c. Jangan menghantar emel kepada seseorang dengan mengunakan akaun penguna dan katalaluan orang lain melalui apa cara sekalipun.

d. Anda adalah dilarang menggunakan cara-cara tertentu untuk menyamar sebagai penghantar emel yang sah.

e. Simpan katalaluan secara sulit dan hendaklah diubah dari semasa ke semasa melalui penggunaan sistem web mel.

f. Anda hendaklah sentiasa mengimbas fail dalam kotak mel dengan perisian antivirus. Berwaspadalah kerana emel adalah cara paling mudah untuk menghantar virus dari sebuah komputer ke computer yang lain. Anda juga hendaklah mempastikan fail yang akan dihantar melalui lampiran (*attachment*) bebas dari virus.

g. Emel rasmi jabatan **tidak boleh didaftarkan** dalam senarai emel (*yahoo groups, google groups)*, kumpulan perbincangan, muat turun, pendaftaran di internet yang menyebabkan anda menerima sejumlah emel berbentuk komersil, porno dan lain-lain.

h. Hubungilah *mmd@met.gov.my* dengan segera jika anda mengesan atau mengesyaki alamat emel anda telah disalahgunakan.

4.0 Etika Penggunaan Internet

MetMalaysia amat menggalakkan penggunaan Internet dalam kakitangan sebagai medium komunikasi secara elektronik untuk **tujuan perkongsian maklumat dan pengetahuan, meningkatkan produktiviti dan kualiti perkhidmatan dan seterusnya mendukung misi dan visi MetMalaysia**.

Antara perkara yang perlu dipatuhi bagi menjamin kesahihan, keutuhan dan kebolehcapaian maklumat yang berterusan adalah:

a. Hak Akses Pengguna

Hak akses hendaklah dilihat sebagai satu kemudahan yang disediakan oleh agensi untuk membantu melicinkan pentadbiran atau memperbaiki perkhidmatan yang disediakan.

Pengguna harus mengambil maklum bahawa semua aset ICT di bawah kawalannya (termasuk maklumat) adalah hak milik Kerajaan.

b. **Memilih Laman**

Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan.

c. **Pengesahan Maklumat**

Bahan yang diperolehi dari Internet perlulah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah juga dinyatakan

d. **Muat Naik Bahan**

Bahan rasmi yang hendak dimuat naik ke Internet hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik

e. **Muat Turun Bahan**

Tindakan memuat turun hanya dibenarkan ke atas bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh jabatan sahaja

f. **Perbincangan Awam**

Hanya pegawai yang mendapat kebenaran sahaja boleh melibatkan diri dan menggunakan kemudahan ini. Kandungan perbincangan awam seperti newsgroup dan bulletin board mestilah mendapat pengesahan daripada Ketua Jabatan tertakluk kepada dasar dan tatacara yang telah ditetapkan. Perlu diingat bahawa setiap maklumat yang dikongsi melambangkan imej Kerajaan. Dengan sebab itu, setiap pengguna mestilah bertindak dengan bijaksana, jelas dan berupaya mengekalkan konsistensi dan keutuhan maklumat berkenaan

g. Pengguna adalah **dilarang** daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan Internet seperti:

i. memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen;

ii. menyedia dan menghantar maklumat berulang-ulang berupa gangguan;

iii. menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan, imej atau bahan-bahan yang mengandungi unsur-unsur lucah;

iv. menyedia, memuat naik, memuat turun dan menyimpan maklumat Internet yang melibatkan sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej Kerajaan;

v. menyalahgunakan kemudahan perbincangan awam atas talian seperti newsgroup dan bulletin board;

vi. memuat naik, memuat turun dan menyimpan gambar atau teks yang bercorak penentangan yang boleh membawa keadaan huru-hara dan menakutkan pengguna Internet yang lain;

vii. memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan atas talian seperti permainan elektronik, video dan lagu;

viii. menggunakan kemudahan chatting melalui Internet;

ix. menggunakan kemudahan Internet untuk tujuan peribadi;

x. menjalankan aktiviti-aktiviti komersial dan politik;

xi. melakukan aktiviti jenayah seperti menyebarkan bahan yang membabitkan perjudian, senjata dan aktiviti pengganas;

xii. memuat naik, memuat turun, menghantar dan menyimpan kad elektronik, video, lagu dan kepilan fail melebihi saiz 2 megabait yang boleh mengakibatkan kelembapan perkhidmatan dan operasi sistem rangkaian komputer; dan

xiii. menggunakan kemudahan modem peribadi untuk membuat capaian terus ke Internet.

h. Memastikan sebarang bahan yang dimuat turun dari internet mestilah bebas daripada kod perosak (virus, worm, Trojan horse dan trap door);

i. Pilihlah masa yang sesuai untuk memindahkan fail. Fail yang bersaiz besar (yang melebihi 1MB) wajar dipindahkan di luar waktu beban puncak.

5.0 Pemakaian

5.1 Penyalah gunaan sumber internet dan sistem emel jabatan dianggap sebagai salah laku yang membolehkan tindakan tatatertib diambil ke atas individu yang melakukan kesalahan.

5.2 Jabatan mempunyai hak untuk menarik balik atau mengantung sebarang akaun emel dan akses internet pengguna yang dikesan atau dipercayai telah disalahgunakan pada bila-bila masa.

5.3 Semua penggunaan emel dan internet MetMalaysia adalah tertakluk kepada Etika Penggunaan Internet dan Emel Jabatan.

5.4 Etika ini mesti dipatuhi sepenuhnya oleh semua peringkat pengguna internet dan emel di MetMalaysia pada sepanjang masa.

Operasi Data & Keselamatan ICT
Bahagian Komunikasi Meteorologi
Jabatan Meteorologi Malaysia

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI

METMalaysia

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT METMALAYSIA VERSI TERKINI

Nama (Huruf Besar) : ____

No. Kad Pengenalan : ____

Jawatan : ____

Bahagian/Jabatan : ____

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT MetMalaysia Versi Terkini; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

....
( ) Tarikh

Pengesahan Pegawai Keselamatan ICT

....
( ) Tarikh
b.p Ketua Pengarah
Jabatan Meteorologi Malaysia

** Dasar Keselamatan ICT boleh diperolehi di laman web MetMalaysia