POLISI KESELAMATAN SIBER

MAHKAMAH SYARIAH WILAYAH PERSEKUTUAN (MSWP)

VERSI 1.0

KANDUNGAN

			HALAMAN
1.	**SEJARAH POLISI KESELAMATAN SIBER MSWP**		1
2.	**TUJUAN**		2
3.	**LATAR BELAKANG**		2
4.	**OBJEKTIF**		2
5.	**PERNYATAAN POLISI**		3
6.	**SKOP**		4
7.	**PRINSIP-PRINSIP**		6
8.	**PENILAIAN RISIKO KESELAMATAN ICT**		7
9.	**PELAN PENGURUSAN KESELAMATAN MAKLUMAT**		9
10.	**KAWALAN-KAWALAN:**		
PKSMSWP - K01 -	**POLISI KESELAMATAN MAKLUMAT**		
	Objektif		12
	PKSMSWP - K01/01	**Pelaksanaan Polisi**	12
	PKSMSWP - K01/02	**Penyebaran Polisi**	12
	PKSMSWP - K01/03	**Penyelenggaraan Polisi**	12
	PKSMSWP - K01/04	**Pematuhan Polisi**	13
PKSMSWP - K02 -	**ORGANISASI KESELAMATAN MAKLUMAT**		
	Objektif		15
	PKSMSWP - K02/01	**Tadbir Urus Keselamatan Maklumat**	15
	PKSMSWP - K02/01/01	Ketua Hakim Syarie (KHS)	15
	PKSMSWP - K02/01/02	Ketua Pegawai Digital (CDO)	15
	PKSMSWP - K02/01/03	Pegawai Keselamatan ICT (ICTSO)	16
	PKSMSWP - K02/01/04	Pentadbir Sistem	18
		Pentadbir Rangkaian dan Keselamatan	18
		Pentadbir Pangkalan Data	19
		Pentadbir Portal / Laman Web	20
		Pentadbir Pusat Data	21
		Pentadbir Sistem Aplikasi	22
		Pentadbir E-mel	23
		Pentadbir Media Sosial dan Aplikasi Sosial MSWP	24
		Pegawai Aset ICT	25
	PKSMSWP - K02/01/05	Pengguna	26

	PKSMSWP - K02/01/06	Jawatankuasa Keselamatan ICT	28
	PKSMSWP - K02/01/07	Pasukan Tindak Balas Insiden Keselamatan ICT (CERTMSWP)	29
	PKSMSWP - K02/02	**Pihak Luar**	30
	PKSMSWP - K02/02/01	Keperluan Keselamatan Dalam Perkhidmatan ICT	30
PKSMSWP - K03 -	**KESELAMATAN SUMBER MANUSIA**		
	Objektif		32
	PKSMSWP - K03/01	**Sebelum Perkhidmatan**	32
	PKSMSWP - K03/02	**Semasa Perkhidmatan**	33
	PKSMSWP - K03/03	**Bertukar Atau Tamat Perkhidmatan**	34
PKSMSWP - K04 -	**PENGURUSAN ASET**		
	Objektif		36
	PKSMSWP - K04/01	**Akauntabiliti Aset ICT**	36
	PKSMSWP - K04/02	**Peminjaman dan Pemulangan Aset ICT**	37
	PKSMSWP - K04/03	**Pengelasan Maklumat**	38
	PKSMSWP - K04/04	**Pengendalian Maklumat**	38
	PKSMSWP - K04/05	**Pengelasan dan Pengendalian Data Terbuka**	39
	PKSMSWP - K04/06	**Pengendalian Media**	39
	PKSMSWP - K04/06/01	Media Storan	39
PKSMSWP - K05 -	**KAWALAN CAPAIAN**		
	Objektif		42
	PKSMSWP - K05/01	**Kawalan Capaian**	42
	PKSMSWP - K05/02	**Pengurusan Capaian Pengguna**	42
	PKSMSWP - K05/02/01	Pendaftaran Pengguna	42
	PKSMSWP - K05/02/02	Hak Capaian	43
	PKSMSWP - K05/02/03	Pengurusan Kata Laluan	43
	PKSMSWP - K05/03	**Capaian Sistem Pengoperasian**	44
	PKSMSWP - K05/03/01	Capaian Sistem Pengoperasian	44
	PKSMSWP - K05/03/02	Token/ Sijil Digital	46
	PKSMSWP - K05/04	**Capaian Aplikasi dan Maklumat**	46
	PKSMSWP - K05/05	**Capaian Jarak Jauh**	47
	PKSMSWP - K05/06	**Kawalan Capaian Rangkaian**	48
	PKSMSWP - K05/07	**Peralatan Mudah Alih**	49
	PKSMSWP - K05/08	***Bring Your Own Device* (BYOD)**	49
	PKSMSWP – K05/09	**Telekerja**	50
PKSMSWP - K06	**KAWALAN KRIPTOGRAFI**		

	Objektif		53
	PKSMSWP - K06/01	**Kriptografi**	53
PKSMSWP - K07	**KESELAMATAN FIZIKAL DAN PERSEKITARAN**		
	Objektif		55
	PKSMSWP - K07/01	**Keselamatan Kawasan**	55
	PKSMSWP - K07/01/01	Kawasan Larangan ICT	55
	PKSMSWP - K07/01/02	Kawalan Masuk Fizikal	56
	PKSMSWP - K07/02	**Keselamatan Peralatan**	57
	PKSMSWP - K07/02/01	Peralatan ICT	57
	PKSMSWP - K07/02/02	*Clear Desk* dan *Clear Screen*	58
	PKSMSWP - K07/02/03	Media Tandatangan Digital	59
	PKSMSWP - K07/02/04	Perisian dan Aplikasi	59
	PKSMSWP - K07/02/05	Perkakasan Tanpa Penyeliaan	60
	PKSMSWP - K07/02/06	Peralatan di Luar Premis	60
	PKSMSWP - K07/02/07	Pelupusan	61
	PKSMSWP - K07/02/08	Penyelenggaraan	62
	PKSMSWP - K07/03	**Kawalan Persekitaran**	62
	PKSMSWP - K07/03/01	Kawalan Persekitaran	62
	PKSMSWP - K07/03/02	Kabel Rangkaian	63
	PKSMSWP - K07/03/03	Bekalan Kuasa	64
	PKSMSWP - K07/03/04	Prosedur Kecemasan	64
	PKSMSWP - K07/03/05	Mekanisme Pelaporan Insiden Bukan ICT	64
	PKSMSWP - K07/03/06	Mekanisme Kawalan Peralatan Sewaan/Ujicuba *(Proof Of Concept)*	65
	PKSMSWP - K07/04	**Keselamatan Sistem Dokumentasi**	65
PKSMSWP - K08 -	**KESELAMATAN OPERASI**		
	Objektif		68
	PKSMSWP - K08/01	**Prosedur Operasi**	68
	PKSMSWP - K08/01/01	Pengendalian Dokumen Prosedur Operasi	68
	PKSMSWP - K08/01/02	Pengurusan Perubahan	68
	PKSMSWP - K08/01/03	Pengasingan Tugas dan Tanggungjawab	69
	PKSMSWP - K08/02	**Perancangan dan Penerimaan Sistem**	70
	PKSMSWP - K08/02/01	Perancangan Kapasiti	70
	PKSMSWP - K08/02/02	Penerimaan Sistem	70
	PKSMSWP - K08/03	**Perlindungan dari Perisian Berbahaya**	70
	PKSMSWP - K08/03/01	Perlindungan dari Perisian Berbahaya	70
	PKSMSWP - K08/03/02	Perlindungan dari *Mobile Code*	71
	PKSMSWP - K08/04	***Housekeeping***	71

	PKSMSWP - K08/04/01	*Backup*	71
	PKSMSWP - K08/05	**Pengurusan Media**	72
	PKSMSWP - K08/05/01	Media Storan Mudah Alih	72
	PKSMSWP - K08/05/02	Prosedur Pengendalian Media	72
	PKSMSWP - K08/06	**Paparan Maklumat Umum**	73
	PKSMSWP - K08/07	**Pemantauan**	73
	PKSMSWP - K08/07/01	Pemantauan	73
	PKSMSWP - K08/07/02	Pengauditan dan Forensik ICT	74
	PKSMSWP - K08/07/03	Jejak Audit	75
	PKSMSWP - K08/07/04	Sistem Log	76
PKSMSWP - K09 -	**KESELAMATAN KOMUNIKASI**		
	Objektif		78
	PKSMSWP - K09/01	**Pengurusan Rangkaian**	78
	PKSMSWP - K09/02	**Pengurusan Penghantaran dan Penerimaan Maklumat**	79
	PKSMSWP - K09/03	**Pengurusan Mel Elektronik (E-mel)**	79
	PKSMSWP - K09/04	**Pengurusan Sidang Video**	80
PKSMSWP - K10	**PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM**		
	Objektif		85
	PKSMSWP - K10/01	**Kawalan Prosesan Aplikasi**	85
	PKSMSWP - K10/01/01	Pengesahan Data *Input*	85
	PKSMSWP – K10/01/02	Kawalan Proses	85
	PKSMSWP – K10/01/03	Pengesahan Data *Output*	86
	PKSMSWP - K10/02	**Keselamatan Fail Sistem**	86
	PKSMSWP - K10/03	**Keselamatan Dalam Proses Pembangunan Dan Sokongan**	86
	PKSMSWP - K10/03/01	Peraturan Keselamatan Dalam Pembangunan Sistem	86
	PKSMSWP - K10/03/02	Prosedur Perubahan	87
	PKSMSWP - K10/03/03	Semakan Teknikal Aplikasi Selepas Perubahan Platform	87
	PKSMSWP - K10/03/04	Kawalan Terhadap Perubahan Kepada Perisian	87
	PKSMSWP - K10/03/05	Prinsip Kejuruteraan Sistem Yang Selamat	87
	PKSMSWP - K10/03/06	Persekitaran Pembangunan Sistem Yang Selamat	87
	PKSMSWP - K10/03/07	Pembangunan Sistem Secara Luar *(Outsource)*	88
	PKSMSWP - K10/03/08	Ujian Keselamatan Sistem	88
	PKSMSWP - K10/03/09	Pembocoran Maklumat	88
	PKSMSWP - K10/04	**Data Ujian**	89

	PKSMSWP - K10/05	**Kawalan Terhadap Keterdedahan Teknikal**	89
	PKSMSWP - K10/06	**Perkhidmatan E-Dagang**	89
	PKSMSWP - K10/07	**Pembangunan Aplikasi Mudah Alih**	90
	PKSMSWP - K10/07/01	Prosedur Integrasi Pembangunan Aplikasi Mudah Alih	90
PKSMSWP - K11 -	**HUBUNGAN PEMBEKAL**		
	Objektif		92
	PKSMSWP - K11/01	**Keselamatan Maklumat Dalam Hubungan Dengan Pembekal**	92
	PKSMSWP - K11/02	**Pengurusan Penyampaian Perkhidmatan Pembekal**	93
PKSMSWP - K12 -	**RISIKO DAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN**		
	Objektif		96
	PKSMSWP - K12/01	**Mekanisme Pelaporan Insiden Keselamatan ICT**	96
	PKSMSWP - K12/02	**Prosedur Pengurusan dan Pengendalian Insiden Keselamatan ICT**	97
PKSMSWP - K13 -	**KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN**		
	Objektif		101
	PKSMSWP - K13/01	**Pengurusan Kesinambungan Perkhidmatan**	101
	PKSMSWP - K13/01/01	Pelan Pemulihan Bencana	102
	PKSMSWP - K13/02	***Redundancy***	102
PKSMSWP - K14 -	**PEMATUHAN**		
	Objektif		105
	PKSMSWP - K14/01	**Pematuhan Polisi**	105
	PKSMSWP - K14/02	**Pematuhan kepada Polisi, Peraturan dan Penilaian Teknikal Keselamatan**	106
	PKSMSWP - K14/03	**Pematuhan Keperluan Audit**	106
	PKSMSWP - K14/04	**Pelanggaran Perundangan**	106
11.	**GLOSARI**		107

12. SENARAI LAMPIRAN

Lampiran 1	Surat Akuan Pematuhan Polisi Keselamatan Siber MSWP	115
Lampiran 2	Borang Permohonan E-mel dan Capaian Aplikasi	116
Lampiran 3	Surat Perakuan Akta Rahsia Rasmi 1972	117
Lampiran 4	Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT MSWP	119
Lampiran 5	Senarai Perundangan dan Peraturan	120

SEJARAH POLISI KESELAMATAN SIBER MSWP

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
3 JANUARI 2023	1.0	Mesyuarat JKICT BIL. 1/2022	3 JANUARI 2023

TUJUAN

Polisi Keselamatan Siber (PKS) Mahkamah Syariah Wilayah Persekutuan (MSWP) ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga MSWP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MSWP dalam melindungi maklumat di ruang siber.

LATAR BELAKANG

PKS MSWP ini dibangungkan untuk menjamin kesinambungan urusan MSWP dengan meminimumkan kesan insiden keselamatan siber. Polisi ini disediakan berpandu kepada Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) dan Arahan Teknologi Maklumat Disember 2007.

OBJEKTIF

Objektif utama PKS MSWP adalah seperti berikut:

1. Memastikan kelancaran operasi jabatan yang berlandaskan ICT dengan mencegah serta meminimumkan kerosakan atau kemusnahan aset ICT jabatan.

2. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripadakesan kegagalan atau kelemahan daripada segi kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan.

3. Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan.

4. Meningkatkan tahap kesedaran keselamatan ICT kepada para kakitangan, pengguna danpihak luaran.

5. Memperkemaskan pengurusan risiko.

6. Mencegah penyalahgunaan atau kecurian aset ICT jabatan.

7. Melindungi aset ICT daripada penyelewengan oleh pengguna dan pihak luaran.

PERNYATAAN POLISI

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

Keselamatan ICT adalah bermaksud keadaan bagi segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan. Terdapat empat komponen asas keselamatan IT, iaitu:

1. Melindungi maklumat rahsia rasmi dan maklumat rasmi MSWP dari capaian tanpa kuasa yang sah.

2. Menjamin setiap maklumat adalah tepat dan sempurna.

3. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna.

4. Memastikan akses hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat daripada sumber-sumber yang sah.

PKS MSWP merangkumi perlindungan ke atas semua bentuk maklumat elektronik dan bukan elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaankepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah sepertiberikut:

1. **Kerahsiaan** – maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkanakses tanpa kebenaran.

2. **Integriti** – data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanyaboleh diubah dengan cara yang dibenarkan.

3. **Tidak boleh disangkal** – punca data dan maklumat hendaklah dari punca yang sah dantidak boleh disangkal.

4. **Kesahihan** – data dan maklumat hendaklah dijamin kesahihannya.

5. **Kebolehsediaan – data dan maklumat hendaklah boleh diakses pada bila-bila masa.**

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

SKOP

Sistem ICT MSWP terdiri daripada organisasi, manusia, perisian, perkakasan, telekomunikasi, kemudahan ICT, data dan maklumat. MSWP telah menetapkan keperluan-keperluan asas keselamatan seperti berikut:

1. Data dan maklumat termasuk *hardcopy* dan *softcopy* hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.

2. Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan melindungi kepentingan MSWP.

Bagi menentukan sistem ICT ini terjamin keselamatannya sepanjang masa, PKS MSWP ini merangkumi perlindungan ke atas semua bentuk maklumat ICT kerajaan yang dimasukkan, di wujud, di musnah, disimpan, dijana, dicetak, diakses, diedar dan yang dibuat salinan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

1. Data dan maklumat

   Semua data dan maklumat yang disimpan atau digunakan di pelbagai media atau peralatan ICT.

2. Peralatan ICT

   Semua peralatan komputer seperti *server*, *firewall,* komputer peribadi, komputer *desktop*, pencetak, peralatan multimedia dan alat-alat prasarana seperti *Uninterruptible Power Supply* (UPS), punca kuasa dan lain-lain.

3. Media storan

   Semua media storan yang digunakan untuk menyimpan data dan maklumat seperti *optical disk, flash disk, hard disk, USB flash drive, catridge tape, compact disc* (CD) dan lain-lain.

4. Media komunikasi

   Semua peralatan berkaitan komunikasi seperti pelayan atau perkakasan rangkaian, *gateway, router*, *wireless* LAN, peralatan sidang video*, modem*, kabel rangkaian, NIC, *switch* dan sebagainya.

5. Perisian

   Semua jenis perisian yang digunakan untuk mengendali, memproses, menyimpan danmenghantar data atau maklumat. Ini termasuklah sistem aplikasi seperti Portal MSWP dan perisian sistem seperti Windows, LINUX dan perisian utiliti, perisian komunikasi, sistem pengurusan pangkalan data, fail program, fail data dan lain-lain.

6. Dokumentasi

   Semua dokumen termasuk prosedur dan manual pengguna yang berkaitan dengan asetICT, dokumen pemasangan dan pengoperasian peralatan dan perisian.

7. Premis Komputer dan Komunikasi

   Semua kemudahan serta premis yang diguna untuk menempatkan perkara 1 hingga 6di atas.

8. Manusia

   Semua pengguna yang dibenarkan.

9. Perkhidmatan

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

   a. perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;

   b. sistem halangan akses seperti sistem kad akses; dan

   c. perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistempencegah kebakaran dan lain-lain.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada PKS MSWP 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. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

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. Kebertanggungjawaban atau Akauntabiliti

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

4. Pengasingan

   Tugas mewujud, menghapus, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi data, operasi,pangkalan data dan rangkaian.

5. Pengauditan

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

6. Pematuhan

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

7. Pemulihan

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

8. Saling Bergantung

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

PENILAIAN RISIKO KESELAMATAN ICT

MSWP hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat daripada ancaman dan kerentanan yang semakin meningkat hari ini. Justeru itu, MSWP 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.

MSWP hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan 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 MSWP 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.

MSWP 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.

MSWP 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 bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhikriteria yang telah ditetapkan oleh pengurusan atasan.

3. Mengelak atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak atau mencegah berlakunya risiko.

4. Memindahkan risiko kepada pihak luaran yang berkepentingan.

PELAN PENGURUSAN KESELAMATAN MAKLUMAT

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

Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), Polisi Keselamatan Siber MSWP dan surat pekeliling/arahan terkini untukmenangani isu-isu operasi projek.

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

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

1. Peranti Pengkomputeran Peribadi

   Peranti Pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, komputer *desktop*, telefon pintar, tablet dan peranti storan.

2. Peranti Rangkaian

   a. Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti *switch*, *router*, *firewall*, peranti VPN dan kabel.

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

3. Aplikasi

    a. Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.

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

4. Pelayan

    a. Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.

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

5. Persekitaran Fizikal

    a. Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

    b. MSWP hendaklah merujuk ke Pejabat Ketua Pegawai Keselamatan Kerajaan untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

    c. Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth*.

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

KAWALAN 01

POLISI KESELAMATAN MAKLUMAT

KAWALAN 01: POLISI KESELAMATAN MAKLUMAT

Objektif		
PKS MSWP ini diwujudkan untuk melindungi aset ICT bagi memastikan kelancaran operasi jabatansecara 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, kebolehsediaan dan kesahihan.		
PKSMSWP-K01/01	**Pelaksanaan Polisi**	
	Pelaksanaan polisi ini akan dijalankan oleh Ketua Hakim Syarie (KHS), dan dibantu oleh Jawatankuasa Keselamatan ICT (JKICT) MSWP yang terdiri daripada Ketua Pegawai Data (CDO), Pegawai Keselamatan ICT (ICTSO) dan ahli-ahli yang dilantik.	KHS
PKSMSWP-K01/02	**Penyebaran Polisi**	
	Polisi ini perlu disebarkan kepada semua yang terlibat dengan infrastruktur ICT meliputi semua pengguna.	ICTSO
PKSMSWP-K01/03	**Penyelenggaraan Polisi**	
	PKS MSWP adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan PKS MSWP: i. Mengenalpasti dan menentukan perubahan yang diperlukan. ii. Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan JKICT.	ICTSO JKICT

	iii. Memaklumkan cadangan pindaan yang telah dipersetujui oleh JKICT kepada KHS bagi tujuan pengesahan. iv. Memaklumkan pindaan yang telah disahkan oleh Ketua Hakim Syarie kepada semua kakitangan MSWP, pengguna dan pembekal. v. Mengkaji semula dasar ini secara berkala sekurang-kurangnya dua (2) tahun sekali atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	
PKSMSWP-K01/04	**Pematuhan Polisi**	
	PKS MSWP mestilah dipatuhi oleh semua pengguna.	Pengguna

KAWALAN 02

ORGANISASI KESELAMATAN MAKLUMAT

KAWALAN 02: ORGANISASI KESELAMATAN MAKLUMAT

Objektif		
Menerangkan peranan dan tanggungjawab semua pihak yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS MSWP.		
PKSMSWP-K02/01	**Tadbir Urus Keselamatan Maklumat**	
PKSMSWP-K02/01/01	**Ketua Hakim Syarie (KHS)**	
	Peranan dan tanggungjawab KHS adalah seperti berikut: i. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah PKS MSWP. ii. Memastikan semua pengguna mematuhi PKS MSWP. iii. Memastikan semua keperluan jabatan seperti sumber kewangan, sumber kakitangan dan perlindungan keselamatan adalah mencukupi. iv. Memastikan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam PKS MSWP.	KHS
PKSMSWP-K02/01/02	**Ketua Pegawai Digital (CDO)**	
	Jawatan CDO disandang oleh Ketua Pendaftar (KP) dengan lantikan secara rasmi oleh KHS. Peranan dan tanggungjawab CDO adalah seperti berikut: i. Membaca, memahami dan mematuhi PKS MSWP. ii. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MSWP. iii. Memastikan kawalan keselamatan maklumat dalam organisasi diseragam dan diselaraskan dengan sebaiknya.	CDO

	iv. Menentukan keperluan keselamatan ICT. v. Mempengerusikan Jawatankuasa Keselamatan ICT (JKICT). vi. Memastikan program-program kesedaran mengenai Keselamatan ICT dilaksanakan. vii. Memastikan dokumen Pelan Pemulihan Bencana (DRP) diwujudkan dan dilaksanakan	
PKSMSWP-K02/01/03 Pegawai Keselamatan ICT (ICTSO)		
	Jawatan ICTSO MSWP disandang oleh Ketua Unit Teknologi Maklumat yang dilantik secara rasmi oleh KHS. Peranan dan tanggungjawab ICTSO adalah seperti beriikut: i. Membaca, memahami dan mematuhi PKS MSWP. ii. Mengurus keseluruhan program keselamatan ICT MSWP. iii. Menguatkuasakan pelaksanaan PKS di MSWP. iv. Memastikan pengurusan risiko dan audit keselamatan ICT berpandukan dokumen Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) untuk mengenal pasti ketidakpatuhan kepada PKS. v. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS MSWP. vi. Memastikan semua kakitangan MSWP, kontraktor dan pembekal yang terlibat dengan aset ICT MSWP mematuhi dasar, piawaian dan garis panduan keselamatan ICT. vii. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MSWP.	ICTSO

	viii. Menentukan kawalan akses pengguna terhadap aset ICT MSWP. ix. Memastikan pengurusan risiko dan audit keselamatan ICT berpandukan dokumen Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) untuk mengenal pasti ketidakpatuhan kepada PKS MSWP. x. Mencadangkan langkah-langkah pengukuhan bagi mematuhi dasar-dasar berkaitan keselamatan ICT MSWP. xi. Melaporkan sebarang penemuan mengenai keselamatan ICT kepada JKICT. xii. Menyimpan rekod atau laporan terkini tentang ancaman keselamatan ICT MSWP. xiii. Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlaku ancaman keselamatan ICT dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian. xiv. Melaporkan insiden keselamatan ICT kepada pihak NACSA dan seterusnya membantu dalam penyiasatan atau pemulihan. xv. Melaporkan insiden keselamatan ICT kepada CDO bagi insiden yang memerlukan Pelan Kesinambungan Perkhidmatan (PKP). xvi. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera. xvii. Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan.	

	xviii. Memastikan pematuhan PKS MSWP oleh pihak luar seperti pembekal dan kontraktor yang mencapai dan menggunakan aset ICT MSWP untuk tujuan penyelenggaraan dan sebagainya. xix. Memastikan Pelan Strategik ICT (ICT Strategic Plan - ISP) MSWP mengandungi aspek keselamatan.	
PKSMSWP-K02/01/04 Pentadbir Sistem		
	Pentadbir Sistem terdiri daripada seperti berikut: i. Pentadbir Rangkaian. ii. Pentadbir Keselamatan. iii. Pentadbir Portal (Web Master). iv. Pentadbir Pusat Data. v. Pentadbir Sistem Aplikasi. vi. Pentadbir E-mel. vii. Pentadbir Media Sosial dan Aplikasi Sosial MSWP. viii. Pegawai Aset ICT.	Pentadbir Sistem
Pentadbir Rangkaian dan Keselamatan		
	Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut: i. Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di MSWP beroperasi sepanjang masa. ii. Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna. iii. Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada.	Pentadbir Rangkaian dan Keselamatan

	iv. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil. v. Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian MSWP secara tidak sah seperti melalui peralatan modem dan *dial-up*. vi. Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian. vii. Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian. viii. Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT (*Security Posture Assessment* - SPA) serta penilaian risiko keselamatan maklumat	
	Pentadbir Pangkalan Data	
	Peranan dan tanggungjawab Pentabir Pangkalan Data adalah seperti berikut: i. Melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data. ii. Memastikan pangkalan data boleh digunakan pada setiap masa. iii. Melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data. iv. Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur.	Pentadbir Pangkalan Data

	v. Melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip PKS. vi. Melaksanakan proses pembersihan data (housekeeping) di dalam pangkalan data. vii. Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.	
	Pentadbir Portal/ Laman Web	
	Peranan dan tanggungjawab Pentadbir Portal / Laman Web adalah seperti berikut: i. Menerima kandungan laman web yang terkini dan telah disahkan kesahihan daripada sumber yang sah. ii. Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar. iii. Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman. iv. Menghadkan capaian Pentadbir Portal/ Laman Web ke web server. v. Mengasingkan kandungan dan aplikasi atas talian untuk capaian secara Intranet dan Internet ke portal MSWP. vi. Memastikan data-data sulit tidak boleh disalin atau dicetak oleh orang yang tidak berhak. vii. Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi. viii. Melaksanakan proses *backup* dan *restore* secara berkala.	Pentadbir Portal / Laman Web

	ix. Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di web server. x. Melaporkan sebarang pelanggaran keselamatan laman portal kepada ICTSO.	
	Pentadbir Pusat Data	
	Peranan dan tanggungjawab Pentabir Pusat Data adalah seperti berikut: i. Memastikan persekitaran fizikal dan keselamatan Pusat Data berada dalam keadaan baik dan selamat. ii. Memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data. iii. Menjadualkan dan melaksanakan proses salinan (backup and restore) ke atas pangkalan data secara berkala. iv. Menyediakan perancangan pemulihan bencana mengikut prinsip Pengurusan Kesinambungan Perkhidmatan (PKP) dalam PKS. v. Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan. vi. Melaporkan sebarang pelanggaran keselamatan Pusat Data MSWP kepada ICTSO. vii. Memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.	Pentadbir Pusat Data

	Pentadbir Sistem Aplikasi	
	Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut: i. Mengkaji cadangan pembangunan atau penyelarasan sistem atau modul di MSWP. ii. Melaksanakan kajian semula serta memperbaiki sistem atau modul sedia ada di MSWP. iii. Membuat pertimbangan dan mengusulkan cadangan pelaksanaan sistem atau modul di MSWP. iv. Melaksanakan pemantauan dan penyelenggaraan terhadap sistem atau modul dari semasa ke semasa. v. Bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem atau modul. vi. Menyediakan dokumentasi sistem atau modul dan manual pengguna. vii. Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas. viii. Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya. ix. Memastikan *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi terkemas kini supaya terhindar daripada ancaman virus dan penggodam. x. Mematuhi dan melaksanakan prinsip-prinsip PKS dalam pewujudan akaun pengguna ke atas setiap sistem aplikasi. xi. Mengehadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan dari penyalahgunaannya.	Pentadbir Sistem Aplikasi

	xii. Melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya.	
	Pentadbir E-mel	
	Peranan dan tanggungjawab Pentabir E-mel adalah seperti berikut: i. Memastikan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara jabatan dilakukan dengan segera atas tujuan keselamatan maklumat. ii. Membekukan akaun pengguna jika perlu bagi pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib. iii. Memastikan pengguna e-mel MSWP berkemahiran menggunakan e-mel dan melaksanakan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan. iv. Memastikan kemudahan e-mel dapat dicapai melalui pelbagai peralatan ICT dan alat komunikasi. v. Mengesah dan memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan. vi. Memastikan maklumat perhubungan e-mel pengguna perlu dikemas kini dari semasa ke semasa.	Pentadbir E-mel

Pentadbir Media Sosial dan Aplikasi Sosial MSWP		
	Peranan dan tanggungjawab Pentadbir Media Sosial dan Aplikasi Sosial MSWP adalah seperti berikut: i. Memaklumkan kepada semua ahli kumpulan berkenaan tujuan utama kumpulan aplikasi pesanan diwujudkan dan memikirkan sama ada peraturan asas diperlukan. ii. Prihatin terhadap peraturan atau syarat-syarat yang digariskan oleh penyedia platform. iii. Menegur *posting* atau komen untuk memastikan perbincangan berada di landasan yang betul. iv. Sentiasa semak *posting* atau komen (dengan seorang *moderator*, jika boleh). v. Mempertimbangkan untuk mengeluarkan atau menyekat mereka yang terus membuat *posting* atau komen jelik. vi. Menggunakan platform untuk menyampaikan informasi yang tepat dan terkini. vii. Menjalankan kajian untuk mengetahui pendapat dan maklum balas daripada pengikut media sosial. viii. Membuat strategi agar maklumat yang betul disampaikan boleh disebarkan secara meluas dan teratur. ix. Memberi maklum balas kepada sebarang pertanyaan dan keraguan yang ditinggalkan di platform media sosial dalam jangka masa yang bersesuaian.	Pentadbir Media Sosial dan Aplikasi Sosial MSWP

	Pegawai Aset ICT	
	Pegawai Aset ICT ialah pegawai yang dilantik oleh Pegawai Pengawal. Peranan dan tanggungjawab Pegawai Aset ICT adalah seperti berikut: i. Memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan. ii. Memastikan penerimaan aset ICT Kerajaan dilaksanakan oleh pegawai yang dilantik oleh Ketua Jabatan/Bahagian. iii. Memastikan semua aset ICT Kerajaan yang diterima, didaftarkan menggunakan Sistem Pemantauan Pengurusan Aset (SPA) dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset. iv. Memastikan semua aset ICT Kerajaan yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan secara bertulis daripada Ketua Jabatan/Pegawai Aset/Pegawai- pegawai lain yang diberi kuasa oleh Ketua Jabatan. v. Memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/ penggantian/ naik-taraf aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira. vi. Memastikan semua aset ICT Kerajaan diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia dan nama MSWP/Seksyen/Unit berkenaan di tempat yang mudah dilihat dan sesuai pada aset berkenaan. vii. Memastikan semua aset ICT Kerajaan ditandakan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan.	Pegawai Aset ICT

	viii. Memastikan senarai daftar induk aset ICT Kerajaan disediakan. ix. Memastikan senarai aset ICT Kerajaan disediakan dipaparkan mengikut lokasi. x. Memastikan setiap kerosakan aset ICT Kerajaan dilaporkan untuk tujuan penyelenggaraan. xi. Bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT Kerajaan. xii. Merancang, memantau dan memastikan pemeriksaan aset ICT Kerajaan dilaksanakan ke atas keseluruhan aset ICT Kerajaan sekurang-kurangnya sekali setahun. xiii. Memastikan setiap kes kehilangan aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur.	
PKSMSWP-K02/01/05 Pengguna		
	Pengguna terdiri daripada warga MSWP dan pihak luaran yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan. Peranan dan tanggungjawab pengguna adalah seperti berikut: i. Membaca, memahami dan mematuhi PKS MSWP. ii. Mengetahui dan memahami implikasi keselamatan ICT daripada tindakannya. iii. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat. iv. Melaksanakan prinsip-prinsip PKS MSWP dan menjaga kerahsiaan maklumat MSWP.	Pengguna

	v. Melaksanakan langkah-langkah perlindungan seperti berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum. vi. Mengawal aktiviti penggunaan media sosial dan aplikasi sosial seperti di bawah: a. mengelakkan ketirisan maklumat; b. tidak memberi atau mendedahkan sebarang komen atau pernyataan yang menyentuh perkara-perkara yang boleh menjejaskan imej dan dasar kerajaan; c. tidak menyebarkan maklumat yang menyalahi peraturan dan undang-undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan vii. Tidak menggunakan saluran media sosial atau media sosial hingga mengganggu fokus dalam urusan kerja.	

	viii. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera. ix. Menghadiri program-program kesedaran mengenai keselamatan ICT x. Menandatangani Surat Akuan Pematuhan (**Lampiran 1**) bagi mematuhi PKS MSWP.	
PKSMSWP-K02/01/06 Jawatankuasa Keselamatan ICT (JKICT)		
	Keanggotaan JKICT adalah seperti berikut: **Pengerusi**: CDO **Ahli**: i. ICTSO/Ketua Unit Teknologi Maklumat. ii. Penolong Pegawai Teknologi Maklumat. iii. Ahli-ahli jemputan yang berkaitan. **Urusetia**: Unit Teknologi Maklumat **Bidang Kuasa**: i. Merancang, melaksana, menyemak dan memantau dasar, strategi dan pelan tindakan operasi dan keselamatan siber MSWP; ii. Merancang, melaksana, menyelaras dan memantau pengurusan operasi dan keselamatan siber MSWP; iii. Merancang, melaksana, menyelaras dan memantau pelaksanaan pelan tindakan komunikasi dan operasi ICT MSWP; iv. Melaporkan kemajuan, penyelarasan dan pemantauan keselamatan siber dan pelaksanaan pelan tindakan komunikasi dan operasi ICT kepada Pegurusan Tertinggi MSWP; dan v. Meluluskan Polisi Keselamatan Siber.	JKICT

PKSMSWP-K02/01/07 Pasukan Tindak Balas Insiden Keselamatan ICT MSWP (CERTMSWP)		
	Keanggotaan CERTMSWP adalah seperti berikut: **Pengerusi**: CDO **Ahli**: i. ICTSO/Ketua Unit Teknologi Maklumat. ii. Penolong Pegawai Teknologi Maklumat. iii. Penolong Pegawai Teknologi Maklumat (Labuan). iv. Penolong Pegawai Teknologi Maklumat (Putrajaya). v. Juruteknik Komputer. **Bidang Kuasa**: i. Menerima dan mengesan aduan keselamatan ICT daripada GCERT serta menilai tahap dan jenis insiden. ii. Merekodkan dan menjalankan siasatan awal insiden yang diterima dari GCERT. iii. Menangani tindak balas (responsive) insiden keselamatan ICT dan mengambil tindakan baikpulih minimum. iv. Menghubungi dan melapor insiden yang berlaku kepada NACSA sama ada sebagai input atau untuk tindakan seterusnya melalui pautan url https://www.nacsa.gov.my/incident_report_organisation.php. v. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada Warga MSWP.	JKICT

PKSMSWP-K02/02	**Pihak Luar**	
PKSMSWP-K02/02/01	**Keperluan Keselamatan Dalam Perkhidmatan ICT**	
	Pihak Luar terdiri daripada pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan atau pelawat yang mengunjungi MSWP atas urusan rasmi. Perkara yang perlu dipatuhi: i. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. ii. Akses kepada aset ICT MSWP perlu berlandaskan perjanjian dan peraturan yang telah ditetapkan. Perjanjian yang dimeterai perlu mematuhi perkara-perkara berikut: a. PKS MSWP; b. Tapisan Keselamatan; c. Arahan Teknologi Maklumat 2007 (IT *Instructions*); d. Perakuan Akta Rahsia Rasmi 1972; dan e. Hak Harta Intelek.	Pihak Luar ICTSO

KAWALAN 03

KESELAMATAN SUMBER MANUSIA

KAWALAN 03: KESELAMATAN SUMBER MANUSIA

Objektif		
Memastikan semua pengguna yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam melindungi keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.		
PKSMSWP - K03/01 Sebelum Perkhidmatan		
	Memastikan semua pengguna yang berkepentingan memahami tanggungjawab masing-masing dalam melindungi keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT. Perkara yang mesti dipatuhi termasuk yang berikut: i. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab semua pengguna yang berkepentingan dalam menjamin keselamatan ICT sebelum, semasa dan selepas perkhidmatan. ii. Lulus tapisan keselamatan berasaskan keperluan perundangan, peraturan dan etika semasa yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan. iii. Memastikan semua pengguna menandatangani Surat Akuan Pematuhan PKS MSWP dan Perakuan Akta Rahsia Rasmi 1972. iv. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	ICTSO

PKSMSWP - K03/02 Semasa Perkhidmatan		
	Memastikan semua pengguna yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong PKS MSWP dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi termasuk yang berikut: i. Memastikan semua pengguna yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan ditetapkan MSWP. ii. Memastikan latihan dan program kesedaran yang berkaitan keselamatan ICT diberikan kepada pengguna dari semasa ke semasa. iii. Memastikan pelaksanaan latihan jabatan sentiasa mematuhi Pekeliling Perkhidmatan semasa yang berkuat kuasa (Dasar Latihan Sektor Awam), dan perancangan latihan jabatan bersesuaian dengan fungsi serta tugas-tugas semasa pengguna. iv. Memantapkan pengetahuan berkaitan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. v. Memastikan adanya tindakan tatatertib dan/atau perundangan ke atas semua pengguna sekiranya berlaku pelanggaran keselamatan maklumat jabatan.	ICTSO

PKSMSWP - K03/03 Bertukar Atau Tamat Perkhidmatan		
	Memastikan pertukaran atau tamat perkhidmatan semua pengguna yang berkepentingan diuruskan dengan teratur. Perkara yang perlu dipatuhi termasuk: i. Memastikan semua aset ICT dikembalikan kepada Bahagian Pengurusan Maklumat, MSWP mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan. ii. Membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan MSWP dan/atau terma perkhidmatan.	ICTSO

KAWALAN 04

PENGURUSAN ASET

KAWALAN 04: PENGURUSAN ASET

Objektif		
Memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT MSWP.		
PKSMSWP - K04/01 Akauntabiliti Aset ICT		
	Memberi kawalan dan sokongan perlindungan yang bersesuaian ke atas semua aset ICT MSWP. Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi: i. Memastikan semua aset ICT dikenal pasti, dikelaskan, didokumenkan, diselenggarakan dan dilupuskan. Maklumat aset direkodkan dan dikemas kini dalam Sistem Pengurusan Aset (SPA), Kad Daftar Harta Modal dan Aset Alih Bernilai Rendah sebagaimana mengikut Pekeliling Perbendaharaan AM 2 Tahun 2018:Tatacara Pengurusan Aset Alih Kerajaan atau senarai aset yang berkaitan. ii. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja. iii. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MSWP. iv. Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan. v. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya. vi. Penggunaan aset ICT MSWP mestilah tujuan tugas rasmi sahaja.	Pegawai Aset ICT Pengguna

PKSMSWP - K04/02 Peminjaman dan Pemulangan Aset ICT		
	Peminjaman Langkah-langkah perlu diambil termasuklah seperti berikut: i. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan bagi membawa keluar peralatan bagi tujuan yang dibenarkan. ii. Melindungi dan mengawal peralatan sepanjang masa. iii. Merekodkan aktiviti peminjaman dan pemulangan peralatan. iv. Menyemak peralatan ketika peminjaman dan pemulangan dilakukan. **Pemulangan** i. Memastikan semua aset ICT dikembalikan mengikut peraturan dan atau terma perkhidmatan yang ditetapkan bagi pegawai yang: a. Bertukar keluar. b. Bersara. c. Ditamatkan perkhidmatan. d. Diarahkan oleh Ketua Jabatan. ii. Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.	Pegawai Aset ICT

PKSMSWP - K04/03 Pengelasan Maklumat		
	Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada MSWP. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan dan dilabel sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan sama ada: i. Rahsia Besar. ii. Rahsia. iii. Sulit. iv. Terhad.	Pegawai Pengelas
PKSMSWP - K04/04 Pengendalian Maklumat		
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. ii. Memeriksa maklumat dan menentukan ketepatannya dan lengkap dari semasa ke semasa. iii. Menentukan maklumat sedia untuk digunakan. iv. Menjaga kerahsiaan kata laluan. v. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan. vi. Melaksanakan peraturan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan. vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.	Pengguna

	viii. Mewujudkan salinan pendua maklumat penting bagi mengurangkan risiko kehilangan dan kemusnahan.	
PKSMSWP - K04/05 Pengelasan dan Pengendalian Data Terbuka		
	Data Terbuka ialah data yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi Kerajaan dan organisasi swasta untuk pelbagai tujuan. MSWP akan menyediakan set data terbuka berdasarkan bidang atau sektor atau kluster. Kategori set data ini tidak terhad dan boleh berubah mengikut fungsi teras dan keperluan semasa Jabatan. Data terbuka yang telah diperakukan akan diterbitkan ke Portal Data Terbuka Sektor Awam (DTSA) di bawah pengurusan MAMPU.	Jawatankuasa Penyelarasan Data Terbuka
PKSMSWP - K04/06 Pengendalian Media		
PKSMSWP - K04/06/01 Media Storan		
	Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti optical disk, flash disk, hard disk, USB flash drive, catridge tape, compact disc (CD). Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Bagi menjamin keselamatan, langkah-langkah berikut perlu diambil: i. Semua media storan perlu dikawal bagi mencegah daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan. ii. Akses dan pergerakan kepada media storan perlu direkodkan.	Jawatankuasa Penyelarasan Data Terbuka

	iii. Bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan dengan mendapat kelulusan pemilik maklumat terlebih dahulu. iv. Semua media storan data yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat. v. Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti (*data safe*) yang mempunyai ciri-ciri keselamatan termasuk tahan daripada dipecahkan, api, air dan medan magnet. vi. Storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang lebih privasi dan tidak terbuka kepada umum. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja. vii. Perkakasan *backup* hendaklah diletakkan di tempat yang selamat dan terhad kepada pengguna yang dibenarkan sahaja. viii. Salinan atau *backup* pada media storan kedua hendaklah diadakan bagi tujuan keselamatan dan bagi mengelakkan kehilangan data dan seterusnya disimpan secara *offsite* di lokasi yang telah ditetapkan. ix. Sebarang kehilangan data terperingkat di dalam media storan yang berlaku hendaklah dilaporkan mengikut Prosedur Pelaporan Insiden.	

KAWALAN 05

KAWALAN CAPAIAN

KAWALAN 05: KAWALAN CAPAIAN

Objektif		
Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT.		
PKSMSWP-K05/01	**Kawalan Capaian**	
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong polisi kawalan capaian pengguna sedia ada.	Pentadbir Sistem
PKSMSWP-K05/02	**Pengurusan Capaian Pengguna**	
PKSMSWP-K05/02/01	**Pendaftaran Pengguna**	
	Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut: i. Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan. ii. Permohonan akaun bagi pengguna baru direkodkan menggunakan Borang Permohonan E-mel dan Capaian Aplikasi seperti di **Lampiran 2**. iii. Akaun pengguna hendaklah mencerminkan identiti pengguna. iv. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika kaedah penggunaannya melanggar peraturan. v. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang.	Pentadbir Sistem Pengguna

	vi. Pentadbir sistem boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: a. Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu yang panjang; b. Bertukar bidang tugas kerja; c. Bertukar ke agensi lain; d. Bersara; atau e. Ditamatkan perkhidmatan.	
PKSMSWP-K05/02/02 Hak Capaian		
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat, atas prinsip perlu mengetahui (need-to-know-basis). Keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pegawai dan kakitangan yang dibenarkan.	Pentadbir Sistem
PKSMSWP-K05/02/03 Pengurusan Kata Laluan		
	Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MSWP seperti berikut: i. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun. ii. Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan antara huruf dan nombor dan aksara khas.	Pentadbir Sistem Pengguna

	iii. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna. iv. Kata laluan sistem pengoperasian (OS) atau Directory Service hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama. v. Kata laluan mestilah ditukar secara kerap, tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun. vi. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program. vii. Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula. viii. Kata laluan hendaklah disimpan dalam bentuk yang telah disulitkan (*encrypted*). ix. Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	
PKSMSWP-K05/03	**Capaian Sistem Pengoperasian**	
PKSMSWP-K05/03/01	**Capaian Sistem Pengoperasian**	
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian kepada sumber sistem komputer. Kemudahan ini juga perlu bagi: i. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan. ii. Merekodkan capaian yang berjaya dan gagal.	Pentadbir Sistem

	iii. Membekalkan kemudahan untuk pengesahan (bagi sistem kata laluan kunci digunakan, kualiti kata kunci perlu mendapat pengesahan). Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: i. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan. ii. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*. iii. Menjana amaran (alert) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi termasuk berikut: i. Mengawal capaian ke atas sistem operasi menggunakan kaedah log on yang terjamin. ii. 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. iii. Mewujudkan fungsi pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah kukuh mengikut polisi kata laluan yang berkuat kuasa. iv. Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	

PKSMSWP-K05/03/02 Token/Sijil Digital		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Penggunaan token atau sijil digital hendaklah digunakan bagi capaian sistem kerajaan elektronik yang dikhususkan. ii. Token hendaklah disimpan dengan selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain. iii. Perkongsian penggunaan token adalah tidak dibenarkan sama sekali. iv. Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pengeluar token.	Pengguna
PKSMSWP-K05/04 Capaian Aplikasi dan Maklumat		
	Kawalan ini bertujuan melindungi sistem maklumat dan aplikasi sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di MSWP adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi: i. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan. ii. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini.	Pentadbir Sistem Pengguna

	iii. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah. iv. Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan. v. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah. vi. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja. vii. Maklumat tarikh login terakhir hendaklah direkodkan. viii. Pelaksanaan *Session timeout* digalakkan.	
PKSMSWP-K05/05	**Capaian Jarak Jauh**	
	i. Capaian jarak jauh yang dimaksudkan merangkumi: a. Capaian daripada sistem rangkaian dalaman; dan b. Capaian daripada sistem rangkaian luaran ke sistem rangkaian dalaman sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pengeluar token. ii. Penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (*encryption*). iii. Lokasi bagi akses ke sistem ICT MSWP hendaklah dipastikan selamat.	Pentadbir Sistem Pengguna

	iv. Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada pentadbir rangkaian dan keselamatan. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	
PKSMSWP-K05/06	**Kawalan Capaian Rangkaian**	
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: i. Mewujudkan segmen rangkaian yang bersesuaian bagi membezakan di antara rangkaian MSWP dan rangkaian awam. ii. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dengan peralatan yang menepati kesesuaian penggunaannya. iii. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT. iv. Capaian pengguna jarak jauh (remote user) perlulah dikawal dan dipantau. v. Capaian fizikal dan logikal ke atas perkakasan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal. vi. Penggunaan Internet di MSWP hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian dan Keselamatan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan malicious code, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MSWP.	Pentadbir Rangkaian dan Keselamatan

	vii. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya. viii. Content Filtering boleh digunakan untuk mengawal dan memantau akses ke Internet. Pengecualian akan dipertimbangkan bagi setiap permohonan.	
PKSMSWP-K05/07	**Peralatan Mudah Alih**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan pergerakan perkakasan tersebut daripada kehilangan atau kerosakan. ii. Peralatan mudah alih hendaklah disimpan atau dikunci di tempat yang selamat apabila tidak digunakan. iii. Memastikan peralatan mudah alih yang dibawa keluar dari pejabat perlu disimpan dan dijaga dengan baik bagi mengelakkan daripada kecurian.	Pegawai Aset ICT Pengguna
PKSMSWP-K05/08	***Bring Your Own Device* (BYOD)**	
	BYOD merupakan peralatan mudah alih persendirian seperti telefon pintar, komputer tablet atau komputer riba yang digunakan oleh pengguna yang melaksanakan tugas rasmi melalui sambungan rangkaian MSWP. Pengguna yang menggunakan kemudahan wi-fi jabatan atau *data line* persendirian untuk akses kepada Internet tertakluk kepada PKS MSWP yang sedang berkuat kuasa.	Pengguna

	Sebagai garis panduan, pengguna bertanggungjawab memastikan langkah-langkah keselamatan perlindungan berkaitan penggunaan BYOD seperti berikut: i. Mengelak risiko kebocoran maklumat rasmi. ii. Mengelakkan ancaman risiko keselamatan ICT. iii. Memastikan produktiviti pengguna tidak terjejas dalam menjalankan urusan rasmi jabatan. iv. Meningkatkan integriti data. Bagi mengawal dan memantau pelaksanaan BYOD, fungsi keselamatan kata laluan hendaklah diaktifkan bagi mengelakkan akses yang tidak dibenarkan. Pengguna hendaklah bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD.	
PKSMSWP-K05/09 Telekerja		
	Telekerja merujuk kepada pekerjaan yang dijalankan secara jarak jauh dan pengguna berada di luar pejabat Kerajaan unuk melaksanakan tugas rasmi melalui sambungan rangkaian persendirian kepada rangkaian MSWP. Pengguna yang bekerja secara jarak jauh dan menggunakan kemudahan telesidang jabatan atau sambungan data persendirian untuk akses kepada Internet tertakluk kepada PKS MSWP yang sedang berkuat kuasa. Sebagai garis panduan, pengguna bertanggungjawab memastikan langkah-langkah keselamatan perlindungan berkaitan semasa telekerja seperti berikut: i. Mengelak risiko kebocoran maklumat rasmi.	Pengguna

	ii. Mengelakkan ancaman risiko keselamatan ICT. iii. Memastikan produktiviti pengguna tidak terjejas dalam menjalankan urusan rasmi jabatan. iv. Meningkatkan integriti data. Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada persekitaran telekerja.	

KAWALAN 06

KRIPTOGRAFI

KAWALAN 06: KAWALAN KRIPTOGRAFI

Objektif		
Melindungi kerahsiaan, integriti dan kesahihan maklumat yang merangkumi data dalam sistem rangkaian, sistem aplikasi dan pangkalan data.		
PKSMSWP-K06/01	**Kriptografi**	
	Kunci enkripsi mestilah dilindungi dengan menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut. Kriptografi turut merangkumi kaedah-kaedah seperti berikut: i. Kesemua pelaksanaan sistem hendaklah menggunakan ID atau kata laluan dan dibuat enkripsi. ii. Penggunaan PKI (*Public Key Infrastructure*) yang selamat yang dibekalkan oleh Kerajaan.	Pentadbir Sistem Pengguna

KAWALAN 07

KESELAMATAN FIZIKAL & PERSEKITARAN

KAWALAN 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif		
Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan dan ancaman.		
PKSMSWP-K07/01 Keselamatan Kawasan		
PKSMSWP-K07/01/01 Kawasan Larangan ICT		
	Kawasan larangan ICT bagi MSWP ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga MSWP yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis tersebut. Kawasan larangan lokasi ICT MSWP adalah Pusat Data MSWP. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas premis tersebut adalah seperti berikut: i. Sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran. ii. Akses adalah terhad kepada warga MSWP yang telah diberi kuasa sahaja dan dipantau pada setiap masa. iii. Pemantauan dilaksanakan menggunakan peralatan yang bersesuaian seperti CCTV. iv. Peralatan keselamatan fizikal seperti cctv dan sistem akses masuk perlu diperiksa secara berkala. v. Butiran pelawat yang keluar masuk ke pusat data hendaklah direkodkan. vi. Pelawat yang masuk ke pusat data perlu sentiasa diawasi atau diiringi sepanjang masa mengikut keperluan sewajarnya.	Pentadbir Pusat Data

	vii. Lokasi pusat data hendaklah tidak berhampiran dengan kawasan laluan awam. viii. Memperkukuhkan dinding, siling, tingkap dan pintu termasuk memastikan pintu sentiasa dikunci untuk mengawal kemasukan dan mengelakkan pecah masuk. ix. Mengehadkan jalan keluar masuk.	
PKSMSWP-K07/01/02 Kawalan Masuk Fizikal		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: i. Warga MSWP a. Semua warga hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; dan b. Semua pas keselamatan hendaklah diserahkan kembali kepada mswp apabila pengguna berhenti atau bersara. ii. Pelawat Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu masuk utama Premis MSWP. Pas ini hendaklah dikembalikan semula selepas tamat lawatan. iii. Kehilangan Pas Kehilangan pas mestilah dilaporkan dengan segera.	Pengguna Pelawat

PKSMSWP-K07/02	**Keselamatan Peralatan**	
PKSMSWP-K07/02/01	**Peralatan ICT**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: i. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan. ii. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan. iii. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran pentadbir sistem. iv. Pengguna mesti memastikan perisian antivirus bagi semua peralatan ICT yang dibekalkan oleh jabatan seperti komputer peribadi, komputer riba, pelayan dan lain- lain yang berada di bawah tanggungjawab mereka sentiasa aktif dan dikemaskini di samping turut melakukan imbasan ke atas media storan yang digunakan. v. Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna. vi. Aset ICT hendaklah disimpan di tempat yang selamat dan sentiasa di bawah kawalan pegawai yang bertanggungjawab. Arahan Keselamatan Kerajaan hendaklah sentiasa dipatuhi bagi mengelak berlakunya kerosakan atau kehilangan aset. vii. Sekiranya peralatan ICT tidak digunakan, peralatan tersebut hendaklah disimpan di dalam almari atau kabinet atau peti besi atau stor atau bilik khas yang berkunci untuk penyimpanan peralatan ICT.	Pengguna Pentadbir Sistem Pegawai Aset ICT

	viii. Peralatan ICT yang kritikal perlu disokong oleh UPS. ix. UPS yang berkuasa tinggi perlu diletakkan di bilik yang berasingan bersuhu rendah yang dilengkapi dengan pengudaraan yang sesuai. x. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti switch, router dan lain-lain perlu diletakkan di dalam bilik atau rak berkunci. xi. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai. xii. Peralatan ICT yang hendak dibawa keluar dari premis MSWP perlu mendapat kelulusan Pegawai Aset Bahagian atau Unit. xiii. Aset ICT yang hilang mesti dilaporkan mengikut pekeliling perbendaharaan sedia ada.	
PKSMSWP-K07/02/02 *Clear Desk* dan *Clear Screen*		
	Prosedur *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: i. Menggunakan kemudahan katalaluan atau log keluar apabila meninggalkan komputer. ii. Memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Pengguna

	iii. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci.	
PKSMSWP-K07/02/03 Media Tandatangan Digital		
	Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah–langkah berikut: i. Pengguna hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan. ii. Tidak boleh dipindah milik atau dipinjamkan. iii. Sebarang kehilangan yang berlaku hendaklah dilaporkan kepada pihak yang dipertanggungjawabkan.	Pentadbir Sistem Pengguna
PKSMSWP-K07/02/04 Perisian Dan Aplikasi		
	Penggunaan sebarang perisian dan aplikasi hendaklah mematuhi langkah-langkah berikut: i. Hanya perisian yang rasmi sahaja dibenarkan bagi kegunaan jabatan. ii. Lesen perisian (*registration code*, *serials*, *cd-keys*) perlu disimpan berasingan daripada *cd-rom*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak. iii. Kod sumber (*source code*) sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan. iv. Sistem aplikasi, perisian dan kod sumber tidak dibenarkan dikongsi, diagih, dibawa keluar atau didemontrasikan kepada pihak lain kecuali dengan kebenaran pengurusan ICT.	Pegawai Aset ICT Pentadbir Sistem

PKSMSWP-K07/02/05 Perkakasan Tanpa Penyeliaan *(Unattended Equipment)*		
	Pengguna perlu memastikan mana-mana perkakasan yang ditinggalkan tanpa penyeliaan mematuhi ciri-ciri keselamatan seperti mempunyai kata laluan dan sebagainya. Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.	Pengguna
PKSMSWP-K07/02/06 Peralatan di Luar Premis		
	Perkakasan yang dibawa keluar dari premis MSWP adalah terdedah kepada pelbagai risiko. Perkakasan yang dibawa keluar premis MSWP merangkumi: i. Penggunaan perkakasan secara sementara bagi keperluan mesyuarat, latihan dan sebagainya; dan ii. Penempatan perkakasan secara kekal di sesebuah agensi lain. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Peralatan perlu dilindungi dan dikawal sepanjang masa. ii. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Pengguna

PKSMSWP- K07/02/07 Pelupusan		
	Aset ICT yang hendak dilupuskan perlu mematuhi tatacara pelupusan semasa. Langkah-langkah berikut perlu diambil dalam memastikan peralatan ICT MSWP dilupuskan dengan teratur iaitu: i. Pegawai aset ICT akan mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya. ii. Peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan. iii. Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal. iv. Pelupusan peralatan ICT boleh dilakukan secara berpusat atau tidak berpusat mengikut tatacara pelupusan semasa yang berkuat kuasa. v. Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan. vi. Maklumat lanjut berhubung pelupusan boleh dirujuk kepada pekeliling perbendaharaan semasa yang berkuat kuasa. vii. Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara.	Pegawai Aset ICT Pengguna

PKSMSWP-K07/02/08 Penyelenggaraan		
	Peralatan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: i. Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang di selenggara. ii. Memastikan perkakasan hanya diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja. iii. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan. iv. Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pentadbir Sistem Pegawai Aset ICT
PKSMSWP-K07/03 Kawalan Persekitaran		
PKSMSWP-K07/03/01 Kawalan Persekitaran		
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk perolehan, menyewa, mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu ke Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: i. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti. ii. Semua ruang pejabat yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang bersesuaian seperti alat pencegah kebakaran dan pintu kecemasan.	ICTSO

	iii. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan. iv. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT. v. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT. vi. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer. vii. Semua peralatan perlindungan keselamatan dan kebakaran hendaklah di selenggara bagi memastikannya sentiasa berfungsi dengan baik.	
PKSMSWP-K07/03/02 Kabel Rangkaian		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: i. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat. ii. Menggunakan kabel mengikut spesifikasi yang telah ditetapkan. iii. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*.	Pentadbir Rangkaian

PKSMSWP-K07/03/03 Bekalan Kuasa		
	Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa: i. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT. ii. Peralatan sokongan seperti UPS dan penjana kuasa *(power generator)* boleh digunakan bagi perkhidmatan kritikal seperti di bilik pelayan supaya mendapat bekalan kuasa berterusan. iii. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	ICTSO
PKSMSWP-K07/03/04 Prosedur Kecemasan		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: i. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Pelan Tindakan dan Kecemasan MSWP. ii. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Kebakaran yang dilantik mengikut aras.	Pengguna Pegawai Keselamatan Kebakaran
PKSMSWP-K07/03/05 Mekanisme Pelaporan Insiden Bukan ICT		
	Semua pengguna yang terlibat haruslah melaporkan dan merekodkan sebarang kejadian atau kerosakan peralatan bukan ICT kepada pihak pentadbiran bahagian.	Pengguna

PKSMSWP-K07/03/06 Mekanisme Kawalan Peralatan Sewaan/Ujicuba *(Proof Of Concept)*		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: i. Penerimaan Peralatan yang diterima bebas daripada virus, *backdoor*, *worm* dan perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT jabatan. ii. Penyelenggaraan a. Capaian melalui rangkaian luar MSWP adalah tidak dibenarkan kecuali mendapat kebenaran bertulis ICTSO; dan b. Aktiviti penyelenggaraan adalah di bawah pengawasan pegawai MSWP. iii. Pemulangan a. Maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (*secured delete*); dan b Memastikan semua maklumat jabatan tidak tertinggal pada peralatan.	Pentadbir Sistem
PKSMSWP-K07/04 Keselamatan Sistem Dokumentasi		
	Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi: i. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan. i. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Pentadbir Sistem Pentadbir Fail

	ii. Setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti terbuka, terhad, sulit, rahsia atau rahsia besar. iii. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan. iv. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur arahan keselamatan. v. Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan, disimpan dan dihantar secara elektronik.	

KAWALAN 08

KESELAMATAN OPERASI

KAWALAN 08: KESELAMATAN OPERASI

Objektif		
Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.		
PKSMSWP-K08/01 Prosedur Operasi		
PKSMSWP-K08/01/01 Pengendalian Dokumen Prosedur Operasi		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: i. Semua prosedur operasi ICT yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal. ii. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap. iii. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pentadbir Sistem
PKSMSWP-K08/01/02 Pengurusan Perubahan		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: i. Pengubahsuaian melibatkan perkakasan, sistem pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran Pengurus ICT, pegawai atasan atau pemilik aset ICT terlebih dahulu. ii. Aktiviti seperti memasang, menyenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan.	Pentadbir Sistem

	iii. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. iv. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau sebaliknya.	
PKSMSWP-K08/01/03 Pengasingan Tugas dan Tanggungjawab		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: i. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT. ii. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah dilakukan oleh pegawai yang berlainan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. iii. Perkakasan dan rangkaian yang digunakan bagi pembangunan dan penyelenggaraan aplikasi hendaklah diasingkan daripada persekitaran produksi.	Pentadbir Sistem

PKSMSWP-K08/02	**Perancangan dan Penerimaan Sistem**	
PKSMSWP-K08/02/01	**Perancangan Kapasiti**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: i. 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. ii. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem
PKSMSWP-K08/02/02	**Penerimaan Sistem**	
	Semua sistem baharu, termasuk sistem yang dikemas kini atau diubahsuai hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem
PKSMSWP-K08/03	**Perlindungan dari Perisian Berbahaya**	
PKSMSWP-K08/03/01	**Perlindungan dari Perisian Berbahaya**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: i. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) mengikut prosedur penggunaan yang betul dan selamat. ii. Memasang dan menggunakan hanya perisian yang tulen. iii. Memastikan paten antivirus pada peralatan ICT dikemas kini dengan versi terkini	Pentadbir Sistem Pengguna

	iv. Mengimbas semua perisian, sistem, media storan dan kepilan fail dengan antivirus yang telah disediakan oleh jabatan sebelum menggunakannya. v. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat. vi. 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.	
PKSMSWP-K08/03/02 Perlindungan dari *Mobile Code*		
	Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pengguna
PKSMSWP-K08/04 *Housekeeping*		
PKSMSWP-K08/04/01 *Backup*		
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana atau insiden, *backup* seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. *Backup* hendaklah direkodkan dan disimpan di *offsite*, di antaranya adalah: i. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaharu. ii. Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. iii. Menguji sistem *backup* sedia ada dan bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.	Pentadbir Sistem

	iv. *Backup* dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan backup bergantung pada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi.	
PKSMSWP-K08/05	**Pengurusan Media**	
PKSMSWP-K08/05/01	**Media Storan Mudah Alih**	
	Penghantaran atau pemindahan media storan mudah alih yang mengandungi maklumat terperingkat ke luar pejabat mestilah mematuhi pekeliling yang terkini dan berkuatkuasa.	Pentadbir Sistem
PKSMSWP-K08/05/02	**Prosedur Pengendalian Media**	
	Di antara prosedur-prosedur pengendalian media termasuk: i. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat. ii. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja. iii. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja. iv. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan. v. Media yang mengandungi maklumat terperingkat hendaklah dihapus atau dimusnahkan mengikut peraturan dan prosedur yang betul dan selamat.	Pentadbir Sistem Pengguna

PKSMSWP-K08/06	**Paparan Maklumat Umum**	
	Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat umum adalah seperti berikut: i. Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu. ii. Memastikan segala maklumat yang hendak dipaparkan telah disahkan dan diluluskan sebelum dimuat naik ke portal. iii. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian.	Pengguna
PKSMSWP-K08/07	**Pemantauan**	
PKSMSWP-K 08/07/01	**Pemantauan**	
	Bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, di antaranya seperti berikut: i. Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang difikirkan sesuai dan boleh diterima bagi memantau kawalan capaian. ii. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala. iii. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan. iv. Kesalahan, kesilapan atau penyalahgunaan perlu di log, dianalisis dan diambil tindakan sewajarnya. v. Masa yang berkaitan dengan sistem pemprosesan maklumat dalam MSWP perlu diselaraskan dengan sumber masa yang dipersetujui.	Pentadbir Sistem

PKSMSWP-K08/07/02 Pengauditan dan Forensik ICT		
	CERTMSWP mestilah bertanggungjawab merekod dan menganalisis: i. Sebarang percubaan pencerobohan kepada sistem ICTMSWP. ii. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery*), pencerobohan (*intrusion*) ancaman (*threats*) dan kehilangan fizikal (*physical loss*). iii. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. iv. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan. v. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan. vi. Aktiviti instalasi dan penggunaan perisian yang membebankan *bandwidth* rangkaian. vii. Aktiviti penyalahgunaan akaun e-mel. viii. Aktiviti penukaran *IP address* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian. Langkah-langkah yang perlu diambil adalah seperti berikut: i. CERTMSWP akan menentukan prosedur pengumpulan bahan bukti yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan.	CERTMSWP

	ii. Proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat. iii. Sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, format laporan khas perlu disediakan. iv. Semua proses dan hasil siasatan adalah SULIT.	
PKSMSWP-K08/07/03 Jejak Audit		
	Setiap sistem mestilah mempunyai jejak audit. Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi ciri-ciri berikut: i. Rekod setiap aktiviti transaksi. ii. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan. iii. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya. iv. 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 akan 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

PKSMSWP-K08/07/04 Sistem Log		
	Fail log hendaklah disimpan untuk tempoh sekurang-kurangnya enam (6) bulan. Jenis fail log bagi pelayan dan aplikasi yang perlu diaktifkan adalah seperti berikut: i. Fail log sistem pengoperasian; ii. Fail log servis (web, e-mel); iii. Fail log aplikasi (*audit trail*); dan iv. Fail log rangkaian (*switch*, *firewall*, IPS) Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: i. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna. ii. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera. iii. Sekiranya wujud aktiviti-aktiviti tidah sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	Pentadbir Sistem

KAWALAN 09

KESELAMATAN KOMUNIKASI

KAWALAN 09: KESELAMATAN KOMUNIKASI

Objektif		
Memastikan sistem komunikasi yang digunakan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.		
PKSMSWP-K09/01 Pengurusan Rangkaian		
	Infrastruktur Rangkaian perlu dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi dalam rangkaian. Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut: i. Semua tanggungjawab atau kerja-kerja operasi dan rangkaian hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan. ii. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkansahaja. iii. Semua capaian kepada internet dan sistem aplikasi mestilah melalui *firewall*. iv. Memasang perisian IPS bagi mengesan dan menghalang sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MSWP. v. Menggunakan *web content filter* untuk menyekat aktiviti yang dilarang. vi. Sebarang penyambungan rangkaian yang bukan dibawah kawalan MSWP adalah tidak dibenarkan. vii. Kemudahan bagi *wireless* LAN MSWP dengan pelaksanaan kawalan keselamatan.	Pentadbir Rangkaian

PKSMSWP-K09/02	**Pengurusan Penghantaran dan Penerimaan Maklumat**	
	Bertujuan untuk memastikan keselamatan penghantaran dan penerimaan maklumat dan perisian dalam agensi dan mana-mana entiti luar terjamin. i. Polisi, prosedur dan kawalan penghantaran dan penerimaan maklumat yang formal perlu diwujudkan untuk melindungi maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi. ii. Perjanjian perlu diwujudkan untuk penghantaran dan penerimaan maklumat dan perisian di antara MSWP dengan pihak luar. iii. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan dan penerimaan. iv. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya. v. Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat MSWP.	Pentadbir Sistem
PKSMSWP-K09/03	**Pengurusan Mel Elektronik (E-mel)**	
	Penggunaan e-mel MyGovUC MAMPU di MSWP hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet. Di antara prosedur-prosedur pengurusan e-mel termasuk: i. Mengehadkan jenis dan saiz fail lampiran bagi tujuan mengelakkan jangkitan virus dan serangan e-mel *bombing*. ii. Penghantaran dokumen rasmi hendaklah menggunakan e-mel rasmi jabatan sahaja.	Pentadbir E-mel Pegawai Tadbir (Sumber Manusia) Pengguna

	iii. Penggunaan e-mel rasmi bagi tujuan peribadi adalah tidak dibenarkan. iv. Penghantaran lampiran dalam format atau *extension "*.exe, *.bat"* dan " **.com"* tidak dibenarkan. v. Permohonan akaun e-mel hendaklah menggunakan Borang Permohonan E-mel dan Capaian Aplikasi seperti di **Lampiran 2**. Hanya warga MSWP atau pengguna yang dibenarkan sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi jabatan. vi. Pegawai Tadbir (Sumber Manusia) perlu memaklumkan sebarang status pengguna (bertukar jabatan, bersara,diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke mswp) di bahagian masing-masing bagi tujuan pengemaskinian e-mel yang terlibat. vii. Menggunakan fungsi *smart attach* untuk penghantaran fail yang bersaiz lebih 10 MB. viii. E-mel rasmi yang dihantar atau diterima hendaklah disimpan dan diarkibkan mengikut panduan yang digariskan. ix. Menggunakan enkripsi bagi dokumen terperingkat yang dihantar secara elektronik.	
PKSMSWP-K09/04	**Pengurusan Penggunaan Sidang Video *(Video Conferencing)***	
	Penggunaan Sidang Video (VC) di MSWP hendaklah mematuhi Garis Panduan Penggunaan Sidang Video untuk memastikan Sidang Video dapat dijalankan dengan lancar.	Pentadbir Sistem

Garis panduan bagi urusetia atau penganjur mesyuarat adalah seperti berikut:

i. Permohonan Persidangan

a. Urusetia atau penganjur hendaklah mengemukakan permohonan untuk mengadakan persidangan video kepada Unit Teknologi Maklumat melalui memo dalaman atau e-mel bagi tujuan penyediaan pautan, pemasangan peralatan teknikal dan juga khidmat sokongan teknikal;

b. Permohonan hendaklah dikemukakan tiga (3) hari bekerja sebelum mesyuarat sebenar diadakan; dan

c. Sebarang pembatalan, perubahan waktu, tarikh atau tempat mesyuarat secara sidang video yang telah dipohon juga perlu dimaklumkan kepada Unit Teknologi Maklumat bagi tujuan penyelarasan.

ii. Pelaksanaan Persidangan

a. Urusetia atau penganjur sesuatu mesyuarat atau acara adalah bertanggungjawab untuk menjadi hos dan mengoperasikan VC sepanjang mesyuarat berlangsung;

b. Pihak ICTMSWP akan menyediakan pautan VC untuk setiap mesyuarat. Urusetia atau penganjur perlu memastikan pautan tersebut adalah betul dan berfungsi;

c. Urusetia atau penganjur perlu memaklumkan awal kepada semua ahli mesyuarat atau peserta berkenaan butir mesyuarat berserta pautan VC serta memastikan hanya ahli yang berdaftar dan dijemput sahaja diberikan maklumat VC;

	d. Sebarang rakaman video boleh disimpan secara atas awan *(cloud)* sekiranya perlu untuk rujukan semula selepas selesai mesyuarat; e. Sesi pengujian boleh dilaksanakan sebelum sesuatu mesyuarat berlangsung bagi memastikan pautan dan peralatan VC berfungsi dalam keadaan yang baik; dan f. Adalah menjadi tanggungjawab urusetia atau penganjur untuk memaklumkan segera kepada pihak ICTMSWP yang bertugas selepas tamat mesyuarat. Ini adalah untuk memastikan semua peralatan dan perisian VC dapat diambil semula atau ditamatkan sesi dengan sempurna. Garis panduan bagi Ahli Mesyuarat adalah seperti berikut: i. Sebelum Sesi a. Pegawai perlu menggunakan nama sebenar dan e-mel rasmi untuk memudahkan komunikasi dan memudahkan urusetia merekodkan kehadiran setiap ahli mesyuarat; b. Peralatan yang digunakan hendaklah mempunyai mikrofon dan kamera yang berfungsi dengan baik. Fungsi mikrofon hendaklah dalam keadaan *mute* dan kamera video dalam keadaan *stop*. Pegawai bolehlah *unmute* atau membuka kamera video sekiranya diarahkan urusetia atau untuk tujuan pengujian awal; c. Pegawai dinasihatkan menggunakan satu peralatan VC sahaja pada satu-satu masa. Jauhi objek atau peralatan elektronik yang boleh menyebabkan gangguan kepada kualiti suara dan video;	

	d. Pegawai hendaklah berpakaian kemas dan sopan ketika acara rasmi dan berada di persekitaran yang sesuai; dan e. Telefon bimbit dalam tetapan *mode* senyap. ii. Semasa Sesi a. Kekalkan fungsi mikrofon dalam keadaan mute dan tekan start video; b. Gunakan fungsi raise hand atau menaip soalan di dalam chatbox sekiranya ingin bertanya soalan; c. Sekiranya hos atau pengerusi membenarkan anda untuk bertanya soalan, unmute fungsi mikrofon; d. Pegawai yang ingin membentangkan sesuatu dari skrin komputer masing-masing, minta kebenaran hos untuk membenarkan anda berkongsi skrin komputer (fungsi share screen); dan e. Sekiranya ada keperluan untuk meninggalkan VC semasa mesyuarat berlangsung, pegawai dinasihatkan memaklumkan urusetia terlebih awal untuk memudahkan perjalanan mesyuarat. iii. Selepas Sesi Pastikan anda *Leave Meeting* selepas selesai sesi persidangan video berkenaan.	

KAWALAN 10

PEROLEHAN, PEMBANGUNAN & PENYELENGGARAAN SISTEM

KAWALAN 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Objektif		
Memastikan sistem yang dibangunkan sendiri secara dalaman atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.		
PKSMSWP-K10/01	**Kawalan Prosesan Aplikasi**	
	i. Perolehan dan pembangunan, penambahbaikan serta penyelenggaraan sistem secara dalaman atau luaran hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu sistem pemprosesan dan ketepatan maklumat. ii. Ujian keselamatan hendaklah dijalankan ke atas sistem aplikasi untuk menyemak pengesahan dan integriti data. iii. Sistem yang dibangunkan atau digunakan hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan sebelum digunakan.	Pentadbir Sistem ICTSO
PKSMSWP-K10/01/01	**Pengesahan Data *Input***	
	Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.	Pentadbir Sistem
PKSMSWP-K10/01/02	**Kawalan Proses**	
	Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa proses dijalankan.	Pentadbir Sistem

PKSMSWP-K10/01/03	**Pengesahan Data *Output***	
	Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pentadbir Sistem
PKSMSWP-K10/02	**Keselamatan Fail Sistem**	
	Fail sistem perlu dikawal dan dikendalikan dengan baik danselamat. i. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan. ii. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji. iii. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpakebenaran, penghapusan dan kecurian. iv. Mengaktifkan log audit bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan. v. Data ujian hendaklah dipilih dan penggunaannya dikawal serta dilindungi.	Pentadbir Sistem
PKSMSWP-K10/03	**Keselamatan Dalam Proses Pembangunan dan Sokongan**	
PKSMSWP-K10/03/01	**Peraturan Keselamatan Dalam Pembangunan Sistem**	
	Tatacara pembangunan perisian dan sistem yang mengambil kira aspek keselamatan maklumat hendaklah diwujudkan dan dilaksanakan di dalam organisasi.	ICTSO

PKSMSWP-K10/03/02 Prosedur Perubahan		
	Perubahan atau pengubahsuaian ke atas kitaran hayat pembangunan sistem, sistem pengoperasian dan aplikasi hendaklah dikawal, diuji, di rekod dan disahkan sebelum digunakan mengikut SOP yang telah ditetapkan.	Pentadbir Sistem
PKSMSWP-K10/03/03 Semakan Teknikal Aplikasi Selepas Perubahan Platform		
	Semakan dan pengujian terhadap aplikasi perlu dilaksanakan sekiranya berlaku perubahan terhadap platform pengoperasian bagi memastikan fungsi dan operasi sistem tidak terjejas. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Memastikan sistem aplikasi, integriti data dan kawalan akses disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilaksanakan. ii. Ujian penerimaan pengguna perlu dilaksanakan setelah perubahan platform selesai dilaksanakan.	Pentadbir Sistem
PKSMSWP-K10/03/04 Kawalan Terhadap Perubahan Kepada Perisian		
	Sebarang perubahan terhadap perisian adalah tidak digalakkan, kecuali kepada perubahan yang perlu sahaja dan perubahan tersebut perlu dihadkan.	Pentadbir Sistem
PKSMSWP-K10/03/05 Prinsip Kejuruteraan Sistem Yang Selamat		
	Prinsip kejuruteraan sistem yang selamat hendaklah dibangunkan, didokumenkan, dikaji dan diguna pakai ke atas semua pelaksanaan sistem maklumat.	Pentadbir Sistem
PKSMSWP-K10/03/06 Persekitaran Pembangunan Sistem Yang Selamat		
	Persekitaran pembangunan sistem yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem.	Pentadbir Sistem

PKS PKSMSWP-K10/03/07 Pembangunan Sistem Secara Luaran *(Outsource)*		
	Pembangunan perisian aplikasi secara *outsource* hendaklah mematuhi perkara-perkara berikut: Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Setiap projek perlu dipantau oleh ICTMSWP. ii. Kontrak perbekalan hendaklah memasukkan klausa kod sumber menjadi hak milik MSWP. iii. Kod sumber yang diserahkan kepada MSWP mesti bebas daripada sebarang ralat dan kerentanan. iv. Mengutamakan kepakaran teknologi tempatan. v. Pembangunan aplikasi hendaklah dijalankan dalam persekitaran pengkomputeran MSWP. vi. Penggunaan *data masking* semasa pengujian. vii. Data ujian hendaklah dilupuskan secara kekal (*secured delete*) selepas projek disiapkan/tamat kontrak. viii. Aktiviti *backup* hendaklah berjaya dilakukan sebelum projek tamat.	ICTSO
PKSMSWP-K10/03/08 Ujian Keselamatan Sistem		
	Aktiviti pengujian keselamatan sistem hendaklah dilaksanakan atas sistem baharu, tambah baik, naik taraf dan versi baharu berdasarkan kriteria yang telah ditetapkan.	Pentadbir Sistem ICTSO
PKSMSWP-K10/03/09 Pembocoran Maklumat		
	Sebarang peluang untuk membocorkan maklumat perlu dilarang dan dihalang.	ICTSO

PKSMSWP-K10/04 Data Ujian		
	Memastikan data yang digunakan untuk pengujian adalah dilindungi.	Pentadbir Sistem
PKSMSWP-K10/05 Kawalan Terhadap Keterdedahan Teknikal		
	Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: i. Memperoleh maklumat keterdedahan teknikal sistem maklumat yang digunakan. ii. Menilai tahap kerentanan bagi mengenal pasti tahap risiko yang bakal dihadapi. iii. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICTSO
PKSMSWP-K10/06 Perkhidmatan E-dagang		
	Bertujuan untuk memastikan keselamatan perkhidmatan e-dagang dan penggunaannya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan. ii. Maklumat yang terlibat dalam transaksi dalam talian perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan.	Pentadbir Sistem Pengguna

	iii. Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	
PKSMSWP-K10/07 Pembangunan Aplikasi Mudah Alih		
	Menerangkan perkara yang perlu dipatuhi dalam membangunkan aplikasi mudah alih agar lebih selamat.	Pentadbir Sistem
PKSMSWP-K10/07/01 Prosedur Integrasi Pembangunan Aplikasi Mudah Alih		
	Pembangunan aplikasi mudah alih yang melibatkan integrasi dengan sistem induk hendaklah menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang tidak memberi risiko ancaman keselamatan.	Pentadbir Sistem

KAWALAN 11

HUBUNGAN PEMBEKAL

KAWALAN 11: HUBUNGAN PEMBEKAL

Objektif		
Memastikan aset ICT MSWP yang boleh dicapai oleh pembekal dilindungi. Semua pembekal adalah tertakluk kepada Dasar Keselamatan Kerajaan yang berkuat kuasa.		
PKSMSWP-K11/01	**Keselamatan Maklumat Dalam Hubungan Dengan Pembekal**	
	Perkara–perkara yang perlu dipatuhi adalah seperti berikut: i. Pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas. ii. Pengurusan pembekal adalah tertakluk kepada peraturan yang sedang berkuat kuasa. iii. Pengawalan dan pemantauan akses pembekal. iv. Keperluan minimum keselamatan maklumat bagi setiap pembekal seperti keperluan perundangan atau pekeliling berkaitan hendaklah dinyatakan dalam perjanjian. v. Akses kepada aset ICT MSWP perlu berlandaskan kepada perjanjian kontrak perkhidmatan yang telah dipersetujui dengan pihak ketiga. vi. Capaian dari luar rangkaian MSWP oleh pihak ketiga adalah tidak dibenarkan kecuali dengan kebenaran ICTSO. vii. Capaian kepada kod sumber program dari luar pejabat oleh pihak ketiga tidak dibenarkan kecuali mendapat kebenaran bertulis ICTSO. viii. Pembekal hendaklah menandatangani Perakuan Akta Rahsia Rasmi 1972 seperti di **Lampiran 3**.	ICTSO Pembekal

	ix. Semua perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut peraturan-peraturan semasa. x. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. Perubahan dalam perjanjian dengan pembekal; b. Perubahan yang dilakukan oleh mswp bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian polisi dan prosedur; dan c. Perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	
PKSMSWP-K11/02	**Pengurusan Penyampaian Perkhidmatan Pembekal**	
	Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan penyampaian perkhidmatan adalah sama seperti perjanjian pembekal. MSWP hendaklah sentiasa memantau, mengkaji semula dan mengaudit penyampaian perkhidmatan pembekal. Perkara-perkara berikut hendaklah dipatuhi: i. Pemantauan tahap prestasi perkhidmatan bagi mengesahkan pembekal mematuhi perjanjian perkhidmatan. ii. Laporan perkhidmatan yang dihasilkan oleh pembekal hendaklah dipantau dan status kemajuan dikemukakan kepada MSWP. iii. Semua perubahan perkhidmatan pembekal hendaklahdilaksanakan secara teratur dan mengikut peraturan-peraturan semasa.	ICTSO Pentadbir Sistem

	Perkara-perkara yang perlu diambil kira adalah seperti berikut: i. Perubahan dalam perjanjian dengan pembekal. ii. Perubahan yang dilakukan oleh mswp bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian polisi dan prosedur. iii. Perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	

KAWALAN 12

RISIKO DAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

KAWALAN 12: RISIKO DAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

Objektif		
Untuk memastikan semua insiden dikendalikan dengan konsisten, cepat, tepat dan berkesan termasuk saluran komunikasi keselamatan dan *security events* bagi memastikan sistem ICT MSWP dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej MSWP dan sistem penyampaian perkhidmatan.		
PKSMSWP - K12/01 Mekanisme Pelaporan Insiden Keselamatan ICT		
	i. Pelaporan Semua insiden keselamatan ICT yang berlaku mesti dilaporkan segera kepada CERTMSWP untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan bagi mengelakkan kerosakan bahan bukti tanpa melaksanakan tindakan secara sendirian. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. Antara insiden keselamatan ICT yang perlu dilaporkan adalah: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak- pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau yang disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses yang hilang, dicuri, didedahkan atau yang disyaki sedemikian; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal berfungsi atau dicapai, dan komunikasi tersalah hantar; dan	ICTSO Pengguna CERTMSWP

	e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka yang boleh menjejaskan keselamatan ICT. ii. Pelaporan NACSA a. ICTSO melaporkan kepada NACSA apabilaberlaku sebarang insiden keselamatan ICT sekiranya perlu. b. Pasukan CERTMSWP dengan persetujuan ICTSO akan menghubungi NACSA untuk melaporkan atau mendapatkan bantuan apabila wujud potensi insiden atau berlaku sebarang insiden keselamatan ICT. iii. Tindakan Dalam Keadaan Berisiko Tinggi Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak. iv. ICTSO melaporkan kepada NACSA apabila berlaku sebarang insiden keselamatan ICT sekiranya perlu v. Insiden Keselamatan Sistem Pentadbir sistem yang terlibat mesti melaporkan sebarang kejadian yang melibatkan keselamatan ICT kepada CERTMSWP.	
PKSMSWP - K012/02 Prosedur Pengurusan dan Pengendalian Insiden Keselamatan ICT		
	Pasukan CERTMSWP perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan Prosedur Pengurusan Pelaporan Dan Pengendalian Insiden Keselamatan ICT MSWP seperti Carta Alir di **Lampiran 4.**	ICTSO Pengguna CERTMSWP

	CERTMSWP menerima aduan atau laporan daripada pengguna, laporan yang dikesan daripada pihak NACSA atau laporan daripada sumber lain. Seterusnya, maklumat tentang insiden akan didaftarkan. Siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden tersebut. Laporan insiden kemudiannya dimaklumkan kepada pihak NACSA. Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan dipanjangkan kepada agensi penguat kuasa undang- undang. CERTMSWP yang diketuai oleh ICTSO akan menjalankan tindakan pengendalian secara capaian jauh (*remote*) atau *on-site.* Sekiranya laporan tersebut memerlukan bantuan pihak NACSA, permohonan akan dihantar bagi mendapatkan maklum balas pihak NACSA. Bagi laporan yang memerlukan bantuan daripada CERT agensi yang lain, permohonan akan dihantar melalui pihakNACSA dan khidmat nasihat akan disalurkan. CERTMSWP seterusnya akan menyediakan laporan dan ICTSO mengesahkan sekiranya DRP perlu diaktifkan atau sebaliknya. Pengesahan akan dihantar kepada CDO bagi mengaktifkan DRP. Laporan insiden yang tidak memerlukan PKP akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan. 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 keselamatan ICT. ii. Mematuhi Pelan Pemulihan Bencana (DRP). iii. Menyimpan jejak audit dan memelihara bahan buktidan rekod.	

	iv. Menyediakan tindakan pencegahan supaya insiden serupa tidak berulang. v. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	

KAWALAN 13

KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

KAWALAN 13: KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Objektif		
Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.		
PKSMSWP - K13/01 Pengurusan Kesinambungan Perkhidmatan		
	Pengurusan Kesinambungan Perkhidmatan (PKP) ialah mekanisme bagi mengurus dan memastikan kepentingan stakeholder sistem penyampaian perkhidmatan dilindungi dan imej MSWP terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan MSWP di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan. Ketua Hakim Syarie adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan bagi member perlindungan keselamatan kepada aset ICT MSWP. Pelan PKP terdiri daripada tiga (3) pelan utama iaitu Kumpulan Tindak Balas Kecemasan (ERT), Pelan Komunikasi Krisis (CCP) dan Pelan pemulihan Bencana (DRP). Pelan PKP perlu dibangunkan dan mengandungi perkara-perkara berikut: i. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan.	Pasukan DRP MSWP

	ii. Senarai pengguna berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga perlu disediakan sebagai maklumat alternatif bagi pegawai yang tidak dapat hadir untuk menangani insiden. iii. Senarai maklumat yang lengkap yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan. iv. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh. v. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan. Pelan PKP hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan pegawai yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan MSWP hendaklah memastikan salinan pelan PKP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

PKSMSWP - K13/01/01 Pelan Pemulihan Bencana		
	Pelan Pemulihan Bencana hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh Jawtankuasa Pemandu PKP MSWP dan perkara-perkara berikut perlu diberi perhatian: i. Mengenal pasti semua tanggungjawab dan prosedur kecemasan dan pemulihan. ii. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan. iii. Mendokumentasikan proses dan prosedur yang telah dipersetujui. iv. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT. v. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan. vi. Membuat *backup*. vii. Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.	Pasukan DRP MSWP
PKSMSWP - K13/02 *Redundancy*		
	Semua sistem aplikasi dan perkakasan yang kritikal hendaklah mempunyai kemudahan *redundancy* dan diuji (*failover test*) keberkesanannya mengikut keperluan.	ICTSO Pentadbir Sistem

KAWALAN 14

PEMATUHAN

KAWALAN 14: PEMATUHAN

Objektif		
Meningkatkan tahap keselamatan ICT bagi mengelak daripada pelanggaran kepada PKS MSWP.		
PKSMSWP - K14/01 Pematuhan Polisi		
	Setiap pengguna di MSWP hendaklah membaca, memahami dan mematuhi PKS MSWP dan undang-undang atau peraturan-peraturan lain yang berkaitan. Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua warga di MSWP adalah seperti di **Lampiran 5**. Perkara yang perlu dipatuhi adalah seperti berikut: i. Semua perlembagaan, undang-undang, peraturan, perjanjian yang dimeterai dan lain-lain perkara yang relevan kepada keselamatan sistem maklumat dan organisasi hendaklah dikenal pasti, didokumentasikan dan dikemaskini. ii. Peraturan yang sesuai dilaksanakan untuk pematuhan ke atas perlembagaan, undang-undang dan keperluan perjanjian mengenai penggunaan material yang tertakluk kepada hak milik harta intelek. iii. Rekod penting hendaklah dilindungi daripada hilang, rosak dan dipalsukan selaras dengan keperluanundang-undang, peraturan dan keperluan perjanjian MSWP. iv. Perlindungan ke atas data dan maklumat privasi hendaklah mematuhi perundangan, peraturan dan terma perjanjian jika perlu. v. Penyalahgunaan pemprosesan maklumat adalah tidak dibenarkan. vi. Penggunaan kriptografi dikawal selaras dengan perjanjian, perundangan dan peraturan yang berkuat kuasa.	Pengguna

PKSMSWP - K14/02 Pematuhan kepada Polisi, Peraturan dan Penilaian Teknikal Keselamatan		
	ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi polisi, piawaian dan keperluan teknikal. Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi piawaian pelaksanaan keselamatan. Sebarang penilaian pematuhan teknikal seperti aktiviti *Security Posture Assessment* (SPA) mestilah dijalankan oleh individu yang kompeten dan dibenarkan	ICTSO
PKSMSWP - K14/03 Pematuhan Keperluan Audit		
	Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dikawal dan diselia bagi mengelakkan berlaku penyalahgunaan.	ICTSO
PKSMSWP - K14/04 Pelanggaran Perundangan		
	Pelanggaran polisi ini boleh diambil tindakan undang-undang dan tatatertib di bawah Akta Rahsia Rasmi 1972 dan Perintah-perintah Am Bab D - Peraturan-peraturan Pegawai Awam (Kelakuan Dan Tatatertib).	Pengguna

GLOSARI

GLOSARI

Terma	Keterangan
Active Directory (AD)	Teknologi *Microsoft* yang digunakan untuk mengurus komputer dan perkakasan lain dalam rangkaian.
Antivirus	Perisian yang mengimbas virus pada media storan, seperti cakera keras(hard disk) dan *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari suatu tempat ke suatu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
Aset ICT	Peralatan ICT termasuk komputer, media storan, *server, router, firewall*, rangkaian dan lain-lain.
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 PC utama) dalam jangka masa yang ditetapkan.
BYOD	*Bring Your Own Device*
CCTV	*Closed-circuit television* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
CERT Agensi	*Computer Emergency Response Team* Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
CDO/CIO	*Chief Digital Officer/Chief Information Officer* Ketua Pegawai Digital/Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi bagi mewujudkan budaya kerja yang dipacu oleh digital
Clear Desk dan *Clear Screen*	Tidak meninggalkan dokumen data dan maklumat terperingkat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
Data-at-rest	*Data-at-rest* (data-dalam-simpanan) Data yang tidak aktif yang disimpan secara fizikal dalam bentuk digital (contohnya pangkalan data, gudang data, hamparan, arkib dan sebagainya).
Data-in-motion	*Data-in-motion* (data-dalam-pergerakan) Data-dalam-pergerakan atau data transit maklumat digital yang sedangdalam proses pergerakan di dalam atau antara sistem komputer.
Data-in-use	*Data-in-use* (data-dalam-penggunaan) Data yang digunakan ialah data yang sedang diperbaharui, diproses, dihapus, diakses atau dibaca oleh sistem. Jenis data ini tidak disimpan secara pasif, tetapi bergerak aktif melalui infrastruktur IT.
Data masking	*Data masking* ialah kaedah penyembunyian data asli yang digunakan untuk tujuan pengujian dan latihan.

Terma	Keterangan
Defence-in-depth	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
DRC	*Disaster Recovery Centre* Pusat Pemulihan Bencana
DRP	*Disaster Recovey Plan* Pelan Pemulihan Bencana
Encryption	Enkripsi atau penyulitan. Proses enkripsi data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat *(information theft/espionage),* penipuan *(hoaxes).*
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas..
ICT	*Information and Communication Technology*
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
ISDN	*Integrated Services Digital Networks* Menggunakan isyarat digital pada talian telefon analog yang sedia ada.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna pada mana-mana komputer boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.

Terma	Keterangan
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 yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Berperanan bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Sebagai contoh, Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
ISMS	*Information Security Management System*
MSWP	Organisasi MSWP merangkumi bahagian/seksyen/unit seperti berikut: 1. Bahagian Kehakiman; 2. Bahagian Pengurusan Kehakiman dan Pendaftaran 3. Mahkamah Rayuan Syariah 4. Mahkamah Tinggi Syariah 5. Mahkamah Rendah Syariah 6. MSWP Labuan 7. MSWP Putrajay 8. Seksyen Pengurusan Kes 9. Seksyen Sulh 10. Seksyen Bahagian Sokongan Keluarga 11. Seksyen Khidmat Pengurusan dan Sumber Manusia i. Unit Pentadbiran ii. Unit Sumber Manusia iii. Unit Kewangan iv. Unit Perolehan v. Unit Teknologi Maklumat 12. Seksyen Rekod
Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman keselamatan ICT yang boleh menjejaskan kelancaran operasi dan sistem ICT MSWP.
Kriptografi	Kaedah untuk menukar data dan maklumat biasa (piawaian format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
KPKK	Ketua Pegawai Keselamatan Kerajaan
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Lightning arrestor	Alat yang digunakan untuk mencegah daripada ancaman kilat.
Lock	Mengunci komputer.
Log out	*Log-out* komputer

Terma	Keterangan
	Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Merupakan perisian hasad atau jahat yang memasuki sistem komputer dan menyebabkan risiko keselamatan seperti kerosakan komputer, gangguan capaian Internet dan sebagainya tanpa disedari oleh pengguna.
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 komputer.
Mobile Code	*Mobile code* merupakan perisian yang boleh dipindahkan antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh *Java Applet, ActiveX* dan sebagainya pada pelayar Internet.
NACSA	*National Cyber Security Agency* Agensi Keselamatan Siber Negara
Outsource	Maklumat yang diproses dan diperoleh di luar daripada sesuatu organisasi atau struktur kerja.
Peripheral	Aset yang digunakan untuk menyokong pemprosesan maklumat.
Perisian Aplikasi	Merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Pengguna	Pengguna terdiri daripada warga MSWP dan pihak luaran yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT MSWP.
Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan daripada segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
Pegawai Keselamatan	Pegawai yang memastikan keselamatan perlindungan di jabatan terjamin sepanjang masa.
Pihak Luar	Pihak luar terdiri daripada pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan atau pelawat yang mengunjungi MSWP atas urusan rasmi.
PKI	*Public-Key Infrastructure* Infrastruktur Kunci Awam
PKP	Pengurusan Kesinambungan Perkhidmatan
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.

Terma	Keterangan
Rahsia Besar	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada negara.
Restoration	Pemulihan ke atas data.
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 ia tidak digunakan dalam jangka masa tertentu.
Server	Pelayan
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.
Switch	Alat yang boleh menapis (*filter*) dan memajukan (*forward*) isyarat paketdata antara segmen rangkaian LAN.
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.
Threat	*Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.*
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
WAN	*Wide Area Network* Rangkaian yang merangkumi kawasan yang luas.

Terma	Keterangan
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.
Worm	Sejenis virus yang boleh beraplikasi dan membiak dengan sendiri. Ia biasanya menjangkiti sistem operasi yang lemah atau tidak dikemaskini.

LAMPIRAN

Lampiran 1

SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER MSWP

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
MAHKAMAH SYARIAH WILAYAH PERSEKUTUAN (MSWP)

Nama (Huruf Besar)	:	……
No. Kad Pengenalan	:	……
Jawatan	:	……
Bahagian/Seksyen/Unit	:	……
Organisasi (selain MSWP)	:	……
No. Kontrak (jika berkaitan)	:	……

Adalah dengan sesungguhnya saya mengaku bahawa:

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

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

.....
(Tandatangan)

Mahkamah Syariah Wilayah Persekutuan .....

Tarikh : .....

Lampiran 2

BORANG PERMOHONAN E-MEL DAN CAPAIAN APLIKASI

BORANG PERMOHONAN CAPAIAN APLIKASI

UNIT TEKNOLOGI MAKLUMAT MSWP
Kompleks Mahkamah Syariah Wilayah Persekutuan,
No. 71, Jalan Sri Hartamas 1, Taman Sri Hartamas 50676 Kuala Lumpur

ID Staf:

BAHAGIAN A : JENIS PERMOHONAN (Tandakan 'X' pada jenis permohonan yang berkenaan)		
☐ Sijil Digital Roaming (Aplikasi : ESyariah)	☐ Sijil Digital Token (Aplikasi : ePerolehan, 1gfmas)	
☐ Emel	**ID Pilihan Pertama**	@esyariah.gov.my
	ID Pilihan Kedua	@esyariah.gov.my
☐ mySMS		

BAHAGIAN B : MAKLUMAT PEMOHON	
Nama Penuh (Seperti dalam kad pengenalan)	
No. MyKad	
Jawatan Dan Gred	
Bahagian/Seksyen/Unit	
No. Telefon Pejabat	
No. Telefon Bimbit	
Emel Alternatif	*(contoh : Yahoo/Gmail)*

BAHAGIAN C : PERAKUAN PEMOHON

Saya dengan ini mengesahkan bahawa kesemua maklumat yang diberikan adalah benar.

_____ Tandatangan Pemohon

_____ Tarikh

BAHAGIAN D : PENGESAHAN KETUA JABATAN / KETUA PENDAFTAR

Dengan ini, saya mengesahkan dan menyokong permohonan tersebut di atas.

Tandatangan & Cop Pegawai :

Tarikh :

BAHAGIAN E : UNTUK KEGUNAAN UNIT TEKNOLOGI MAKLUMAT

Status Permohonan			Tandatangan & Cop Pegawai ICT:
Sijil Digital : ☐ Diluluskan ☐ Ditolak	**ID Emel Diluluskan :** ☐ Pilihan Pertama ☐ Pilihan Kedua ☐ Dipinda _____	**mySMS :** ☐ Diluluskan ☐ Ditolak	Tarikh :

Nota :
Pemohon dimaklumkan melalui : _____

Lampiran 3

SURAT PERAKUAN AKTA RAHSIA RASMI 1972 (MULA PERKHIDMATAN)

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Saya faham bahawa segala rahsia rasmi dan suratan rasmi yang saya peroleh semasa berurusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan, bertulis atau dengan cara elektronik kepada sesiapa jua dalam apa-apa bentuk, sama ada dalam masa atau selepas berurusan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis daripada pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila urusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia telah selesai.

Tandatangan :

Nama (huruf besar) : _____
No. Kad Pengenalan : _____
Jawatan : _____
Jabatan/Organisasi : _____
Tarikh : _____

Disaksikan oleh,

Tandatangan :

Nama (huruf besar) : _____
No. Kad Pengenalan : _____
Jawatan : _____
Jabatan/Organisasi : _____
Tarikh : _____

Cop Jabatan/Organisasi :

_____

SURAT PERAKUAN AKTA RAHSIA RASMI 1972 (TAMAT PERKHIDMATAN)

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN APABILA TAMAT KONTRAK PERKHIDMATAN DENGAN KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Dengan ini menjadi satu kesalahan di bawah Akta tersebut bagi saya menyampaikan dengan tiada kebenaran apa-apa rahsia rasmi atau suratan rasmi kepada mana-mana orang lain, sama ada atau tidak orang itu memegang jawatan dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau mana-mana Kerajaan Malaysia, dan sama ada di Malaysia atau di negara luar, sebelum dan selepas saya tamat kontrak perkhidmatan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia.

Saya mengaku bahawa tidak lagi ada dalam milik saya atau kawalan saya apa-apa perkataan kod rasmi, isyarat timbal, atau kata laluan rasmi yang rahsia, atau apa-apa benda, suratan atau maklumat, anak kunci, lencana, alat meteri, atau cap bagi atau yang dipunyai, atau diguna, dibuat atau diadakan oleh mana-mana jabatan Kerajaan atau oleh mana-mana pihak berkuasa diplomat yang dilantik oleh atau yang bertindak di bawah kuasa Kerajaan Malaysia atau Seri Paduka Baginda yang tidak dibenarkan berada dalam milikan atau kawalan saya.

Tandatangan :

Nama (huruf besar) : _____
No. Kad Pengenalan : _____
Jawatan : _____
Jabatan/Organisasi : _____
Tarikh : _____

Disaksikan oleh,

Tandatangan :

Nama (huruf besar) : _____
No. Kad Pengenalan : _____
Jawatan : _____
Jabatan/Organisasi : _____
Tarikh : _____

Cop Jabatan/Organisasi :

_____

Lampiran 4

RINGKASAN PROSES PELAPORAN INSIDEN KESELAMATAN ICT MSWP

Pelaporan Kepada NACSA

Insiden Keselamatan Siber:

i. Penafian Perkhidmatan (DDoS)
ii. Pencerobohan (*Intrusin*)
iii. *Cubaan Pencerobohan* (*Intrusion Attempts*)
iv. Jangkitan Perisian Merbahaya
v. Penghosan Perisian Merbahaya (*Malware Hosting*)
vi. Potensi Serangan (Potential Attack)
vii. Pemalsuan (*Forgery*)
viii. Spam
ix. Ancaman *(Harrassment/Threat)*

Tindakan:

i. Memaklumkan kepada ICTSO.
ii. ICTSO memaklumkan kepada NACSA.
iii. Tindakan oleh KHS, ICTSO, CERTMSWP, CERT JPM (sekiranya perlu) untuk siasatan, langkah susulan dan tindakan pengukuhan.

Pelaporan Kepada Fasiliti/JPM

Insiden Keselamatan Bukan Siber:

i. Pelanggaran Dasar
ii. Kehilangan Fizikal
ii. Kelemahan Perisian

Tindakan:

i. Memaklumkan kepada KHS/Ketua Bahagian/Ketua Seksyen dan ICTSO dengan segera.
ii. Mengisi Borang Pelaporan Insiden Keselamatan MSWP.
iii. Borang yang lengkap diisi dihantar kepada CERTMSWP, dan diemelkan kepada CERT JPM.
iv. Tindakan oleh CERTMSWP untuk siasatan, langkah susulan dan tindakan pengukuhan.

Lampiran 5

SENARAI PERUNDANGAN DAN PERATURAN

Bil.	Nama Perundangan/Peraturan
1.	Akta Tandatangan Digital 1997;
2.	Akta Rahsia Rasmi 1972;
3.	Akta Jenayah Komputer 1997;
4.	Akta Hak cipta (Pindaan) Tahun 1997;
5.	Akta Komunikasi dan Multimedia 1998;
6.	Akta 709 – Akta Perlindungan Data Peribadi 2010;
7.	Akta 658 – Akta Perdagangan Elektronik 2006;
8.	Akta 629 – Akta Arkib Negara 2003;
9.	Akta 606 – Akta Cakera Optik 2000;
10.	Akta 298 – Kawasan Larangan Tempat Larangan 1959;
11.	Akta 56 – Akta Keterangan 1950;
12.	Arahan Keselamatan;
13.	Arahan Perbendaharaan;
14.	Arahan Teknologi Maklumat 2007
15.	Arahan 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara;
16.	Arahan 24 – Dasar dan Mekanisme Pengurusan Krisis Siber Negara;
17.	Dasar Pengurusan Rekod dan Arkib Elektronik
18.	Etika Penggunaan E-mel dan Internet MSWP;
19.	Garis Panduan Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam (MAMPU);
20.	Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013;
21.	Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam 04/2006;
22.	Garis Panduan Pengurusan Rekod;
23.	Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi;
24.	Guideline to Determine Information Security Professionals Requirement for the CNII Agencies /Organisations;
25.	National Cyber Security Policy (NCSP);
26.	Panduan Pelaksanaan Audit ISMS Sektor Awam;
27.	Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”;

Bil.	Nama Perundangan/Peraturan
28.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 bertajuk "Pengurusan Laman Web Agensi Sektor Awam";
29.	Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)";
30.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan";
31.	Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 bertajuk "Panduan Pengurusan Pejabat bertarikh 30 April 2007";
32.	Pekeliling Transformasi Pentadbiran Awam Bilangan 3 Tahun 2017: Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan;
33.	Pekeliling Am Bilangan 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam;
34.	Pekeliling Perbendaharaan Malaysia PK 2/2013 – Kaedah Perolehan Kerajaan;
35.	Perintah-Perintah Am;
36.	Pelan Pengurusan Pemulihan Bencana MSWP;
37.	PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2011 (Pindaan Kedua);
38.	Polisi Keselamatan Siber MAMPU
39.	Prosedur Pengurusan Pelaporan Dan Pengendalian Insiden Keselamatan ICT MSWP;
40.	1Pekeliling Perbendaharaan AM 2 Tahun 2018: Tatacara Pengurusan Aset Alih Kerajaan;
41.	Rancangan Malaysia Ke-11;
42.	Surat Arahan KPPA Tindakan Ke Atas Penjawat Awam Yang Mendedahkan/Membocorkan Dokumen/Maklumat Terperingkat Kerajaan bertarikh 28 Januari 2015;
43.	Surat Arahan MAMPU.702-1/1/7 Jld. 3 (48) bertarikh 23 Mac 2009 bertajuk "Pengaktifan Fail Log *Server* Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan";
44.	Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk "Penggunaan Media Jaringan Sosial di Sektor Awam";
45.	Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi *Digital Document Management System* (DDMS) Sektor Awam yang bertarikh 26 Januari 2015;
46.	Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat yang bertarikh 24 November 2010;
47.	Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;
48.	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
49.	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
50.	Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk MemperkukuhkanKeselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) Di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
51.	Surat Aku Janji;

Bil.	Nama Perundangan/Peraturan
52.	Surat Pekeliling Am Bilangan 3 Tahun 2015 bertajuk "Garis Panduan Permohonan Kelulusan Teknikal Dan Pemantauan Projek ICT Agensi Sektor Awam";
53.	Surat Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2015 bertajuk "Panduan Pelaksanaan Program Turun Padang Sektor Awam";
54.	Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam";
55.	Surat Pekeliling Am Bilangan 4 Tahun 2006 bertajuk "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam";
56.	Surat Pekeliling Perbendaharaan – Garis Panduan Mengenai Pengurusan Perolehan *Information Telecommunication Technology* ICT Kerajaan SPP 3/2013;
57.	Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam;
58.	Surat Pekeliling Am Bilangan 2/1987 – Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987);
59.	Surat Pekeliling Am Bilangan 4 Tahun 2006 Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) versi 1.0 April 2016;