KEMENTERIAN PELANCONGAN,
SENI, DAN BUDAYA

POLISI KESELAMATAN SIBER

VERSI 1.0

KEMENTERIAN PELANCONGAN SENI DAN BUDAYA

ISI KANDUNGAN

TAKRIFAN 2

OBJEKTIF 10

TUJUAN 10

LATAR BELAKANG 10

ASET ICT MOTAC 11

PRINSIP KESELAMATAN 15

TEKNOLOGI 16

PROSES 20

MANUSIA 23

PENYATAAN POLISI KESELAMATAN SIBER 24

BIDANG 01 : POLISI KESELAMATAN MAKLUMAT 26

1.1 HALA TUJU PENGURUSAN UNTUK KESELAMATAN MAKLUMAT 26

1.1.1 POLISI KESELAMATAN MAKLUMAT 26

1.1.2 KAJIAN SEMULA POLISI UNTUK KESELAMATAN MAKLUMAT 26

BIDANG 02 : PERANCANGAN BAGI KESELAMATAN ORGANISASI 27

2.1 PERANCANGAN DALAMAN 27

2.1.1 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT 27

2.1.2 PENGASINGAN TUGAS 32

2.1.3 HUBUNGAN DENGAN PIHAK BERKUASA 32

2.1.4 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS 33

2.1.5 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK 33

2.2 PERANTI MUDAH ALIH, TELEKERJA DAN MESYUARAT DALAM TALIAN 34

2.2.1 POLISI PERANTI MUDAH ALIH 34

2.2.2 TELEKERJA 34

2.2.3 MESYUARAT DALAM TALIAN 35

BIDANG 03 : KESELAMATAN SUMBER MANUSIA 35

3.1 SEBELUM PERKHIDMATAN 35

3.1.1 TAPISAN KESELAMATAN 35

3.1.2 TERMA DAN SYARAT PERKHIDMATAN 36

3.2 DALAM TEMPOH PERKHIDMATAN 36

3.2.1 TANGGUNGJAWAB PENGURUSAN 36

3.2.2 KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT 37
3.2.3 PROSES TATATERTIB 37
3.3 PENAMATAN DAN PERTUKARAN PERKHIDMATAN 38
3.3.1 PENAMATAN ATAU PERTUKARAN TANGGUNG JAWAB PERKHIDMATAN 38

BIDANG 04 : PENGURUSAN ASET 39
4.1 TANGGUNGJAWAB TERHADAP ASET 39
4.1.1 INVENTORI ASET 39
4.1.2 PEMILIKAN ASET 39
4.1.3 PENGGUNAAN ASET YANG DIBENARKAN 40
4.1.4 PEMULANGAN ASET 40
4.2 PENGELASAN MAKLUMAT (*INFORMATION CLASSIFICATION*) 40
4.2.1 PENGELASAN MAKLUMAT (*INFORMATION CLASSIFICATION*) 40
4.2.2 PELABELAN MAKLUMAT 41
4.2.3 PENGENDALIAN ASET 41
4.3 PENGENDALIAN MEDIA 41
4.3.1 PENGURUSAN MEDIA BOLEH ALIH 42
4.3.2 PELUPUSAN MEDIA 42
4.3.3 PEMINDAHAN MEDIA FIZIKAL 42

BIDANG 05 : KAWALAN AKSES 43
5.1 KAWALAN AKSES 43
5.1.1 POLISI KAWALAN AKSES 43
5.1.2 CAPAIAN KEPADA RANGKAIAN DAN PERKHIDMATAN RANGKAIAN 44
5.2 PENGURUSAN AKSES PENGGUNA 44
5.2.1 PENDAFTARAN DAN PEMBATALAN PENGGUNA 44
5.2.2 PERUNTUKAN AKSES PENGGUNA 45
5.2.3 PENGURUSAN HAK AKSES ISTIMEWA 45
5.2.4 KAJIAN SEMULA HAK AKSES PENGGUNA 45
5.2.5 PEMBATALAN ATAU PELARASAN HAK AKSES 45
5.3 TANGGUNGJAWAB PENGGUNA 45
5.3.1 PENGGUNAAN MAKLUMAT PENGESAHAN RAHSIA 46
5.3.2 PENGGUNAAN MAKLUMAT PENGESAHAN RAHSIA (*AUTHENTICATION*) 46
5.4 KAWALAN AKSES SISTEM DAN APLIKASI 46
5.4.1 SEKATAN AKSES MAKLUMAT 47
5.4.2 PROSEDUR LOG MASUK YANG SELAMAT (*SECURE LOG-ON*) 47
5.4.3 SISTEM PENGURUSAN KATA LALUAN 47

5.4.4 PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA 48
5.4.5 KAWALAN AKSES KEPADA KOD SUMBER PROGRAM 48

BIDANG 06 : KRIPTOGRAFI 49
6.1 KAWALAN KRIPTOGRAFI 49
6.1.1 POLISI PENGGUNAAN KAWALAN KRIPTOGRAFI 49
6.1.2 PENGURUSAN KUNCI AWAM 49

BIDANG 07 : KESELAMATAN FIZIKAL DAN PERSEKITARAN 50
7.1 KAWASAN SELAMAT 50
7.1.1 PERIMETER KESELAMATAN FIZIKAL 50
7.1.2 KAWALAN KEMASUKAN FIZIKAL 51
7.1.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN 51
7.1.4 PERLINDUNGAN DARIPADA ANCAMAN LUAR DAN PERSEKITARAN 51
7.1.5 BEKERJA DI KAWASAN SELAMAT 52
7.1.6 KAWASAN PENYERAHAN DAN PEMUNGGAHAN 53
7.2 PERALATAN ICT 53
7.2.1 PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT 53
7.2.2 UTILITI SOKONGAN 55
7.2.3 KESELAMATAN KABEL 55
7.2.4 PENYELENGGARAAN PERALATAN 56
7.2.5 PENGALIHAN ASET 56
7.2.6 KESELAMATAN PERALATAN DAN ASET DI LUAR PREMIS 57
7.2.7 PELUPUSAN PERALATAN YANG SELAMAT ATAU PENGGUNAAN SEMULA 57
7.2.8 PERALATAN PENGGUNA TANPA KAWALAN 59
7.2.9 POLISI MEJA KOSONG DAN SKRIN KOSONG 59

BIDANG 08 : KESELAMATAN OPERASI 60
8.1 PROSEDUR DAN TANGGUNGJAWAB OPERASI 60
8.1.1 PROSEDUR OPERASI YANG DIDOKUMENKAN 60
8.1.2 PENGURUSAN PERUBAHAN 60
8.1.3 PENGURUSAN KAPASITI 61
8.1.4 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN OPERASI 61
8.2 PERLINDUNGAN DARIPADA PERISIAN HASAD (*MALWARE*) 61
8.2.1 KAWALAN DARIPADA PERISIAN HASAD (*MALWARE*) 62
8.3 SANDARAN (*BACKUP*) 62

8.4 PENGELOGAN DAN PEMANTAUAN (*LOGGING AND MONITORING*) 63
8.4.1 PENGELOGAN KEJADIAN (*EVENT LOGGING*) 63
8.5 KAWALAN PEMASANGAN PERISIAN 64
8.5.1 PEMASANGAN PERISIAN PADA SISTEM PENGOPERASIAN 83
8.6 PENGURUSAN KERENTANAN TEKNIKAL 64
8.6.1 PENGURUSAN KERENTANAN TEKNIKAL 64
8.6.2 SEKATAN KE ATAS PEMASANGAN PERISIAN 65
8.7 JEJAK AUDIT 65
8.7.1 KAWALAN JEJAK AUDIT 65

BIDANG 09 : KESELAMATAN KOMUNIKASI 66

9.1 PENGURUSAN KESELAMATAN RANGKAIAN 66
9.1.1 KAWALAN RANGKAIAN 66
9.1.2 KESELAMATAN PERKHIDMATAN RANGKAIAN 67
9.1.3 PENGASINGAN DALAM RANGKAIAN 67
9.2 PEMINDAHAN DATA DAN MAKLUMAT 67
9.2.1 PROSEDUR PEMINDAHAN DATA DAN MAKLUMAT 68
9.2.2 PERJANJIAN MENGENAI PEMINDAHAN DATA DAN MAKLUMAT 68
9.2.3 PESANAN ELEKTRONIK (E-MEL) 68
9.2.4 PENGURUSAN PORTAL DAN MEDIA SOSIAL 69

BIDANG 10 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM 70

10.1 KEPERLUAN KESELAMATAN SISTEM MAKLUMAT 70
10.1.1 ANALISIS DAN SPESIFIKASI KEPERLUAN KESELAMATAN MAKLUMAT 70
10.1.2 PERLINDUNGAN PERKHIDMATAN APLIKASI YANG MENGGUNAKAN RANGKAIAN AWAM 70
10.1.3 MELINDUNGI TRANSAKSI PERKHIDMATAN APLIKASI 71
10.2 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN 71
10.2.1 POLISI KESELAMATAN DALAM PEMBANGUNAN SISTEM 71
10.2.2 PROSEDUR KAWALAN PERUBAHAN SISTEM 71
10.2.3 SEMAKAN TEKNIKAL APLIKASI SELEPAS PERUBAHAN PLATFORM 72
10.2.4 KAWALAN TERHADAP PERUBAHAN KEPADA PERISIAN 72
10.2.5 PRINSIP KEJURUTERAAN SISTEM YANG SELAMAT 72
10.2.6 PERSEKITARAN PEMBANGUNAN YANG SELAMAT 73
10.2.7 PEMBANGUNAN OLEH KHIDMAT LUARAN 73
10.2.8 PENGUJIAN KESELAMATAN SISTEM 74

10.3 DATA UJIAN 74
10.3.1 PERLINDUNGAN DATA UJIAN 74

BIDANG 11 : HUBUNGAN PEMBEKAL 75
11.1 KESELAMATAN MAKLUMAT DALAM HUBUNGAN PEMBEKAL 75
11.1.2 KAWALAN KESELAMATAN MAKLUMAT MELALUI PERJANJIAN DENGAN PEMBEKAL 75
11.1.3 RANTAIAN BEKALAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI 75
11.2 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PEMBEKAL 76
11.2.1 PEMANTAUAN DAN PENILAIAN PERKHIDMATAN PEMBEKAL 76
11.2.2 MENGURUSKAN PERUBAHAN KEPADA PERKHIDMATAN PEMBEKAL 76

BIDANG 12 : PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT 77
12.1 PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT DAN PENAMBAHBAIKAN 77
12.1.1 TANGGUNGJAWAB DAN PROSEDUR 77
12.1.2 PELAPORAN KEJADIAN KESELAMATAN MAKLUMAT 77
12.1.3 PELAPORAN KELEMAHAN KESELAMATAN MAKLUMAT 78
12.1.4 PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT 79
12.1.5 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT 79
12.1.6 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT 80
12.1.7 PENGUMPULAN BAHAN BUKTI 80

BIDANG 13 : ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN 81
13.1 KESINAMBUNGAN KESELAMATAN MAKLUMAT 81
13.1.1 PERANCANGAN KESINAMBUNGAN KESELAMATAN MAKLUMAT 81
13.1.2 PELAKSANAAN KESINAMBUNGAN KESELAMATAN MAKLUMAT 82
13.1.3 MENENTUSAHKAN, MENGKAJI SEMULA DAN MENILAI KESINAMBUNGAN KESELAMATAN MAKLUMAT 83
13.2 LEWAHAN (*REDUNDANCY*) 83
13.2.1 KETERSEDIAAN KEMUDAHAN PEMPROSESAN MAKLUMAT 83

BIDANG 14 : PEMATUHAN 84
14.1 PEMATUHAN TERHADAP KEPERLUAN PERUNDANGAN DAN KONTRAK 84
14.1.1 PENGENALPASTIAN KEPERLUAN UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI 84
14.1.2 HAK HARTA INTELEK 84

14.1.3 PERLINDUNGAN REKOD 84
14.1.4 PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI 85
14.1.5 PERATURAN KAWALAN KRIPTOGRAFI 85
14.2 KAJIAN SEMULA KESELAMATAN MAKLUMAT 85
14.2.1 KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI 86
14.2.2 PEMATUHAN POLISI DAN STANDARD KESELAMATAN 86
14.2.3 KAJIAN SEMULA PEMATUHAN TEKNIKAL 86

LAMPIRAN 1 87
LAMPIRAN 2 90

SEJARAH DOKUMEN

NAMA DOKUMEN	VERSI	KELULUSAN	TARIKH KUAT KUASA
Dasar Keselamatan ICT	3.0	MESYUARAT JPICT BIL. 1/2015	20 Mei 2015
Polisi Keselamatan Siber	1.0	MESYUARAT JPICT BIL. 4/2023	06 Okt 2023

TAKRIFAN

Bagi maksud menjelaskan istilah-istilah yang digunapakai di dalam polisi ini adalah seperti berikut:

1	Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
2	Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
3	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
4	*Backup* (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat.
5	Baki risiko	Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan.
6	*Bandwidth*	Jalur lebar. Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
7	BCP/PKP	*Business Continuity Planning*/Pelan Kesinambungan Perkhidmatan
8	CCTV	*Closed-Circuit Television System* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
9	CSIRT MOTAC	*Cyber Security Incident Response Team* (CSIRT) atau Pasukan Tindakan Kecemasan Siber MOTAC.

10	CIA	*Confidentiality, Integrity and Availability.*
11	CGSO	*Chief Government Security Officer* Ketua Pegawai Keselamatan Kerajaan.
12	CDO	*Chief Digital Officer* Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan maklumat bagi menyokong arah tuju sesebuah organisasi.
13	*Clear Desk* dan *Clear Screen*	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
14	*Data-at-rest* (data-dalam-simpanan)	*Refers to data that is being stored in stable destination system. Data at rest is frequently defined as data that is not in use or is not traveling to system endpoints, such as mobile devices or workstations.*
15	*Data-in-motion* (data-dalam pergerakan)	*Refers to a stream of data moving through any kind of network. It represents data which is being transferred or moved.*
16	*Data-in-use* (data-dalam-penggunaan)	*Refers to data that is not simply being passively stored in a stable destination, such as a central data warehouse, but is working its way through other parts of an IT architecture.*
17	*Denial of service*	Halangan pemberian perkhidmatan.
18	*Defence-in-depth*	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisma lapisan pertahanan untuk melindungi data dan maklumat.
19	*Downloading*	Aktiviti muat turun sesuatu perisian.
20	*Encryption*	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.

21	*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.
22	*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*).
23	*Hard disk*	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
24	*Hub*	*Hub* merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu port kepada semua port yang lain.
25	ICT	*Information and Communication Technology*. Teknologi Maklumat dan Komunikasi.
26	ICTSO	*ICT Security Officer* (Pegawai Keselamatan ICT). Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
27	Impak teknikal	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.
28	Impak fungsi MOTAC	Melibatkan perkara-perkara yang menjejaskan dari segi kewangan, reputasi, ketidakpatuhan dan perlanggaran privasi.
29	Insiden keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
30	Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.

31	*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.
32	Intranet	Rangkaian dalaman yang dimiliki oleh MOTAC atau sesebuah organisasi dan hanya boleh dicapai oleh kakitangan yang diberi kebenaran sahaja.
33	*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.
34	*Intrusion Prevention System (IPS)*	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contoh: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
35	ISDN	*Integrated Services Digital Networks* Menggunakan isyarat digital pada talian telefon analog yang sedia ada.
36	JPICT	Jawatankuasa Pemandu ICT
37	Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman dari pihak luar atau apa-apa kemungkinan yang boleh menjejaskan kelancaran sistem.
38	Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran Keselamatan.

39	Kriptografi	Kaedah untuk menukar data dan maklumat biasa (*standard format*) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
40	LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
41	*Lock*	Mengunci komputer
42	*Logout*	Log keluar daripada sistem komputer. Keluar daripada sesuatu sistem atau aplikasi komputer.
43	*Malicious Code*	Kod hasad. Perkakasan atau perisian yang telah dimasukan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan *virus, trojan horse, worm, spyware* dan sebagainya.
44	MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia.
45	*Mobile Code*	*Mobile code* merupakan suatu perisian yang boleh dipindahkan di antara komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh *Java Applet, ActiveX* dan sebagainya pada pelayar internet.
46	*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.
47	MOTAC	Kementerian Pelancongan, Seni dan Budaya.
48	*Outsource*	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.

49	Pegawai Pengelas	Pegawai yang bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
50	Pembekal	Pembekal adalah syarikat yang dilantik Kerajaan untuk membekalkan barangan atau perkhidmatan ICT kepada MOTAC.
51	Pengguna	Merujuk warga MOTAC, Jabatan atau Agensi di bawah MOTAC, pembekal dan pihak-pihak lain yang diberi kebenaran menggunakan perkhidmatan ICT.
52	Pengolahan Risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko.
53	Perisian Aplikasi	Merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* atau pun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau MOTAC.
54	Program Utiliti	Perisian aplikasi khas yang mempunyai fungsi atau penggunaan untuk dapat membantu dalam proses analisis, mengkonfigurasi, dan mengoptimumkan dalam melaksanakan penyelenggaraan komputer.
55	*Rollback* (undur)	Pengembalian pangkalan data atau program kepada keadaan stabil sebelum sesuatu ralat berlaku.
56	*Router*	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian internet.
57	Ruang Siber	Sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem tersebut secara fizikal atau maya serta persekitaran fizikal sistem-sistem tersebut dan semua aset yang berkaitan dengan ICT.

58	*Screen saver*	Imej yang akan diaktifkan pada sistem/komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
59	*Server*	Pelayan komputer.
60	*Source Code*	Kod sumber atau kod program (biasanya hanya dipanggil sumber atau kod) merujuk kepada sebarang siri pernyataan yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia.
61	SUB	Setiausaha Bahagian
62	*Switch*	Switch merupakan gabungan *hub* dan *bridge* untuk segmentasi rangkaian. Kegunaan *switch* dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu sistem penghantaran dengan mengurangkan perlanggaran yang berlaku.
63	*Threat*	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
64	*Uninterruptible Power Supply* (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
65	*Video Conference*	Persidangan video. Persidangan/mesyuarat/perbincangan secara maya di mana peserta yang berada di lokasi berbeza boleh berkomunikasi sesama sendiri melalui audio dan video.
66	*Video Streaming*	Teknologi menghantar fail audio dan video secara berterusan melalui Internet.
67	*Virus*	Aturcara yang bertujuan merosakkan data atau sistem aplikasi.
68	*WAN*	*Wide Area Network*. Rangkaian yang merangkumi kawasan yang luas.

69	Warga MOTAC	Kakitangan Kerajaan yang berkhidmat di MOTAC, Jabatan dan Agensi di bawahnya, sama ada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan ICT Kementerian.
70	*Wireless LAN*	Jaringan komputer yang terhubung tanpa melalui kabel.
71	*Worm*	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri. Ia biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.

01

TUJUAN

Polisi Keselamatan Siber (PKS), Kementerian Pelancongan, Seni dan Budaya (MOTAC) ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC dalam melindungi maklumat di ruang siber.

02

LATAR BELAKANG

Polisi ini dibangunkan untuk menjamin kesinambungan urusan MOTAC dengan meminimumkan kesan insiden keselamatan ICT. Polisi ini akan memudahkan perkongsian maklumat sesuai dengan keperluan operasi MOTAC bagi memastikan semua maklumat dilindungi

03

OBJEKTIF

Objektif utama Polisi Keselamatan Siber ini dibangunkan adalah seperti berikut:

i. Menerangkan kepada semua pengguna merangkumi warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber;

ii. Memastikan keselamatan penyampaian perkhidmatan MOTAC di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;

iii. Memastikan kelancaran operasi MOTAC dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

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

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

ASET ICT MOTAC

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

i. Maklumat

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

a) Maklumat Rahsia Rasmi

Di bawah Akta Rahsia Rasmi 1972 [Akta 88], maksud Maklumat Rahsia Rasmi ialah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 [Akta 88] dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuk apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.

b) Maklumat Rasmi

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

c) Maklumat Pengenalan Peribadi (*Personally Identifiable Information* (PII))

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

d) Data Terbuka

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

ii. Aliran data

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

a) Saluran komunikasi dan aliran data antara sistem di MOTAC;
b) Saluran komunikasi dan aliran data ke sistem luar; dan
c) Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

iii. Platform Aplikasi dan Perisian

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

iv. Peranti Fizikal dan Sistem

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

a) Pelayan;
b) Peranti/ Peralatan Rangkaian;
c) Komputer Peribadi/ Komputer Riba;
d) Telefon/ Peranti Pintar;
e) Media Storan;
f) Peranti dengan sambungan ke rangkaian, contohnya pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV);
g) Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi Kerajaan; dan
h) Peranti pengesahan (*authentication devices*), contohnya token keselamatan, *dongle* dan alat pengimbas biometrik.

v. Sistem Luaran

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

vi. Sumber Luaran

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

a) Perisian Sebagai Satu Perkhidmatan (*Software as a Service atau SaaS*);
b) Platform Sebagai Satu Perkhidmatan (*Platform as a Service atau PaaS*);
c) Infrastruktur Sebagai Satu Perkhidmatan (*Infrastructure as a Service atau IaaS*);
d) Storan Pengkomputeran Awan; dan
e) Pemantauan Keselamatan.

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

PENILAIAN RISIKO KESELAMATAN ICT

5. MOTAC hendaklah mengenal pasti risiko yang berkaitan dengan maklumat yang terlibat. Risiko ialah kebarangkalian MOTAC tidak dapat melaksanakan fungsi MOTAC dengan baik. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber MOTAC.

6. Penilaian risiko hendaklah dilaksanakan secara berkala atau apabila berlaku sebarang perubahan kepada persekitaran ruang siber MOTAC.

7. Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

i. Kerentanan *(Vulnerability)*

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

ii. Ancaman

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

iii. Impak

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

iv. Tahap Risiko

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

v. Penguraian Risiko

a) Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko

perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya.

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

1) **Teknologi**

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

2) **Proses**

Rekayasa semula (*re-engineering*) proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

3) **Manusia**

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

vi. Pengurusan Risiko

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

a) Mengenal pasti kerentanan;

b) Mengenal pasti ancaman;

c) Menilai risiko;

d) Menentukan penguraian risiko;

e) Memantau keberkesanan penguraian risiko; dan

f) Memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

PRINSIP KESELAMATAN

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

i. Prinsip "Perlu-Tahu"

MOTAC hendaklah melaksanakan mekanisme bagi memberikan kebenaran kepada capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah berdasarkan prinsip "Perlu-Tahu" yang membenarkan capaian maklumat yang diperlukan untuk melaksanakan tugasnya sahaja. Bagi capaian spesifik maklumat Rahsia Rasmi, penggunaan yang dibenarkan hendaklah dihadkan kepada masa, lokasi, peranan dan fungsi pengguna tersebut.

ii. Hak Keistimewaan Minimum

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

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

iii. Pengasingan Tugas

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

iv. Kawalan Capaian Berdasarkan Peranan

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

v. Peminimuman Data

MOTAC hendaklah mengamalkan prinsip peminimuman data yang menghadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

TEKNOLOGI

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

i. Peringkat Pemprosesan Data

a) Data-dalam-simpanan

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

2) Maklumat Rahsia Rasmi, Maklumat Rasmi dan Maklumat Pengenalan Peribadi (PII) perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

b) Data-dalam-pergerakan

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

c) Data-dalam-penggunaan

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

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

d) Perlindungan Ketirisan Data

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

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

ii. Elemen Dalam Persekitaran Pengkomputeran

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

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

Setiap projek ICT hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan seperti di bawah:

a) Peranti Pengkomputeran Peribadi

1) Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh pengguna untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja, telefon pintar, tablet dan peranti storan.

2) Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada MOTAC. Walau bagaimanapun, peranti pengkomputeran peribadi milik persendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk

ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

a) Peranti Rangkaian

1) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti *switch*, *router*, *firewall*, *Virtual Private Network* (VPN) dan kabel.

2) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan dan data-dalam-simpanan bagi menghalang ketirisan data.

b) Aplikasi

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

2) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan dan data-dalam-simpanan bagi menghalang ketirisan data.

c) Pelayan

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

2) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan dan data-dalam-simpanan bagi menghalang ketirisan data.

d) Persekitaran Fizikal

1) Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

2) MOTAC hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan

Kerajaan Malaysia untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

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

2) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan dan data-dalam-simpanan bagi menghalang ketirisan data.

e) **Pengkomputeran Awan**

1) Pengkomputeran awan merujuk lokasi yang menempatkan sistem ICT menggunakan perkhidmatan pengkomputeran awan yang disediakan melalui internet oleh pihak ketiga dikenali sebagai Penyedia Perkhidmatan Awan (*Cloud Service Provider* (CSP)).

2) MAMPU dalam persekitaran yang terkawal, selamat, berasaskan standard dan amalan terbaik global telah menyediakan perkhidmatan pengkomputeran awan di Pusat Data Sektor Awam (PDSA) kepada Agensi Sektor Awam yang dikenali sebagai perkhidmatan MyGovCloud@PDSA.

3) Pelaksanaan projek ICT hendaklah menggunakan pengkomputeran awan dengan memberikan keutamaan kepada penggunaan perkhidmatan MyGovCloud@PDSA terutamanya yang melibatkan aplikasi kritikal kerajaan.

4) MOTAC hendaklah merujuk kepada MAMPU untuk mendapatkan nasihat mengenai perkhidmatan pengkomputeran awan yang akan dilaksanakan dan mematuhi polisi yang digariskan.

PROSES

10. MOTAC hendaklah melindungi keselamatan ICT dengan melaksanakan perkara-perkara berikut:

i. Konfigurasi Asas

a) Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan.

b) Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

ii. Kawalan Perubahan Konfigurasi

a) Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.

b) Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.

c) Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

iii. Sandaran dan Pemulihan (*Backup and Restore*)

a) Sandaran dan pemulihan hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa untuk memastikan bahawa proses kerja boleh dilaksanakan.

b) Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

iv. Kitaran Pengurusan Aset

a) Pindah

1) Pemindahan hak milik aset berlaku dalam keadaan berikut:

i) Warga MOTAC meninggalkan agensi disebabkan oleh persaraan, perletakan jawatan atau penugasan semula;

ii) Aset yang dikongsi untuk kegunaan sementara;

iii) Pemberian aset kepada agensi lain; dan

iv) Aset dikembalikan setelah tamat tempoh sewaan.

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

b) Pelupusan

1) Pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya.

2) Berdasarkan keputusan CGSO, pelupusan perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara 2003 (Akta 629) dan Warta Kerajaan P.U.(A)377. Peraturan-Peraturan Arkib Negara (Penetapan Borang-Borang bagi Pelupusan Rekod Awam) 2008.

3) Pelupusan boleh dalam bentuk pemusnahan fizikal dan/atau sanitasi data.

4) Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa.

c) Kitaran Hayat

1) Kitaran hayat data hendaklah diuruskan mengikut Akta 629.

2) Akta 629 memberikan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

MANUSIA

11. Warga MOTAC, pembekal dan pihak-pihak yang berkepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

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

i. Kompetensi Pengguna

a) Kompetensi pengguna termasuk:

1) Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan ICT dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan ICT.

2) Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga MOTAC berhubung alat-alat keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.

b) Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian mendalam.

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

i. Kompetensi Pelaksana

a) Warga MOTAC yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

b) ICTSO hendaklah memenuhi syarat-syarat berikut:

1) Mempunyai pengetahuan asas dalam keselamatan ICT;

2) Mempunyai pengalaman dalam bidang keselamatan ICT; dan

3) Telah menjalani tapisan keselamatan daripada agensi yang diberi kuasa.

c) ICTSO yang dilantik oleh MOTAC hendaklah memenuhi keperluan kompetensi di atas. ICTSO bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan ICT di MOTAC.

ii. Peranan Pengguna

a) Peranan pengguna hendaklah diberi berdasarkan keperluan dan bidang tugas pengguna.

b) Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.

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

d) Warga MOTAC yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT MOTAC dikembalikan sekiranya berlaku perubahan peranan.

e) Warga MOTAC yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset MOTAC yang berkaitan seperti tersenarai dalam senarai aset dalam Nota Serah Tugas.

f) Warga MOTAC lain yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset MOTAC dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh MOTAC.

PENYATAAN POLISI KESELAMATAN SIBER

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

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

i. Kerahsiaan

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

ii. Integriti

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

iii. Tidak Boleh Disangkal

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

iv. Kesahihan

Data dan maklumat hendaklah dipastikan kesahihannya.

v. Ketersediaan

Data dan maklumat hendaklah boleh diakses pada bila-bila masa

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

16. Sebanyak 14 bidang keselamatan yang terlibat di dalam Polisi Keselamatan

BIDANG 01 :
POLISI KESELAMATAN MAKLUMAT

PERKARA	PERANAN
1.1 HALA TUJU PENGURUSAN UNTUK KESELAMATAN MAKLUMAT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan MOTAC dan perundangan yang berkaitan.	
Pelaksanaan polisi ini akan dijalankan oleh Ketua Jabatan MOTAC dengan disokong oleh JPICT yang terdiri daripada CDO, ICTSO, SUB/Pengarah Bahagian dan ahli-ahli yang dilantik oleh Ketua Jabatan MOTAC. Polisi Keselamatan Siber mestilah dipatuhi oleh semua warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC. Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan MOTAC kepada warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC.	Ketua Setiausaha/ CDO/ICTSO/SUB/ Pengarah Bahagian/ JPICT
1.1.2 KAJIAN SEMULA POLISI UNTUK KESELAMATAN MAKLUMAT	
Polisi ini perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan dan polisi Kerajaan. Berikut ialah prosedur yang berkaitan dengan kajian semula Polisi Keselamatan Siber MOTAC: i. Mengenal pasti dan menentukan perubahan yang diperlukan; ii. Mengemukakan cadangan pindaan untuk tindakan dan pertimbangan kepada JPICT bagi tujuan pengesahan; iii. Memaklumkan pindaan yang telah disahkan oleh JPICT kepada warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC; dan iv. Polisi ini hendaklah dikaji semula setiap **TIGA (3) TAHUN SEKALI** atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	CDO/ICTSO/JPICT

BIDANG 02 :
PERANCANGAN BAGI KESELAMATAN ORGANISASI

PERKARA	PERANAN
2.1 PERANCANGAN DALAMAN	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber MOTAC.	
2.1.1 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT	
i. Memastikan penguatkuasaan pelaksanaan Polisi ini; ii. Memastikan warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini; iii. Memastikan semua keperluan MOTAC seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi; iv. Memastikan pengurusan risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Polisi ini; v. Melantik CDO dan ICTSO; dan vi. Mempengerusikan Mesyuarat JPICT.	KSU/Ketua Jabatan
Peranan dan tanggungjawab CDO adalah seperti berikut: i. Mewujud dan mengetuai pasukan penyelaras keselamatan ICT; ii. Membantu KSU dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan di dalam Polisi ini; iii. Memastikan kawalan keselamatan ICT MOTAC diseragam dan diselaraskan dengan sebaiknya; iv. Memastikan Pelan Strategik Pendigitalan MOTAC (PSPM) mengandungi aspek keselamatan ICT; dan v. Menyelaras pelaksanaan pelan latihan dan program kesedaran siber.	CDO

PERKARA	PERANAN
Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: i. Mengkaji dan menetapkan kawalan keselamatan siber agar ianya berselaras dengan keperluan MOTAC; ii. Menentukan kawalan capaian semua pengguna terhadap aset ICT; iii. Melaporkan ancaman atau insiden keselamatan ICT kepada ICTSO dan mengurus penyiasatan atau pemulihan insiden berkaitan; iv. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman atau insiden keselamatan ICT MOTAC; dan v. Mengkaji pembangunan dan pelaksanaan pelan latihan dan program kesedaran keselamatan ICT.	Pengurus ICT
Pentadbir Sistem ICT adalah terdiri seperti berikut: i. Pentadbir Keselamatan ICT ii. Pentadbir Rangkaian iii. Pentadbir Pusat Data iv. Pentadbir Sistem Aplikasi v. Pentadbir Portal vi. Pentadbir E-mel vii. Pegawai Aset ICT	Pentadbir Sistem ICT
i. Melaksanakan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini; ii. Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan ICT dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; iii. Melaporkan ancaman atau keselamatan ICT kepada Pengurus Keselamatan ICT dan seterusnya membantu dalam penyiasatan atau pemulihan; iv. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT; v. Melaporkan sebarang salah laku pengguna yang melanggar Polisi ini kepada Pengurus Keselamatan ICT; dan vi. Menyedia dan melaksanakan pelan latihan dan program kesedaran keselamatan ICT.	Pentadbir Keselamatan ICT

PERKARA	PERANAN
i. Memastikan kemudahan rangkaian beroperasi sepanjang masa; ii. Memastikan semua peralatan dan perisian rangkaian diselenggara dengan sempurna; iii. Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; iv. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; dan v. Memantau penggunaan rangkaian dan melaporkan kepada Pentadbir Keselamatan ICT sekiranya berlaku penyalahgunaan sumber rangkaian.	Pentadbir Rangkaian
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. Menjadual dan melaksanakan proses sandaran dan pemulihan (*Backup and Restore*) ke atas pangkalan data dan sistem secara berkala; iv. Memastikan pusat data sentiasa beroperasi mengikut polisi yang telah ditetapkan; dan v. Melaporkan sebarang pelanggaran keselamatan pusat data kepada Pentadbir Keselamatan ICT.	Pentadbir Pusat Data
i. Memastikan sistem aplikasi mempunyai kawalan capaian; ii. Memastikan data-data rahsia rasmi tidak boleh disalin atau dicetak oleh orang yang tidak berhak; iii. Memastikan reka bentuk sistem aplikasi dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; iv. Melaksanakan pemantauan dan penyelenggaraan terhadap sistem aplikasi dari semasa ke semasa; v. Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; dan vi. Melaporkan sebarang pelanggaran keselamatan sistem aplikasi kepada Pentadbir Keselamatan ICT.	Pentadbir Sistem Aplikasi

PERKARA	PERANAN
i. Memastikan portal mempunyai kawalan capaian; ii. Menerima kandungan portal yang telah disahkan kesahihan dan terkini daripada sumber yang sah; iii. Memastikan hanya maklumat data terbuka sahaja dipaparkan di portal; iv. Memastikan reka bentuk portal dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; v. Melaksanakan pemantauan dan penyelenggaraan terhadap portal dari semasa ke semasa; vi. Melaporkan sebarang pelanggaran keselamatan portal kepada Pentadbir Keselamatan ICT.	Pentadbir Portal
i. Melaksanakan proses pengurusan akaun e-mel mengikut prosedur MyGovUC oleh MAMPU; ii. Memastikan kemudahan capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi; dan iii. Melaporkan sebarang pelanggaran keselamatan e-mel kepada Pentadbir Keselamatan ICT.	Pentadbir E-mel
i. Memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan; ii. Memastikan penerimaan aset ICT Kerajaan dilaksanakan oleh pegawai yang dilantik oleh KSU/Ketua Jabatan; iii. Memastikan semua aset ICT Kerajaan yang diterima, didaftarkan menggunakan Sistem Pemantauan Pengurusan Aset (SPPA) mengikut tatacara pengurusan aset yang sedang berkuatkuasa; iv. Memastikan semua aset ICT Kerajaan yang dipinjam, direkodkan ke dalam Borang Permohonan Pergerakan/Pinjaman Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan secara bertulis daripada Ketua MOTAC/Pegawai Aset/ Pegawai-pegawai lain yang diberi kuasa oleh Ketua MOTAC; v. Memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/penggantian/naik taraf aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira;	Pegawai Aset ICT

PERKARA	PERANAN
vi. Memastikan semua aset ICT Kerajaan dilabel di tempat yang mudah dilihat dan sesuai pada aset berkenaan; vii. Memastikan setiap kerosakan aset ICT Kerajaan dilaporkan untuk tujuan penyelenggaraan; dan viii. Bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT Kerajaan; ix. Merancang, memantau dan memastikan pemeriksaan aset ICT Kerajaan dilaksanakan ke atas keseluruhan aset ICT Kerajaan sekurang-kurangnya sekali setahun; dan x. Memastikan setiap kes kehilangan aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur.	
Peranan dan tanggungjawab JPICT seperti yang terkandung dalam Surat Pekeliling Am Bil. 3 Tahun 2015 ialah merancang dan menentukan langkah-langkah keselamatan ICT. i. Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; ii. Merekod dan menjalankan siasatan awal insiden yang diterima; iii. Menangani tindak balas insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; iv. Menasihati Pentadbir Sistem ICT untuk mengambil tindakan pemulihan dan pengukuhan; dan v. Menyebarkan makluman berkaitan pengukuhan keselamatan siber kepada Pentadbir Sistem ICT.	JPICT CSIRT MOTAC

PERKARA	PERANAN
i. Membaca, memahami dan mematuhi Polisi ini; ii. Mengetahui dan memahami implikasi keselamatan ICT serta kesan daripada tindakannya; iii. Menjalani tapisan Keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumat rasmi terperingkat; iv. Mematuhi prinsip-prinsip keselamatan Polisi ini dan menjaga kerahsiaan maklumat Kerajaan; v. Melaksanakan langkah-langkah perlindungan seperti yang 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 maklumat; e. Mematuhi polisi, piawaian dan garis panduan keselamatan ICT yang ditetapkan; f. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan kawalan keselamatan ICT dari diketahui umum. vi. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada CSIRT MOTAC dengan segera; vii. Menghadiri program-program kesedaran mengenai keselamatan ICT; viii. Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini; dan ix. Menandatangani **Surat Akuan Pematuhan Polisi Keselamatan Siber MOTAC (LAMPIRAN 2).**	Pengguna

PERKARA	PERANAN
2.1.2 PENGASINGAN TUGAS	
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; ii. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; iii. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan aplikasi; dan iv. Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.	ICTSO/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT
2.1.3 HUBUNGAN DENGAN PIHAK BERKUASA	
Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: i. Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab MOTAC; ii. Mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang perlu dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia (PDRM) dan Suruhanjaya Komunikasi Dan Multimedia Malaysia (SKMM). Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan iii. Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.	CSIRT MOTAC/ Pengurusan Sumber Manusia

PERKARA	PERANAN
2.1.4 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS	
Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau pun forum bagi: i. Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat; ii. Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; iii. Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan iv. Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	Pentadbir Sistem ICT/ Pengguna
2.1.5 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK	
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek MOTAC; ii. Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; iii. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan; Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek MOTAC; iv. Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam Polisi Keselamatan Siber MOTAC. v. Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat.	Pentadbir Sistem ICT/ Pengguna

PERKARA	PERANAN
2.2 PERANTI MUDAH ALIH, TELEKERJA DAN MESYUARAT DALAM TALIAN	
Objektif: Memastikan keselamatan telekerja, mesyuarat dalam talian dan penggunaan peralatan mudah alih.	
2.2.1 POLISI PERANTI MUDAH ALIH	
Membangun serta menyebarkan polisi/arahan/peraturan/langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul berkaitan penggunaan peranti mudah alih.	ICTSO/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT
Meluluskan polisi/arahan/peraturan/langkah-langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada warga MOTAC.	JPICT
Perkara-perkara yang perlu dipatuhi: i. Pendaftaran ke atas peralatan mudah alih; ii. Keperluan ke atas perlindungan secara fizikal; iii. Kawalan ke atas pemasangan perisian peralatan mudah alih; iv. Kawalan ke atas versi dan *patches* perisian; v. Sekatan ke atas akses perkhidmatan maklumat secara dalam talian; vi. Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi; dan vii. Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.	Warga MOTAC

PERKARA	PERANAN
2.2.2 TELEKERJA	
i. Polisi/arahan/peraturan/langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja. ii. Kawalan capaian dijalankan bergantung kepada kategori pengguna, sensitiviti aplikasi dan jenis data yang dicapai dan tetapan mudah alih dan telekerja; dan iii. Capaian maklumat dan aplikasi di pusat data melalui jarak jauh (*remote access*) adalah terhad kepada pengguna yang dibenarkan sahaja dan mestilah melalui *Virtual Private Network* (VPN).	ICTSO/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT/ Warga MOTAC
2.2.3 MESYUARAT DALAM TALIAN	
Mesyuarat dalam talian hendaklah mengadaptasi teknik yang selamat seperti penggunaan kata laluan sebelum dibenarkan terlibat di dalam mesyuarat berkenaan.	Penyelaras/Pentadbir Mesyuarat/Pentadbir Rangkaian

BIDANG 03 :
BIDANG KESELAMATAN DAN SUMBER MANUSIA

PERKARA	PERANAN
3.1 SEBELUM PERKHIDMATAN	
Objektif: Memastikan warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.	
3.1.1 TAPISAN KESELAMATAN	
Tapisan keselamatan hendaklah dijalankan terhadap warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan ii. Menjalankan tapisan keselamatan untuk warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Pengguna

PERKARA	PERANAN
3.1.2 TERMA DAN SYARAT PERKHIDMATAN	
Persetujuan berkontrak dengan warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut: i. Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC yang terlibat dalam menjamin keselamatan aset ICT; dan ii. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Pengguna
3.2 DALAM TEMPOH PERKHIDMATAN	
Objektif : Memastikan warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.	
3.2.1 TANGGUNGJAWAB PENGURUSAN	
Pengurusan hendaklah memastikan warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.	Pengguna

PERKARA	PERANAN
3.2.2 KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT	
Warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber MOTAC dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; ii. Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber MOTAC perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan iii. Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.	Pengguna
3.2.3 PROSES TATATERTIB	
Proses tatatertib yang formal dan disampaikan kepada warga MOTAC hendaklah tersedia bagi membolehkan tindakan diambil terhadap warga MOTAC yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga MOTAC sekiranya berlaku perlanggaran terhadap perundangan dan peraturan yang ditetapkan oleh MOTAC; dan ii. Warga MOTAC yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT MOTAC.	Pengurusan Sumber Manusia /Unit Integriti

PERKARA	PERANAN
3.3 PENAMATAN DAN PERTUKARAN PERKHIDMATAN	
Objektif : Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas warga MOTAC diurus dengan teratur.	
3.3.1 PENAMATAN ATAU PERTUKARAN TANGGUNG JAWAB PERKHIDMATAN	
Warga MOTAC yang telah tamat perkhidmatan hendaklah: i. Memastikan semua aset ICT dikembalikan kepada MOTAC mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; ii. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan MOTAC dan/atau terma perkhidmatan yang ditetapkan; dan iii. Maklumat rasmi MOTAC dalam peranti tidak dibenarkan dibawa keluar dari MOTAC. Warga MOTAC yang telah bertukar perkhidmatan hendaklah: i. Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada MOTAC mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan ii. Menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.	Warga MOTAC

BIDANG 04 :
PENGURUSAN ASET

PERKARA	PERANAN
4.1 TANGGUNGJAWAB TERHADAP ASET	
Objektif: Mengenal pasti aset bagi memberikan dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MOTAC.	
4.1.1 INVENTORI ASET	
Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT MOTAC. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: i. MOTAC hendaklah mengenal pasti Pegawai Penerima Aset di setiap MOTAC untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT; ii. Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan. Maklumat aset direkodkan dan dikemas kini di dalam SPPA mengikut Pekeliling Perbendaharaan AM 2 Tahun 2018 : Tatacara Pengurusan Aset Alih Kerajaan tertakluk kepada perubahan arahan dan peraturan yang berkuat kuasa dari semasa ke semasa; iii. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan iv. Pegawai Aset ICT hendaklah mengesahkan penempatan aset ICT.	Pegawai Aset ICT/ Pegawai Penerima Aset/Warga MOTAC
4.1.2 PEMILIKAN ASET	
Aset yang diselanggara hendaklah hak milik MOTAC. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut: i. Memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset; ii. Memastikan aset telah dikelaskan dan dilindungi;	Pengurus Keselamatan ICT/ Pentadbir Sistem ICT/ Warga MOTAC

PERKARA	PERANAN
iii. Kenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan; iv. Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan v. Memastikan semua jenis aset dipelihara dengan baik.	
4.1.3 PENGGUNAAN ASET YANG DIBENARKAN	
i. Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan; dan ii. Semua perkakasan ICT persendirian yang dibawa hendaklah mematuhi prosedur keselamatan ICT yang telah ditetapkan oleh MOTAC.	Pengguna
4.1.4 PEMULANGAN ASET	
i. Pengurusan Sumber Manusia hendaklah memaklumkan kepada Pegawai Aset ICT sekiranya terdapat pertukaran pengguna yang diarahkan oleh KSU; ii. Warga MOTAC hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar kementerian dan penamatan perkhidmatan atau kontrak.	Pengurusan Sumber Manusia/Warga MOTAC

PERKARA	PERANAN
4.2 PENGELASAN MAKLUMAT *(INFORMATION CLASSFICATION)*	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
4.2.1 PENGELASAN MAKLUMAT (*INFORMATION CLASSIFICATION*)	
Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan. Maklumat hendaklah dikelaskan mengikut kategori Maklumat Rasmi dan Maklumat Rahsia Rasmi oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Maklumat hendaklah dikelaskan kepada kategori berikut: i. Maklumat Rahsia Rasmi ii. Maklumat Rasmi iii. Maklumat Pengenalan Peribadi iv. Data Terbuka	Pegawai Pengelas/ Pengguna
4.2.2 PELABELAN MAKLUMAT	
Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.	Pengguna
4.2.3 PENGENDALIAN ASET	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan;	Pengguna

PERKARA	PERANAN
iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.	
4.3 PENGENDALIAN MEDIA	
Objektif: Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
4.3.1 PENGURUSAN MEDIA BOLEH ALIH	
Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh MOTAC. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut: i. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; ii. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; iii. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; iv. Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan v. Menyimpan semua jenis media di tempat yang selamat.	Pentadbir Sistem ICT/ Pengguna

PERKARA	PERANAN
4.3.2 PELUPUSAN MEDIA	
i. Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan; dan ii. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	Pentadbir Sistem ICT/ Jawatankuasa yang dilantik untuk pelupusan aset
4.3.3 PEMINDAHAN MEDIA FIZIKAL	
i. Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan; dan ii. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	Pentadbir Sistem ICT/ Jawatankuasa yang dilantik untuk pelupusan aset

BIDANG 05 :
KAWALAN AKSES

PERKARA	PERANAN
5.1 KAWALAN AKSES	
Objektif: Mengehadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahamidan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.	
5.1.1 POLISI KAWALAN AKSES	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini mengikut keperluan dan menyokong peraturan kawalan capaian pengguna sedia ada. Perkara yang perlu dipatuhi adalah seperti berikut: i. Keperluan keselamatan aplikasi; ii. Hak akses dan polisi klasifikasi maklumat sistem dan rangkaian; iii. Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa; iv. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; v. Pengasingan peranan kawalan capaian; vi. Kebenaran rasmi permintaan akses; vii. Pembatalan hak akses; viii. Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan ix. Capaian *privilege*.	CIO/ICTSO/ Pentadbir Sistem ICT

PERKARA	PERANAN
5.1.2 CAPAIAN KEPADA RANGKAIAN DAN PERKHIDMATAN RANGKAIAN	
Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat pengesahan daripada Ketua Jabatan/Bahagian masing-masing. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: i. Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian MOTAC, rangkaian agensi lain dan rangkaian awam; ii. Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan iii. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	SUB/ Pengarah Bahagian/ ICTSO/Pentadbir Rangkaian/ Pengguna
5.2 PENGURUSAN AKSES PENGGUNA	
Objektif: Akses 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.	
5.2.1 PENDAFTARAN DAN PEMBATALAN PENGGUNA	
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi: i. Akaun yang diperuntukkan oleh MOTAC sahaja boleh digunakan; ii. Akaun ID pengguna mestilah unik; iii. Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada MOTAC terlebih dahulu; iv. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan v. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan MOTAC.	Pentadbir Sistem ICT/ Pengguna

PERKARA	PERANAN
5.2.2 PERUNTUKAN AKSES PENGGUNA	
Satu proses penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT.	SUB/Pengarah Bahagian/ICTSO/ Pentadbir Sistem ICT
5.2.3 PENGURUSAN HAK AKSES ISTIMEWA	
i. Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal; dan ii. Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas merujuk kepada Prosedur Pendaftaran dan Penamatan Pengguna.	Pentadbir Sistem ICT
5.2.4 KAJIAN SEMULA HAK AKSES PENGGUNA	
i. Menyemak hak akses pengguna pada sela masa yang ditetapkan; dan ii. Mewujudkan Prosedur Pendaftaran dan Penamatan Pengguna sistem masing-masing sebagai rujukan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan.	ICTSO/Pentadbir Sistem ICT
5.2.5 PEMBATALAN ATAU PELARASAN HAK AKSES	
Hak akses pengguna untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam MOTAC.	SUB/Pengarah Bahagian/ICTSO/ Pentadbir Sistem ICT

PERKARA	PERANAN
5.3 TANGGUNGJAWAB PENGGUNA	
Objektif: Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.	
5.3.1 PENGGUNAAN MAKLUMAT PENGESAHAN RAHSIA	
i. Membaca, memahami dan mematuhi Polisi Keselamatan Siber MOTAC; ii. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; iii. Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat MOTAC; iv. Melaksanakan langkah-langkah perlindungan seperti yang 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. Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum. v. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; dan vi. Menghadiri program-program kesedaran mengenai keselamatan ICT.	ICTSO/SUB/ Pengarah Bahagian/ Pentadbir Sistem ICT/ Pengguna

PERKARA	PERANAN
5.3.2 PENGGUNAAN MAKLUMAT PENGESAHAN RAHSIA (*AUTHENTICATION*)	
Pengguna perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.	Pentadbir Sistem ICT/ Pengguna
5.4 KAWALAN AKSES SISTEM DAN APLIKASI	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi.	
5.4.1 SEKATAN AKSES MAKLUMAT	
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut polisi kawalan capaian.	Pentadbir Sistem Aplikasi/ Pengguna
5.4.2 PROSEDUR LOG MASUK YANG SELAMAT (*SECURE LOG-ON*)	
Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti berikut: i. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan MOTAC; ii. Mewujudkan kata laluan yang berkualiti; iii. Menjana amaran (alert) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem; iv. Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin; v. Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna; vi. Mewujudkan sistem pengurusan kata laluan berkualiti; dan vii. Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	Pentadbir Sistem Aplikasi

PERKARA	PERANAN
5.4.3 SISTEM PENGURUSAN KATA LALUAN	
Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MOTAC seperti berikut: i. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; ii. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; iii. Panjang kata laluan mestilah sekurang kurangnya LAPAN (8) AKSARA dengan gabungan antara huruf, aksara khas dan nombor (*alphanumeric*) KECUALI bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; iv. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekali pun; v. Kata laluan paparan kunci *(lock screen*) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; vi. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; vii. Kuat kuasakan pertukaran kata laluan semasa atau selepas log masuk kali pertama atau selepas reset kata laluan; viii. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; ix. Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum TIGA (3) KALI sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; x. Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna; xi. Kata laluan hendaklah ditukarkan selepas 90 hari; dan xii. Mengelakkan penggunaan semua kata laluan yang telah digunakan	ICTSO/Pentadbir Sistem ICT/Pengguna

PERKARA	PERANAN
5.4.4 PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA	
Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding* sistem.	SUB/Pengarah Bahagian/ICTSO/ Pentadbir Sistem ICT
5.4.5 KAWALAN AKSES KEPADA KOD SUMBER PROGRAM	
Capaian kepada kod sumber hendaklah dihadkan. Perkara- perkara yang perlu dipertimbangkan adalah seperti berikut: i) Log audit perlu dikekalkan kepada semua akses kepada kod sumber; ii) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan iii) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik MOTAC.	Pentadbir Sistem ICT

BIDANG 06 :
KRIPTOGRAFI

PERKARA	PERANAN
6.1 KAWALAN KRIPTOGRAFI	
Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan, dan/atau keutuhan maklumat.	
6.1.1 POLISI PENGGUNAAN KAWALAN KRIPTOGRAFI	
Kriptografi merangkumi kaedah-kaedah seperti berikut: i. Enkripsi Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (*encryption*). ii. Tandatangan Digital Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan.	Pengguna
6.1.2 PENGURUSAN KUNCI AWAM	
Pengurusan ke atas Perkhidmatan Prasarana Kunci Awam (*Public Key Infrastructure* (PKI)) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan diubah, dimusnah, dikongsi dan didedahkan sepanjang tempoh sah kunci tersebut. Rujukan berkaitan kriptografi seperti Dasar Kriptografi Negara dan MySeal yang dikeluarkan oleh Cybersecurity Malaysia boleh diguna pakai sebagai panduan.	Pentadbir Sistem ICT/ Pengguna

BIDANG 07 :
KESELAMATAN FIZIKAL DAN PERSEKITARAN

PERKARA	PERANAN
7.1 KAWASAN SELAMAT	
Objektif: Menghalang akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat MOTAC.	
7.1.1 PERIMETER KESELAMATAN FIZIKAL	
Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan aset ICT MOTAC. Perkara-perkara yang perlu dipatuhi seperti berikut: i. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; ii. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; iii. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; iv. Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia; v. Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; vi. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan vii. Memasang alat penggera atau kamera keselamatan.	CGSO/SUB/ Pengarah Bahagian/ Pengurusan Sumber Manusia/Bahagian Pentadbiran

PERKARA	PERANAN
7.1.2 KAWALAN KEMASUKAN FIZIKAL	
Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis MOTAC. Perkara yang perlu dipatuhi adalah seperti berikut: i. Warga MOTAC hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada MOTAC apabila bertukar, tamat perkhidmatan atau bersara; ii. Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan; iii. Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT MOTAC; iv. Kehilangan pas keselamatan hendaklah dilaporkan segera kepada Pihak Berkuasa; dan v. Mematuhi prosedur, peraturan dan polisi sedia ada dalam memasuki ruang kerja di kawasan larangan seperti pusat data, ruang baik pulih perkakasan komputer dan lain-lain ruang yang memerlukan pengawasan dan pemantauan yang khusus.	Pengurusan Sumber Manusia/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT/ Pengguna
7.1.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN	
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti berikut: i. Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV dan pusat data perlu dihadkan daripada diakses tanpa kebenaran; ii. Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan iii. Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi Arahan Keselamatan.	Bahagian Pentadbiran/ICTSO/ Pentadbir Sistem ICT/ Pengguna

PERKARA	PERANAN
7.1.4 PERLINDUNGAN DARIPADA ANCAMAN LUAR DAN PERSEKITARAN	
Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. MOTAC perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	CDO/ICTSO/ SUB/Pengarah Bahagian/ Bahagian Pentadbiran/ Pentadbir Sistem ICT
7.1.5 BEKERJA DI KAWASAN SELAMAT	
Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga MOTAC yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis MOTAC termasuklah Pusat Data. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti berikut: i. Sumber data atau *server*, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; ii. Akses adalah terhad kepada warga MOTAC yang telah diberi kuasa sahaja dan dipantau pada setiap masa; iii. Pemantauan dibuat menggunakan rakaman kamera CCTV atau lain-lain peralatan yang sesuai; iv. Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual; v. Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; vi. Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan;	SUB/Pengarah Bahagian/ Pengurusan Sumber Manusia/ICTSO/ Pentadbir Sistem ICT/ Bahagian Pentadbiran

PERKARA	PERANAN
vii. Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; viii. Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; ix. Memperkukuh dinding dan siling; dan x. Menghadkan jalan keluar masuk.	
7.1.6 KAWASAN PENYERAHAN DAN PEMUNGGAHAN	
i. Titik kemasukan *access point* seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan; dan ii. MOTAC hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.	SUB/Pengarah/ Bahagian Pentadbiran /Pengguna
7.2 PERALATAN ICT	
Objektif: Melindungi peralatan ICT MOTAC daripada kehilangan, kerosakan, kecurian dan disalahgunakan.	
7.2.1 PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT	
Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkah-langkah keselamatan yang perlu diambil adalah seperti 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;	ICTSO/Pentadbir Sistem ICT/ Pengguna/Pegawai Aset ICT

PERKARA	PERANAN
iii. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; iv. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; v. Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; vi. Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna; vii. Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; viii. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Gen-Set); ix. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; x. Peralatan rangkaian seperti *switch, router, hub* dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan 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 ke luar premis MOTAC, perlulah mendapat kelulusan Pegawai Aset ICT dan direkodkan bagi tujuan pemantauan; xiii. Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden; xiv. Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; xv. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pentadbir Sistem ICT; xvi. Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih;	

PERKARA	PERANAN
xvii. Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; xviii. Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal; xix. Pengguna dilarang sama sekali mengubah kata laluan pentadbir yang telah ditetapkan oleh pihak ICT; dan xx. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya.	
7.2.2 UTILITI SOKONGAN	
i. Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan; dan ii. Semua alat sokongan perlu diselenggara dari semasa ke semasa (sekurang-kurangnya setahun sekali).	SUB/Pengarah Bahagian Pentadbiran/ICTSO/ Pentadbir Sistem ICT/Pengguna
7.2.3 KESELAMATAN KABEL	
Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: i. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; ii. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; iii. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan iv. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	ICTSO/Pentadbir Sistem ICT/Bahagian Pentadbiran

PERKARA	PERANAN
7.2.4 PENYELENGGARAAN PERALATAN	
Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan, kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: i. Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; ii. Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; iii. Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; iv. Melaksanakan prosedur sandaran (data, maklumat, polisi dan konfigurasi) sebagai langkah pencegahan dan alternatif bagi penyelesaian secara *rollback*. v. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan vi. Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pengurus Keselamatan ICT/ Pentadbir Sistem ICT/ Pengguna
7.2.5 PENGALIHAN ASET	
Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: i. Peralatan ICT yang hendak dibawa keluar dari premis MOTAC untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Jabatan atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan ii. Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	SUB/Pengarah Bahagian/ICTSO/ Pegawai Aset ICT/ Pengguna

PERKARA	PERANAN
7.2.6 KESELAMATAN PERALATAN DAN ASET DI LUAR PREMIS	
Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis MOTAC. Peralatan yang dibawa keluar dari premis MOTAC adalah terdedah kepada pelbagai risiko. 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; dan iii. Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	Pengguna
7.2.7 PELUPUSAN PERALATAN YANG SELAMAT ATAU PENGGUNAAN SEMULA	
Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (*overwrite*) sebelum dilupuskan atau diguna semula. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MOTAC dan ditempatkan di MOTAC. Peralatan ICT yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan MOTAC. Langkah-langkah seperti berikut hendaklah diambil: i. Bagi peralatan ICT yang akan dilupuskan sebelum dipindah milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat; ii. Pegawai Aset ICT hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya. iii. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; iv. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;	ICTSO/Pentadbir Sistem ICT/ Pengguna/Pegawai Aset ICT

PERKARA	PERANAN
v. Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: a. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; b. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *Central Processing Unit* (CPU) seperti *Random Access Memory* (RAM), *Hardisk, Motherboard* dan sebagainya; c. Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan d. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Jawatankuasa yang dilantik untuk pelupusan aset MOTAC. vi. Pengguna bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; vii. Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal. Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat Salinan. Penyimpanan *bookmark*, akaun dan kata laluan secara terus di memori juga perlu diberi perhatian yang sama; viii. Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa; ix. Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara MOTAC Arkib Negara; dan x. Pegawai Aset ICT bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam SPPA.	ICTSO/Pentadbir Sistem ICT/ Pengguna/Pegawai Aset ICT

PERKARA	PERANAN
7.2.8 PERALATAN PENGGUNA TANPA KAWALAN	
Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: i. Tamatkan sesi aktif apabila selesai tugas; ii. *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan iii. Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.	Pengguna
7.2.9 POLISI MEJA KOSONG DAN SKRIN KOSONG	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkah-langkah yang perlu diambil termasuklah seperti berikut: i. Menggunakan kemudahan password screen saver atau *logout* apabila meninggalkan komputer; ii. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; iii. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat; iv. E-mel masuk dan keluar hendaklah dikawal; dan v. Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	SUB/Pengarah Bahagian/Bahagian Pentadbiran/ Pengguna

BIDANG 08 :
KESELAMATAN OPERASI

PERKARA	PERANAN
8.1 PROSEDUR DAN TANGGUNGJAWAB OPERASI	
Objektif: Memastikan operasi kemudahan pemprosesan maklumat yang betul, cekap dan selamat.	
8.1.1 PROSEDUR OPERASI YANG DIDOKUMENKAN	
Penyedia dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut: i. Semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; ii. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan iii. Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.	SUB/Ketua Unit/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT/ Pentadbir Rangkaian
8.1.2 PENGURUSAN PERUBAHAN	
Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara berikut: i. Mewujudkan prosedur pengurusan perubahan; ii. Merekodkan semua perubahan yang telah dipersetujui dan dilaksanakan; dan iii. Memantau pelaksanaan perubahan.	Pentadbir Sistem ICT

PERKARA	PERANAN
8.1.3 PENGURUSAN KAPASITI	
Kapasiti sistem ICT hendaklah dirancang, diurus dan dikawal dengan terperinci bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan operasi sistem ICT. Keperluan kapasiti perlu mengambil kira ciri-ciri keselamatan bagi meminimumkan risiko gangguan kepada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem ICTN
8.1.4 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN OPERASI	
Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian ataupun perubahan tidak sah ke atas persekitaran operasi.Perkara–perkara yang perlu dipatuhi: i. Mewujudkan prosedur keperluan sumber bagi penyediaan persekitaran untuk pembangunan, pengujian dan operasi; ii. Merekodkan semua penggunaan sumber yang dilaksanakan; iii. Memantau pelaksanaan penggunaan sumber bagi tujuan perancangan kapasiti; dan iv. Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.	Pentadbir Sistem ICT

PERKARA	PERANAN
8.2 PERLINDUNGAN DARIPADA PERISIAN HASAD *(MALWARE)*	
Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.	
8.2.1 KAWALAN DARIPADA PERISIAN HASAD (*MALWARE*)	
Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan *malware* hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut: i. Memasang sistem keselamatan untuk mengesan perisian atau program *malware* seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; ii. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; iii. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; iv. Mengemas kini antivirus dengan *signature/pattern* antivirus yang terkini; v. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; vi. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; dan vii. 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.	Pengurus Keselamatan ICT/ Pentadbir Sistem ICT/ Pengguna

PERKARA	PERANAN
8.3 SANDARAN *(BACKUP)*	
Objektif: Memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.	
Salinan pendua maklumat dan perisian sistem hendaklah disediakan dan diuji secara berkala selaras dengan polisi backup bagi tujuan kesinambungan operasi pemprosesan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti berikut: i. Membuat salinan pendua ke atas semua maklumat dan sistem perisian mengikut jadual yang ditetapkan atau apabila berlaku perubahan versi; ii. Menyimpan salinan pendua di lokasi lain yang selamat; dan iii. Menguji sistem pendua bagi memastikan ianya dapat beroperasi dengan normal	Pengurus Keselamatan ICT/ Pentadbir Sistem ICT/ Pentadbir Pusat Data
8.4 PENGELOGAN DAN PEMANTAUAN *(LOGGING AND MONITORING)*	
Objektif: Semua peristiwa dan bukti kewujudan insiden hendaklah direkodkan untuk tujuan jejak audit.	
8.4.1 PENGELOGAN KEJADIAN (*EVENT LOGGING*)	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Setiap sistem mestilah mempunyai jejak audit; i. Mewujudkan prosedur untuk memantau penggunaan kemudahan memproses maklumat dan dipantau secara berkala; ii. Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; iii. Maklumat log perlu dilindungi daripada sebarang ubah suai dan capaian yang tidak dibenarkan; iv. Sebarang kesalahan, kesilapan atau penyalahgunaan sistem perlu direkodkan, dianalisis dan diambil tindakan sewajarnya;	Pengurus Keselamatan ICT/ Pentadbir Sistem ICT

PERKARA	PERANAN
v. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; vi. Waktu yang berkaitan dengan sistem pemprosesan maklumat MOTAC perlu diselaraskan dengan satu sumber waktu yang piawai; dan vii. Sebarang aktiviti tidak sah seperti kecurian maklumat dan pencerobohan hendaklah dilaporkan kepada CSIRT MOTAC.	
8.5 KAWALAN PEMASANGAN PERISIAN	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MOTAC; dan ii. Lesen perisian (*registration code, CD-keys*, nombor siri dan langganan atas talian) perlu disimpan berasingan daripada CD-ROM, disk atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak.	Pentadbir Sistem ICT
8.6 PENGURUSAN KERENTANAN TEKNIKAL	
Objektif: Memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.	
8.6.1 PENGURUSAN KERENTANAN TEKNIKAL	
Perkara-perkara yang perlu dipatuhi adalah: i. Mengenal pasti maklumat keterdedahan teknikal sistem yang digunakan;	Pengurus Keselamatan ICT/ Pentadbir Sistem ICT/ CSIRT MOTAC

PERKARA	PERANAN
ii. Menilai tahap keterdedahan bagi mengenal pasti risiko yang bakal dihadapi; dan iii. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	
8.6.2 SEKATAN KE ATAS PEMASANGAN PERISIAN	
Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti berikut: i. Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga MOTAC, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC. ii. Memasang dan menggunakan hanya perisian yang tulen dan berdaftar; dan iii. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.	Pengurus Keselamatan ICT/ Pentadbir Sistem ICT/ Pengguna
8.7 JEJAK AUDIT	
Objektif: Meminimumkan kesan aktiviti audit terhadap sistem yang beroperasi.	
8.7.1 KAWALAN JEJAK AUDIT	
i. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan; dan ii. Capaian ke atas sistem maklumat semasa pengauditan perlu dikawal selia bagi mengelakkan sebarang penyalahgunaan.	ICTSO/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT

BIDANG 09 :
KESELAMATAN KOMUNIKASI

PERKARA	PERANAN
9.1 PENGURUSAN KESELAMATAN RANGKAIAN	
Objektif: Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.	
9.1.1 KAWALAN RANGKAIAN	
Infrastruktur rangkaian hendaklah dirancang, diurus dan dikawal bagi melindungi keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah: i. Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berkaitan dengan sistem rangkaian; ii. Peralatan keselamatan seperti *firewall* hendaklah dipasang bagi memastikan hak capaian ke atas sistem dapat dilaksanakan seperti ditetapkan; iii. Sebarang cubaan menceroboh dan aktiviti yang boleh mengancam sistem dan maklumat MOTAC perlu dipantau dan dikesan melalui pemasangan peralatan keselamatan seperti *Intrusion Prevention System* (IPS); iv. Peralatan rangkaian hendaklah diletakkan di lokasi yang bebas dari risiko seperti banjir, gegaran dan habuk; v. Sebarang keperluan penyambungan rangkaian hendaklah melalui proses dan prosedur yang ditetapkan; vi. Penggunaan rangkaian tanpa wayar (*wireless*) LAN di MOTAC hendaklah mematuhi peraturan yang dikeluarkan oleh pihak berkenaan seperti MAMPU dan Majlis Keselamatan Negara (MKN); dan vii. Semua perisian berkaitan rangkaian dan keselamatan seperti *sniffer* atau *network analyzer* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO.	ICTSO/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT

PERKARA	PERANAN
9.1.2 KESELAMATAN PERKHIDMATAN RANGKAIAN	
Perkhidmatan rangkaian hendaklah dipastikan sentiasa selamat bagi memastikan kerahsiaan, integriti dan ketersediaan maklumat terjamin. Perkara-perkara yang perlu dipatuhi adalah: i. Mekanisme keselamatan, tahap kesediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan disediakan secara dalaman ataupun menggunakan sumber luar; ii. Semua trafik keluar dan masuk hendaklah ditapis oleh peralatan keselamatan di bawah kawalan MOTAC; dan iii. Sebarang aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam (PKPA) yang berkuat kuasa perlu disekat melalui penggunaan *WebContent Filtering*	ICTSO/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT
9.1.3 PENGASINGAN DALAM RANGKAIAN	
Pengasingan perkhidmatan rangkaian bertujuan untuk meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan. Perkara–perkara yang perlu dipatuhi adalah: i. Mengenal pasti fungsi dan tanggungjawab pengguna; ii. Mengkonfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan; iii. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; iv. Mengemaskinikan hak capaian pengguna dari masa ke semasa mengikut keperluan; dan v. Operasi rangkaian hendaklah diasingkan untuk meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan	ICTSO/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT

PERKARA	PERANAN
9.2 PEMINDAHAN DATA DAN MAKLUMAT	
Objektif: Memastikan keselamatan maklumat terjamin semasa pertukaran maklumat dengan entiti luar.	
9.2.1 PROSEDUR PEMINDAHAN DATA DAN MAKLUMAT	
Prosedur ini bertujuan untuk mengendali, menyimpan, memindah serta melindungi maklumat daripada didedah tanpa kebenaran atau salah guna serta memastikan keselamatan pemindahan maklumat dengan entiti luar terjamin. Perkara-perkara yang perlu dipatuhi adalah seperti: i. Menghadkan dan menentukan capaian kepada pengguna yang dibenarkan sahaja; ii. Menghadkan pengedaran data untuk tujuan rasmi dan yang dibenarkan sahaja; iii. Polisi, prosedur dan kawalan pemindahan maklumat yang formal perlu diwujudkan untuk melindungi pemindahan maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; iv. Sebarang pemindahan maklumat di antara MOTAC dengan agensi lain, organisasi atau pihak ketiga mestilah dikawal; dan v. Penggunaan perkhidmatan luar seperti aplikasi media sosial dan perkongsian fail untuk pemindahan maklumat rasmi Kerajaan perlu mendapat kelulusan Ketua Jabatan.	SUB/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT/ Pengguna
9.2.2 PERJANJIAN MENGENAI PEMINDAHAN DATA DAN MAKLUMAT	
i. *Non-Disclosure Agreements* (NDA) perlu diwujudkan bagi memastikan kerahsiaan, integriti dan ketersediaan (CIA) maklumat terpelihara semasa proses pemindahan maklumat dan perisian di antara MOTAC dengan agensi luar; dan ii. Keperluan melindungi kerahsiaan meliputi integriti dan kerahsiaan maklumat hendaklah disemak secara berkala dan didokumenkan.	CDO/ ICTSO/ SUB/Pengarah Bahagian/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT

PERKARA	PERANAN
9.2.3 PESANAN ELEKTRONIK (E-MEL)	
Maklumat yang dihantar, diterima dan disimpan melalui mel elektronik MOTAC perlu dilindungi bagi menghindari capaian atau sebaran maklumat yang tidak dibenarkan.	Warga MOTAC
9.2.4 PENGURUSAN PORTAL DAN MEDIA SOSIAL	
i. Memastikan maklumat hebahan (*posting*) sentiasa disemak atau dikomen (dengan seorang moderator); ii. Menyekat mereka yang terus membuat hebahan atau komen jelik; iii. Melaporkan sebarang pelanggaran polisi penggunaan yang sedang berkuat kuasa; dan iv. Maklumat yang terlibat dalam media sosial hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Peraturan bertulis yang berkuat kuasa adalah: a. Garis Panduan Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam (MAMPU); dan b. Pekeliling Kemajuan Pentadbiran Awam Bil. 2 Tahun 2015 - Pengurusan Laman Web Agensi Sektor Awam.	Pentadbir Portal/ Pentadbir Media Sosial/UKK/ Pengguna

BIDANG 10 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

PERKARA	PERANAN
10.1 KEPERLUAN KESELAMATAN SISTEM MAKLUMAT	
Objektif: Memastikan sistem yang dibangunkan secara dalaman atau pun luaran mempunyai ciri-ciri keselamatan maklumat yang kukuh dan berdaya tahan daripada aktiviti berniat jahat serta merangkumi keseluruhan kitaran hayat aset.	
10.1.1 ANALISIS DAN SPESIFIKASI KEPERLUAN KESELAMATAN MAKLUMAT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan; ii. Semua sistem yang dibangunkan sama ada secara dalaman atau luaran hendaklah dikaji supaya mengikut keperluan pengguna dan selaras dengan dasar atau peraturan berkaitan yang berkuat kuasa; dan iii. Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan.	Jawatankuasa Penilaian Teknikal/ JPICT/Pentadbir Sistem ICT/Pembekal
10.1.2 PERLINDUNGAN PERKHIDMATAN APLIKASI YANG MENGGUNAKAN RANGKAIAN AWAM	
Maklumat aplikasi yang menggunakan rangkaian awam hendaklah dilindungi daripada aktiviti tidak sah seperti penipuan, pendedahan maklumat, pengubahsuaian maklumat yang tidak dibenarkan yang menyebabkan pertikaian kontrak. Perkara-perkara yang perlu dipatuhi adalah: i. Identiti pengguna perlu dikenal pasti dan disahkan bagi menentukan tahap capaian maklumat yang dibenarkan; ii. Setiap pengguna sistem perlu diberi peranan mengikut skop dan tanggungjawab yang ditetapkan; dan iii. Memastikan pihak ketiga diberi penjelasan dan menandatangani akuan pematuhan PKS mengenai keperluan mematuhi kontrak dan peraturan keselamatan yang ditetapkan.	Pengurus Keselamatan ICT/ Pentadbir Sistem ICT/ Pihak Ketiga

PERKARA	PERANAN
10.1.3 MELINDUNGI TRANSAKSI PERKHIDMATAN APLIKASI	
i. Maklumat yang terlibat dalam transaksi perkhidmatan atas talian hendaklah dilindungi daripada penghantaran yang tidak lengkap, *mis-routing*, pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan dan duplikasi mesej; ii. Kawalan terhadap keterdedahan perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan; dan iii. Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan.	ICTSO/SUB/ Pengarah Bahagian/ Pengurus Keselamatan ICT/ Pentadbir Sistem ICT
10.2 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN	
Objektif: Memastikan keselamatan maklumat diwujudkan dan dilaksanakan dalam kitar hayat pembangunan sistem.	
10.2.1 POLISI KESELAMATAN DALAM PEMBANGUNAN SISTEM	
Tatacara pembangunan perisian dan sistem yang mengambil kira aspek keselamatan maklumat hendaklah diwujudkan dan dilaksanakan di dalam organisasi dengan membangunkan Dokumen Pelan Pengurusan Keselamatan Maklumat (ISMP) atau yang setara semasa proses pembangunan system.	Pentadbir Sistem ICT
10.2.2 PROSEDUR KAWALAN PERUBAHAN SISTEM	
Prosedur kawalan perubahan hendaklah diwujudkan bagi mengawal sebarang perubahan terhadap sistem sepanjang kitar hayat pembangunan sistem. Perkara-perkara yang perlu dipatuhi adalah sepert berikut:	SUB/Pengarah Bahagian/Pentadbir Sistem

PERKARA	PERANAN
i. Mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan yang ditetapkan dan pelaksanaan hanya mengikut keperluan sahaja; ii. Perubahan atau pengubahsuaian ke atas perisian dan sistem hendaklah diuji, didokumenkan dan disahkan sebelum diguna pakai; dan iii. Setiap perubahan kepada pengoperasian sistem perlu dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap operasi dan keselamatan maklumat.	
10.2.3 SEMAKAN TEKNIKAL APLIKASI SELEPAS PERUBAHAN PLATFORM	
Semakan dan pengujian terhadap aplikasi kritikal 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; dan ii. Ujian penerimaan pengguna perlu dilaksanakan setelah perubahan platform selesai dilaksanakan.	Pentadbir Sistem ICT
10.2.4 KAWALAN TERHADAP PERUBAHAN KEPADA PERISIAN	
Sebarang perubahan terhadap perisian adalah tidak digalakkan, kecuali kepada perubahan yang perlu sahaja dan perubahan tersebut perlu dihadkan.	SUB/Pengarah Bahagian/Pentadbir Sistem ICT
10.2.5 PRINSIP KEJURUTERAAN SISTEM YANG SELAMAT	
Prinsip bagi sistem keselamatan kejuruteraan hendaklah berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) sektor awam yang terkini untuk apa-apa usaha pelaksanaan sistem maklumat.	SUB/ Pentadbir Sistem ICT

PERKARA	PERANAN
10.2.6 PERSEKITARAN PEMBANGUNAN YANG SELAMAT	
Persekitaran pembangunan sistem yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem. Secara umumnya kitar hayat pembangunan sistem termasuk skop dan objektif sistem, pengumpulan keperluan, reka bentuk, pelaksanaan, ujian, penerimaan, pemasangan, konfigurasi, penyelenggaraan dan pelupusan. Persekitaran pembangunan sistem yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem. Secara umumnya kitar hayat pembangunan sistem termasuk skop dan objektif sistem, pengumpulan keperluan, reka bentuk, pelaksanaan, ujian, penerimaan, pemasangan, konfigurasi, penyelenggaraan dan pelupusan.	SUB/Pengarah Bahagian/Pentadbir Sistem ICT
10.2.7 PEMBANGUNAN OLEH KHIDMAT LUARAN	
Prinsip bagi pembangunan menggunakan khidmat luaran hendaklah berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) dan Garis Panduan Pembangunan Aplikasi Sektor Awam yang terkini untuk apa-apa usaha pembangunan dan pelaksanaan sistem maklumat. MOTAC hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Kod sumber (*source code*) adalah menjadi HAK MILIK KERAJAAN. Perkara yang perlu dipatuhi adalah seperti berikut: i. Perkiraan perlesenan, kod sumber ialah **HAK MILIK KERAJAAN** dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource*; ii. Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori "Pembekal hendaklah membenar Kerajaan hak mencapai kod sumber dan melaksanakan pengolahan risiko"; iii. Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik; iv. Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem;	ICTSO/SUB/ Pentadbir Sistem ICT

PERKARA	PERANAN
v. Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian; vi. Data ujian hendaklah dilupuskan secara kekal (*secured delete*) selepas projek disiapkan/tamat kontrak; dan vii. Aktiviti sandaran hendaklah diuji sehingga berjaya dilakukan sebelum projek tamat.	
10.2.8 PENGUJIAN KESELAMATAN SISTEM	
Aktiviti pengujian penerimaan sistem hendaklah dilaksanakan ke atas sistem baru, naik taraf dan versi baru berdasarkan kriteria yang telah ditetapkan. Bagi memastikan integriti data, pengujian hendaklah dijalankan ke atas tiga (3) peringkat pemprosesan maklumat iaitu peringkat kemasukan data (input), peringkat pemprosesan data (*process*) dan peringkat penjanaan laporan (*output*)	ICTSO/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT
10.3 DATA UJIAN	
Objektif: Memastikan perlindungan ke atas data yang digunakan untuk pengujian.	
10.3.1 PERLINDUNGAN DATA UJIAN	
Data ujian hendaklah bersesuaian, dilindungi dan dikawal.	ICTSO/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT/ Pengguna

BIDANG 11 :
HUBUNGAN PEMBEKAL

PERKARA	PERANAN
11.1 KESELAMATAN MAKLUMAT DALAM HUBUNGAN PEMBEKAL	
Objektif: Memastikan aset ICT MOTAC yang boleh dicapai oleh pembekal dilindungi.	
Semua pembekal adalah tertakluk kepada Dasar Keselamatan Kerajaan yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Pembekal hendaklah menandatangani Surat Akuan Pematuhan PKS MOTAC; ii. Pembekal hendaklah menjalani ujian tapisan keselamatan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO); dan iii. Pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas.	SUB/Pengarah Bahagian/ Pemilik Projek/ Pembekal
11.1.2 KAWALAN KESELAMATAN MAKLUMAT MELALUI PERJANJIAN DENGAN PEMBEKAL	
Perjanjian dengan pihak pembekal hendaklah merangkumi keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan perkhidmatan teknologi maklumat dan komunikasi.	Pembekal/PUU/ Pentadbir Sistem ICT
11.1.3 RANTAIAN BEKALAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI	
Perjanjian dengan pembekal hendaklah meliputi risiko keselamatan yang merangkumi perkhidmatan ICT dan kesinambungan bekalan produk dengan pihak ketiga.	SUB/Pengarah Bahagian/Pemilik Projek/Pembekal

PERKARA	PERANAN
11.2 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PEMBEKAL	
Objektif: Kementerian hendaklah memantau, menyemak dan mengaudit perkhidmatan pembekal secara berkala.	
11.2.1 PEMANTAUAN DAN PENILAIAN PERKHIDMATAN PEMBEKAL	
Kementerian hendaklah memantau, menyemak dan mengaudit perkhidmatan pembekal secara berkala.	SUB/Pengarah Bahagian/ Pemilik Projek/ Pembekal
11.2.2 MENGURUSKAN PERUBAHAN KEPADA PERKHIDMATAN PEMBEKAL	
Setiap perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut SOP yang ditetapkan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: i. Perubahan di dalam perjanjian bersama pembekal; ii. Perubahan yang dilakukan oleh Kementerian bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan iii. Perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	SUB/Pengarah Bahagian/Pemilik Projek/Pembekal

BIDANG 12 :
PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

PERKARA	PERANAN
12.1 PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT DAN PENAMBAHBAIKAN	
Objektif: Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kerentanan kelemahan keselamatan.	
12.1.1 TANGGUNGJAWAB DAN PROSEDUR	
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden MOTAC adalah berdasarkan kepada Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT MOTAC yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut: i. Memberikan kesedaran berkaitan Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT MOTAC dan hebahan kepada warga MOTAC sekiranya ada perubahan; dan ii. Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.	ICTSO/SUB/ Pengarah Bahagian/CSIRT MOTAC/Pengurus Keselamatan ICT/ Pentadbir Sistem ICT
12.1.2 PELAPORAN KEJADIAN KESELAMATAN MAKLUMAT	
Perjanjian dengan pihak pembekal hendaklah merangkumi keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan perkhidmatan teknologi maklumat dan komunikasi.	Pembekal/PUU/ Pentadbir Sistem ICT

PERKARA	PERANAN
i. Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT MOTAC. CSIRT MOTAC kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Maklumat didapati hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Makumat disyaki hilang dan didedahkan kepada kepada pihak-pihak yang tidak diberi kuasa; c. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; d. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; e. Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan; f. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan g. Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka. ii. Prosedur pelaporan insiden keselamatan ICT berdasarkan: a. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	ICTSO/SUB/ Pengarah Bahagian/ CSIRT MOTAC
12.1.3 PELAPORAN KELEMAHAN KESELAMATAN MAKLUMAT	
Warga MOTAC dan pembekal yang menggunakan sistem dan perkhidmatan maklumat MOTAC dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.	Pengguna/Warga MOTAC

PERKARA	PERANAN
12.1.4 PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT	
Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.	ICTSO
12.1.5 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT	
Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT MOTAC. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: i. Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; ii. Menjalankan kajian forensik sekiranya perlu; iii. Menghubungi pihak yang berkenaan dengan secepat mungkin; iv. Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti; v. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; vi. Menyediakan pelan kontigensi dan mengaktifkan PKP; vii. Menyediakan tindakan pemulihan segera; dan viii. Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	ICTSO/CSIRT MOTAC

PERKARA	PERANAN
12.1.6 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT	
i. Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya; dan ii. Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.	ICTSO/CSIRT MOTAC
12.1.7 PENGUMPULAN BAHAN BUKTI	
MOTAC hendaklah menentukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.	ICTSO/CSIRT MOTAC

BIDANG 13 :
ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

PERKARA	PERANAN
13.1 KESINAMBUNGAN KESELAMATAN MAKLUMAT	
Objektif: Memastikan kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan bisnes MOTAC.	
13.1.1 PERANCANGAN KESINAMBUNGAN KESELAMATAN MAKLUMAT	
MOTAC hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, MOTAC perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi MOTAC. MOTAC juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti berikut: i. Melantik pasukan tadbir urus PKP MOTAC; ii. Menetapkan polisi PKP; iii. Mengenal pasti perkhidmatan kritikal; iv. Melaksanakan Kajian Impak Perkhidmatan (*Business Impact Analysis* - BIA) dan Penilaian Risiko terhadap perkhidmatan kritikal; v. Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak Balas Kecemasan dan Pelan Pemulihan Bencana ICT vi. Merancang dan melaksanakan program kesedaran dan latihan pasukan PKP dan warga MOTAC; vii. Merancang dan melaksanakan simulasi ke atas dokumen di para (c); dan viii. Merancang dan melaksanakan penyelenggaraan ke atas pelan di para (c).	Ketua Jabatan/SUB/ Pengarah Bahagian/ Koordinator PKP/ CSIRT MOTAC

PERKARA	PERANAN
13.1.2 PELAKSANAAN KESINAMBUNGAN KESELAMATAN MAKLUMAT	
Kementerian hendaklah memantau, menyemak dan mengaudit perkhidmatan pembekal secara berkala.	SUB/Pengarah Bahagian/ Pemilik Projek/ Pembekal
11.2.2 MENGURUSKAN PERUBAHAN KEPADA PERKHIDMATAN PEMBEKAL	
MOTAC hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti berikut: i. Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP; ii. Mengemas kini struktur tadbir urus PKP MOTAC jika berlaku pertukaran pegawai bersara dan bertukar keluar; iii. Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal MOTAC yang telah dikenal pasti berdasarkan kepada Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak Balas Kecemasan dan dan Pelan Pemulihan Bencana ICT terkini; iv. Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal MOTAC; dan v. Melaksanakan *post-mortem* dan mengemaskini pelan-pelan PKP;	Ketua Jabatan/SUB/ Pengarah Bahagian/ Koordinator PKP/ CSIRT MOTAC

PERKARA	PERANAN
13.1.3 MENENTUSAHKAN, MENGKAJI SEMULA DAN MENILAI KESINAMBUNGAN KESELAMATAN MAKLUMAT	
MOTAC hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.	Pengurusan Atasan MOTAC/Koordinator PKP/CSIRT MOTAC/ Warga MOTAC
13.2 LEWAHAN *(REDUNDANCY)*	
Objektif: Memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.	
13.2.1 KETERSEDIAAN KEMUDAHAN PEMPROSESAN MAKLUMAT	
Kemudahan pemprosesan maklumat MOTAC perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (*failover test*) keberkesanannya dari semasa ke semasa.	Pengurus Keselamatan ICT/ Pentadbir Sistem ICT

BIDANG 14 :
PEMATUHAN

PERKARA	PERANAN
14.1 PEMATUHAN TERHADAP KEPERLUAN PERUNDANGAN DAN KONTRAK	
Objektif: Meningkat dan memantapkan tahap keselamatan ICT bagi mengelak dari pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	
14.1.1 PENGENALPASTIAN KEPERLUAN UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI	
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga MOTAC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MAMPU dan pembekal seperti LAMPIRAN 1.	Pengguna, Pembekal, Pakar Runding dan Pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC
14.1.2 HAK HARTA INTELEK	
Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Warga MOTAC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC
14.1.3 PERLINDUNGAN REKOD	
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.	Warga MOTAC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC

PERKARA	PERANAN
14.1.4 PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI	
MOTAC hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang- undang dan peraturan-peraturan Kerajaan Malaysia.	Warga MOTAC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC
14.1.5 PERATURAN KAWALAN KRIPTOGRAFI	
MOTAC perlu memastikan kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang dan peraturan-peraturan. Perkara yang perlu dipatuhi adalah seperti berikut: i. Sekatan ke atas pengimport/pengeksport perkakasan dan perisian komputer yang melaksanakan fungsi-fungsi kriptografi tanpa kelulusan pihak berkuasa; ii. Sekatan ke atas pengimport/pengeksport perkakasan dan perisian yang ditambah/direka untuk mempunyai fungsi kriptografi tanpa kelulusan pihak berkuasa; iii. Sekatan penggunaan enkripsi yang tidak dibenarkan; dan iv. Mematuhi kaedah akses oleh pihak berkuasa Malaysia bagi maklumat enkripsi perkakasan dan perisian.	Warga MOTAC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MOTAC

PERKARA	PERANAN
14.2 KAJIAN SEMULA KESELAMATAN MAKLUMAT	
Objektif: Memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur MOTAC.	
14.2.1 KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI	
Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	SUB/Pengarah Bahagian/Pemilik Perkhidmatan
14.2.2 PEMATUHAN POLISI DAN STANDARD KESELAMATAN	
MOTAC hendaklah membuat kajian semula secara berkala terhadap pematuhan polisi dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian.	SUB/Pengarah Bahagian/Pemilik Perkhidmatan
14.2.3 KAJIAN SEMULA PEMATUHAN TEKNIKAL	
MOTAC hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.	SUB/Pengarah Bahagian/Pemilik Perkhidmatan

LAMPIRAN 1

SENARAI PERUNDANGAN DAN PERATURAN

1. Akta Rahsia Rasmi 1972 [Akta 88];
2. Perintah – Perintah Am;
3. Arahan Perbendaharaan;
4. Pekeliling Perbendaharaan Malaysia PK 2/2013 – Kaedah Perolehan Kerajaan;
5. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama) - "Tatacara Penyediaan, Penilaian dan PenerimaanTender";
6. Surat Pekeliling Am Bilangan 3/2015 – Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Agensi Sektor Awam bertarikh 11 November 2015;
7. Surat Pekeliling Perbendaharaan Bil. 3/1995 - "Peraturan Perolehan Perkhidmatan Perundingan";
8. Akta Tandatangan Digital 1997;
9. Akta Jenayah Komputer 1997;
10. Akta Hak Cipta (Pindaan) Tahun 1997;
11. Akta Komunikasi dan Multimedia 1998;
12. Akta 709 – Akta Perlindungan Data Peribadi 2010;
13. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";
14. Surat Akujanji (Pekeliling Perkhidmatan Bilangan 17 Tahun 2001);
15. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

LAMPIRAN 1

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

17. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi- Agensi Kerajaan";

18. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

19. Surat Pekeliling Am Bil. 4 Tahun 2006 – "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam";

20. Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan (TPA)";

21. Pekeliling Perkhidmatan Bil 5 2007 bertajuk "Panduan Pengurusan Pejabat" bertarikh 30 April 2007;

22. Surat Arahan Ketua Jabatan MAMPU bertarikh 1 Jun 2007 "Langkah-langkah mengenai penggunaan Mel Elektronik Agensi–Agensi Kerajaan", Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan *Government Unified Communication* (MyGovUC);

23. Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan dan Penggunaan Aplikasi *Digital Document Management System* (DDMS) Sektor Awam bertarikh 25 Januari 2015;

24. 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";

25. Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk "Penggunaan Media Jaringan Sosial di Sektor Awam";

26. Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2013 Dalam Sektor Awam;

LAMPIRAN 1

27. Pekeliling Kemajuan Pentadbiran Awam Bilangan 3 Tahun 2015 bertajuk "Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [*Government Public Key Infrastructure* (GPKI)]" bertarikh 23 Oktober 2015;

28. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), April 2016;

29. Arahan Keselamatan (Semakan dan Pindaan 2017);

30. MyPortfolio (Pekeliling Kemajuan Pentadbiran Awam Bil 4 Tahun 2018);

31. Pekeliling Perkhidmatan Bilangan 5 Tahun 2020. Dasar Bekerja Dari Rumah;

32. Arahan Pentadbiran Ketua Jabatan MAMPU Bilangan 4 Tahun 2020 - Polisi Keselamatan Siber MAMPU;

33. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2001 bertajuk "Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam" bertarikh 10 Jun 2021;

34. Perintah-Perintah Am;

35. Arahan Perbendaharaan;

36. Akta Keselamatan Dan Kesihatan Pekerjaan (Pindaan) 2022 (Akta A1648);

37. Pekeliling Am Bil. 1/2015 – Pelaksanaan Data Terbuka Sektor Awam;

LAMPIRAN 2

AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
KEMENTERIAN PELANCONGAN, SENI DAN BUDAYA (MOTAC)

Nama (huruf besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian / Unit : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber (PKS) Kementerian Pelancongan, Seni dan Budaya; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : .....

Tarikh : .....

PENGESAHAN PEGAWAI KESELAMATAN ICT (ICTSO)

.....

(Tandatangan & Cop Jawatan)

Kementerian Pelancongan, Seni dan Budaya

Tarikh : .....

Nota: Semua warga MOTAC perlu membaca PKS MOTAC secara keseluruhan sebelum menandatangani Surat Akuan Pematuhan PKS ini. Dokumen dicapai menerusi https://www.motac.gov.my

Kementerian Pelancongan, Seni dan Budaya
No. 2, Menara 1, Jalan P5/6
Presint 5, 62200 PUTRAJAYA

03 8000 8000
03 8891 7100
info@motac.gov.my