



JABATAN IMIGRESEN MALAYSIA (JIM)

POLISI KESELAMATAN SIBER (PKS)

VERSI 2.0

TERHAD

REKOD PINDAAN DOKUMEN

VERSI	KELULUSAN	TARIKH KUAT KUASA
1.0	JPICT	10 Oktober 2022
2.0	MKSP JPICT	30 April 2026 6 Mei 2026

ISI KANDUNGAN

1.0	Pengenalan.....	1
1.1	Ringkasan Eksekutif.....	1
1.2	Tujuan.....	1
1.3	Objektif.....	1
1.4	Pernyataan Dasar.....	2
1.5	Implikasi Ketidakpatuhan Polisi Keselamatan Siber.....	3
2.0	Tadbir Urus.....	4
3.0	Pengurusan Risiko.....	5
4.0	Prinsip Keselamatan.....	6
5.0	Bidang 1 – Kawalan Organisasi.....	7
5.1	Polisi Keselamatan Siber.....	7
5.2	Peranan dan Tanggungjawab Keselamatan Maklumat.....	8
5.3	Pengasingan Tugas.....	16
5.4	Tanggungjawab Pengurusan.....	17
5.5	Hubungan dengan Pihak Berkuasa.....	18
5.6	Hubungan dengan Kumpulan Berkepentingan yang Khusus.....	19
5.7	Perisikan Ancaman.....	19
5.8	Keselamatan Maklumat dalam Pengurusan Projek.....	20
5.9	Inventori Maklumat dan Aset Lain yang Berkaitan.....	22
5.10	Penggunaan Maklumat yang Boleh Diterima dan Aset Lain yang Berkaitan.....	23
5.11	Pemulangan Aset.....	24
5.12	Pengelasan Maklumat.....	24
5.13	Pelabelan Maklumat.....	25
5.14	Pemindahan Data dan Maklumat.....	25
5.15	Kawalan Capaian.....	28
5.16	Pengurusan Identiti.....	29
5.17	Maklumat Pengesahan Identiti.....	31
5.18	Hak Capaian.....	33
5.19	Keselamatan Maklumat dalam Hubungan dengan Pembekal....	34
5.20	Menangani Keselamatan dalam Perjanjian dengan Pembekal.	35
5.21	Mengurus Keselamatan Maklumat dalam Rantaian Bekalan ICT.	36
5.22	Memantau, Menyemak dan Mengurus Perubahan Perkhidmatan Pembekal.....	37
5.23	Keselamatan Maklumat bagi Penggunaan Perkhidmatan Pengkomputeran Awan.....	38
5.24	Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat.....	39

5.25 PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT.....	40
5.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT.....	40
5.27 PENGAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT.....	41
5.28 PENGUMPULAN BAHAN BUKTI.....	41
5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN.....	41
5.30 KESEDIAAN ICT BAGI KESINAMBUNGAN PERKHIDMATAN.....	42
5.31 KEPERLUAN PERUNDANGAN DAN KONTRAK.....	45
5.32 HAK HARTA INTELEK.....	46
5.33 PERLINDUNGAN REKOD.....	46
5.34 PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI.....	47
5.35 KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI.....	47
5.36 PEMATUHAN DASAR, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT.....	47
5.37 DOKUMENTASI PROSEDUR OPERASI STANDARD.....	48
6.0 BIDANG 2 – KAWALAN SUMBER MANUSIA.....	50
6.1 TAPISAN KESELAMATAN.....	50
6.2 TERMA DAN SYARAT PERKHIDMATAN.....	50
6.3 KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT.....	51
6.4 PROSES TATATERTIB.....	51
6.5 TANGGUNGJAWAB SELEPAS PENAMATAN PERANAN ATAU JAWATAN.....	52
6.6 PERJANJIAN KERAHSIAAN ATAU KETAKDEDAHAN.....	53
6.7 BEKERJA SECARA JARAK JAUH.....	53
6.8 PELAPORAN INSIDEN KESELAMATAN MAKLUMAT.....	55
7.0 BIDANG 3 – KAWALAN FIZIKAL.....	57
7.1 PERIMETER KESELAMATAN FIZIKAL.....	57
7.2 KEMASUKAN FIZIKAL.....	58
7.3. KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN.....	59
7.4 PEMANTAUAN KESELAMATAN FIZIKAL.....	59
7.5 PERLINDUNGAN DARIPADA ANCAMAN FIZIKAL DAN PERSEKITARAN.....	60
7.6 BEKERJA DI KAWASAN SELAMAT.....	61
7.7 POLISI MEJA KOSONG DAN SKRIN KOSONG.....	62
7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT.....	64
7.9 KESELAMATAN ASET DI LUAR PREMIS.....	66
7.10 MEDIA STORAN.....	66
7.11 UTILITI SOKONGAN.....	71
7.12 KESELAMATAN KABEL.....	71
7.13 PENYELENGGARAAN PERALATAN.....	72
7.14 PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN..	73
8.0 BIDANG 4 – KAWALAN TEKNOLOGI.....	76
8.1 POLISI PERANTI MUDAH ALIH.....	76

8.2 PENGURUSAN HAK AKSES ISTIMEWA.....	76
8.3 SEKATAN CAPAIAN MAKLUMAT.....	77
8.4 KAWALAN CAPAIAN KEPADA KOD SUMBER.....	77
8.5 PENGESAHAN IDENTITI YANG SELAMAT.....	77
8.6 PENGURUSAN KAPASITI.....	78
8.7 PERLINDUNGAN DARIPADA PERISIAN HASAD.....	79
8.8 PENGURUSAN KERENTANAN TEKNIKAL.....	81
8.9 PENGURUSAN KONFIGURASI.....	82
8.10 PENGHAPUSAN MAKLUMAT.....	82
8.11 PENYEMBUNYIAN DATA (<i>DATA MASKING</i>).....	82
8.12 PENCEGAHAN KETIRISAN DATA (<i>DATA LEAKAGE PREVENTION</i>).....	83
8.13 SANDARAN MAKLUMAT (<i>INFORMATION BACKUP</i>).....	84
8.14 LEWAHAN (<i>REDUNDANCY</i>) BAGI KEMUDAHAN PEMROSESAN MAKLUMAT.....	85
8.15 PENGELOGAN MAKLUMAT.....	85
8.16 AKTIVITI PEMANTAUAN.....	87
8.17 PENYERAGAMAN JAM.....	88
8.18 PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA.....	88
8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI.....	89
8.20 KESELAMATAN RANGKAIAN.....	89
8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN.....	91
8.22 PENGASINGAN RANGKAIAN.....	92
8.23 PENAPISAN WEB (<i>WEB FILTERING</i>).....	93
8.24 PENGGUNAAN KRIPTOGRAFI.....	93
8.25 KITAR HAYAT PEMBANGUNAN SISTEM YANG SELAMAT.....	96
8.26 KEPERLUAN KESELAMATAN APLIKASI.....	97
8.27 PRINSIP REKA BENTUK DAN KEJURUTERAAN SISTEM YANG SELAMAT.. 99	
8.28 PENGEKODAN SELAMAT.....	100
8.29 PENGUJIAN DAN PENERIMAAN KESELAMATAN SISTEM.....	101
8.30 PEMBANGUNAN SISTEM OLEH SUMBER LUAR.....	103
8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PRODUKSI.....	104
8.32 PENGURUSAN PERUBAHAN.....	105
8.33 DATA PENGUJIAN.....	108
8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PELAKSANAAN AUDIT..... 109	
LAMPIRAN A: SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER JABATAN IMIGRESEN MALAYSIA.....	110
LAMPIRAN B: SENARAI UNDANG-UNDANG YANG TERPAKAI.....	111

SINGKATAN DAN KETERANGAN

SINGKATAN	KETERANGAN
AVR	<i>Automatic Voltage Regulator</i>
BTMR	Bahagian Teknologi Maklumat dan Rekod
BYOD	<i>Bring Your Own Devices</i>
CIA	<i>Confidentiality, Integrity, Availability</i>
CCTV	<i>Closed-Circuit Television System</i>
CGSO	<i>Chief Government Security Officer</i>
CDO	<i>Chief Digital Officer</i>
CPU	<i>Central Processing Unit</i>
EA	<i>Enterprise Architecture</i>
ERT	<i>Emergency Response Team</i>
FAC	<i>Factory Acceptance Check</i>
Gen-Set	<i>Generator Set</i>
ICT	<i>Information and Communication Technology</i>
ICTSO	<i>ICT Security Officer</i>
IDS	<i>Intrusion Detection System</i>
CSIRT	<i>Jabatan Imigresen Malaysia Cyber Security Incident Response Team</i>
IP	<i>Internet Protocol</i>
IPM	<i>Independent Project Management</i>
IPS	<i>Intrusion Prevention System</i>
ISMS	<i>Information Security Management System</i>
IV&V	<i>Independent Verification and Validation</i>
JIM	Jabatan Imigresen Malaysia
JPICT	Jawatankuasa Pemandu ICT
LAN	<i>Local Area Network</i>
	<i>Malaysian Administrative Modernisation and Management Planning Unit</i>
NIISe	<i>National Integrated Immigration System</i>
PII	<i>Personally Identifiable Information</i>
PKI	<i>Public Key Infrastructure</i>
PKP	Pengurusan Kesyinambungan Perkhidmatan

SINGKATAN	KETERANGAN
PSP	Pelan Strategik Pendigitalan
RAKKSSA	Rangka Kerja Keselamatan Siber Sektor Awam
SPA	<i>Security Posture Assessment</i>
SSL	<i>Secure Socket Layer</i>
TPA	Tatacara Pengurusan Aset Alih Kerajaan
UAT	<i>User Acceptance Test</i>
UPS	<i>Uninterruptable Power Supply</i>

ISTILAH DAN KETERANGAN

ISTILAH	KETERANGAN
<i>Access Point</i>	Rangkaian yang mengandungi pengantar dan antenna untuk menghantar dan menerima signal daripada <i>remote client</i> .
Antivirus	Perisian yang mengimbas virus pada media disket storan cakera padat, pita magnetik, <i>optical disk</i> , <i>flash disk</i> , CDROM untuk sebarang kemungkinan adanya virus.
<i>Anti-theft</i>	Digunakan untuk menerangkan peralatan yang bertujuan untuk mengelakkan sesuatu daripada dicuri.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
<i>Authenticity</i>	Kesahihan.
<i>Backup</i> (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat.
<i>Burn Test</i>	Komputer, peranti atau komponen dijalankan untuk jangka masa yang panjang untuk mengenal pasti sebarang masalah yang mungkin berlaku.
CCTV	Sistem TV yang digunakan secara komersial di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
Chief Digital Officer (CDO)	Ketua Pegawai Digital yang bertanggungjawab dalam menentukan strategi dan melaksanakan inisiatif ICT bagi mencapai visi dan objektif pembangunan dan penggunaan ICT sesebuah organisasi.
<i>Clear Screen</i>	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja apabila pengguna tidak berada di tempatnya.
<i>Clear Desk</i>	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
<i>Control measure</i>	Langkah atau tindakan yang dilakukan untuk mengurangkan risiko dan mencegah bahaya.
<i>Counter measure</i>	Langkah atau tindakan yang diambil untuk mengatasi atau mengimbangi yang lain.
<i>Covert Channel</i>	Saluran dalam sistem yang tidak disengajakan atau tidak dibenarkan yang membolehkan dua entiti yang bekerjasama memindahkan maklumat dengan cara yang melanggar dasar keselamatan sistem tetapi tidak melebihi kebenaran capaian entiti.

ISTILAH	KETERANGAN
<i>Defence-in-depth</i>	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
<i>Diagnostic</i>	Urutan atur cara komputer automatik yang menentukan status operasi dalam perisian, perkakasan, atau sebarang gabungannya dalam komponen, sistem atau rangkaian sistem.
<i>Denial-of-Service</i>	Halangan pemberian perkhidmatan.
<i>Dongle</i>	Alat elektronik yang dipasang pada <i>port</i> penyambung komputer seperti <i>port</i> bersiri, selari, atau USB yang mengandungi, nombor siri, kunci dan sebahagian atau keseluruhan algoritma penyahsulitan.
Enkripsi (<i>encryption</i>)	Proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
<i>Escrow</i>	Sebarang sistem yang membuat salinan kunci penyulitan supaya boleh dicapai oleh individu yang dibenarkan pada bila-bila masa.
<i>Firewall</i> / Tembok api	Satu alat yang berfungsi sebagai sistem pertahanan di dalam sistem rangkaian yang menghadkan akses ke dalam rangkaian setempat (LAN) berdasarkan kepada polisi keselamatan yang telah ditakrifkan.
<i>Fraud</i>	Penipuan atau jenayah untuk tujuan kewangan atau peribadi.
<i>Hub</i>	Hub merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bus berbentuk bintang dan menyiarkan (<i>broadcast</i>) data yang diterima daripada sesuatu <i>port</i> kepada semua <i>port</i> yang lain.
ICT Security Officer (ICTSO)	Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
<i>Internet Protocol</i> (IP)	Protokol komunikasi utama yang digunakan untuk menyampaikan datagram (paket) dari <i>host</i> sumber (<i>source</i>) ke <i>host</i> sasaran (<i>target</i>) dalam sistem rangkaian
<i>Intrusion Prevention System</i> (IPS)	Aplikasi keselamatan rangkaian yang mengesan, memantau dan mencegah sebarang anomali atau ancaman di dalam sistem trafik rangkaian.

ISTILAH	KETERANGAN
Insiden Keselamatan	Musibah (<i>adverse event</i>) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
<i>Jailbreak</i>	Proses mengeksploitasi kelemahan peranti elektronik yang dikunci untuk memasang perisian selain daripada yang telah disediakan oleh pengilang untuk peranti itu.
Kawasan Larangan	Kawasan yang dihadkan kemasukan oleh pegawai-pegawai yang tertentu sahaja atau kawasan-kawasan premis atau sebahagian daripada premis di mana perkara-perkara terperingkat disimpan atau diuruskan atau di mana kerja terperingkat dijalankan.
Kerentanan (<i>vulnerability</i>)	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
<i>Diagnostic</i>	Program komputer untuk menentukan status operasi perisian, perkakasan atau kombinasi kedua-duanya.
Dokumen Terperingkat	Dokumen-dokumen rasmi yang dikelaskan kepada Rahsia Besar, Rahsia, Sulit dan Terhad.
Kriptografi	Sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.
<i>Libraries</i>	Koleksi sumber tidak meruap yang digunakan oleh program komputer, selalunya untuk pembangunan perisian.
<i>Local Area Network (LAN)</i>	Rangkaian kawasan tempatan (LAN) membekalkan keupayaan rangkaian ke sekumpulan komputer yang berdekatan satu sama lain, seperti di bangunan pejabat, sekolah, atau rumah.
<i>Lock screen</i>	Sistem antara muka pada komputer untuk mengehadkan akses kepada data di dalam perkakasan.
<i>Mainframe</i>	Perkakasan komputer berprestasi tinggi yang mempunyai pemproses dan memori yang besar.
Media Storan	Perkakasan yang berkaitan dengan penyimpanan data dan maklumat seperti disket, kartij, cakera padat, cakera mudah alih, pita, cakera keras dan pemacu pena.
<i>Malicious Code/ Malware</i>	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, <i>trojan</i> , <i>horse worm</i> , <i>spyware</i> , <i>phishing</i> atau sebagainya.
<i>Mobile Code</i>	Kod perisian yang dipindahkan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi-fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna.

ISTILAH	KETERANGAN
MyPortfolio	MyPortfolio adalah satu kaedah pengurusan ilmu yang memberikan penekanan kepada pengupayaan minda setiap penjawat awam dalam kerangka organisasi pembelajaran (<i>learning organisation</i>). Selain sebagai dokumen rujukan rasmi yang menghuraikan maklumat pewujudan jawatan, proses kerja dan panduan menjalankan tugas bagi jawatan tersebut dalam sesebuah organisasi juga dinyatakan dalam MyPortfolio.
<i>Non-repudiation</i>	Sesuatu kesahihan yang tidak boleh disangkal.
<i>Off site</i>	Di luar kawasan atau sesuatu rangkaian.
<i>Overriding</i>	Memanjang atau menggerakkan sesuatu.
Penghala/ <i>Router</i>	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya pencapaian Internet.
<i>Patches</i>	Perisian yang digunakan untuk membetulkan masalah dalam sistem operasi atau program perisian.
<i>Patch Panel</i>	Susunan <i>port</i> pada satu panel. Setiap <i>port</i> bersambung, melalui kabel tampalan, ke <i>port</i> lain yang terletak di tempat lain dalam bangunan.
<i>Patching</i>	Tampalan.
Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
Pemalsuan paket (<i>packet spoofing</i>)	Tindakan menyembunyikan atau penyamaran paket data yang melangkaui protokol dari mana ianya dihantar atau diterima.
Pengesahan (<i>Authentication</i>)	Kaedah untuk mengesahkan identiti pengguna, peralatan, atau entiti dalam sistem komputer sebelum kebenaran akses kepada sesuatu sistem diberikan.
Pengolahan risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksanakan berdasarkan hasil penilaian risiko.
Pentadbir Sistem	Pentadbir yang menyelenggarakan sistem aplikasi, laman web dan aplikasi mudah alih serta mengurus operasi/ sokongan teknikal.
Perisian aplikasi	Merujuk kepada perisian atau pakej yang selalu digunakan seperti <i>spreadsheet</i> dan <i>word processing</i> ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Perkara-perkara Terperingkat	Dokumen/ surat rasmi yang dikelaskan kepada Rahsia Besar, Rahsia, Sulit dan Terhad.

ISTILAH	KETERANGAN
Prinsip Kejuruteraan	Idea, peraturan atau konsep yang perlu diingat ketika menyelesaikan masalah kejuruteraan.
<i>Private WLAN</i>	Rangkaian komputer dan rangkaian wayarles internet persendirian (<i>private network</i>).
<i>Production</i>	Terma bagi fasa pengeluaran selepas aktiviti membangun, mengemaskini, menyelenggara dan pengujian sistem.
<i>Public Key Infrastructure (PKI)</i>	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui internet.
Rahsia	Merupakan dokumen rasmi, maklumat rasmi dan bahan-bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara menyebabkan kerosakan besar kepada kepentingan atau martabat negara atau memberi keuntungan besar kepada seseorang kuasa asing.
Rahsia Besar	Dokumen rasmi, maklumat rasmi dan bahan-bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada negara.
<i>Risk acceptance</i>	Penerimaan risiko.
<i>Risk stage</i>	Tahap risiko.
<i>Risk treatment plan</i>	Pelan strategi atau mitigasi terhadap risiko dan ancaman siber
<i>Rollback</i>	Proses memulihkan pangkalan data atau program kepada keadaan yang ditetapkan sebelum ini, biasanya untuk pulih daripada ralat.
<i>Rogue device</i>	Nod yang tidak dibenarkan pada rangkaian.
<i>Routing</i>	Mekanisma yang memastikan data sensitif dihantar melalui laluan komunikasi yang selamat.
<i>di-root</i>	Proses membenarkan pengguna sistem pengendalian mudah alih untuk mencapai kawalan istimewa.
Ruang Siber	Sistem-sistem teknologi maklumat dan komunikasi maklumat yang disimpan di dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem secara fizikal atau maya serta persekitaran fizikal sistem-sistem tersebut dan semua aset berkaitan dengan ICT.
<i>Screen saver</i>	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
<i>Secure Socket Layer (SSL)</i>	Protokol kriptografi.

ISTILAH	KETERANGAN
<i>Security Posture Assessment</i>	Aktiviti penilaian status dan tahap sekuriti ke atas peranti, rangkaian, atau sistem, serta kawalan dan proses untuk melindungi aset daripada ancaman siber.
<i>Server</i>	Pelayan komputer.
<i>Segregation</i>	Pecahan dalam rangkaian.
<i>Side Channel</i>	Eksplotasi keselamatan yang bertujuan untuk mengumpulkan maklumat daripada atau mempengaruhi pelaksanaan program sistem dengan mengukur atau mengeksploitasi kesan tidak langsung sistem atau perkakasnya.
<i>Spoofing</i>	<i>Spoofing</i> adalah salah satu bentuk penipuan secara maya yang dilakukan dengan cara menyamar sebagai seseorang atau pihak lain.
<i>Switch</i>	Suatu komponen jaringan komputer yang berfungsi untuk menghubungkan beberapa perangkat komputer agar dapat melakukan pertukaran paket, baik menerima, memproses, dan meneruskan data ke perangkat yang dituju.
<i>Steganography</i>	Amalan menyembunyikan mesej dalam mesej lain atau objek fizikal.
Sulit	Dokumen rasmi, maklumat rasmi dan bahan-bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan kuasa asing.
<i>Super User</i>	Akaun pengguna khas yang digunakan untuk pentadbiran sistem.
<i>Technical Service Design</i>	Proses reka bentuk teknikal melibatkan interaksi antara perkhidmatan dan pengalaman pelanggan.
Terhad	Merupakan dokumen rasmi, maklumat rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi perlu diberi tahap perlindungan.
<i>Trunking</i>	Teknik yang digunakan dalam sistem penghantaran komunikasi data untuk menyediakan banyak pengguna dengan akses ke rangkaian dengan berkongsi beberapa baris atau kekerapan.
<i>Uninterruptable Power Supply (UPS)</i>	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.

ISTILAH	KETERANGAN
Warga JIM	Personel kerajaan yang berkhidmat di JIM samada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan JIM.
<i>Whole-of-government</i>	Pendekatan bersama agensi-agensi kerajaan dalam pelaksanaan pendigitalan di sektor awam.
<i>WiFi</i>	Satu sistem untuk menyambungkan peralatan elektronik seperti komputer dan telefon pintar ke internet tanpa menggunakan wayar.
<i>Wiretapping</i>	Mengintip dengar melalui talian telefon.
<i>Wireless Access Point</i>	Peranti perkakasan rangkaian yang membenarkan peranti <i>WiFi</i> lain menyambung ke rangkaian berwayar.
WLAN	<i>Wireless Local Area Network</i> . Beberapa rangkaian komputer dan rangkaian persendirian (<i>private network</i>) dihubungkan melalui rangkaian awam (<i>public network</i>) atau internet. Ia menjadikan komputer jarak jauh yang mengakses rangkaian tertentu seperti berada di tempat yang sama dengan rangkaian tersebut, dan sambungan tersebut disulitkan.
<i>Worm</i>	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri, yang biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.
VPN	<i>Virtual Private Network</i> . Beberapa rangkaian komputer dan rangkaian persendirian (<i>private network</i>) dihubungkan melalui rangkaian awam (<i>public network</i>) atau internet. Ia menjadikan komputer jarak jauh yang mengakses rangkaian tertentu seperti berada di tempat yang sama dengan rangkaian tersebut, dan sambungan tersebut disulitkan.

1.0 PENGENALAN

1.1 RINGKASAN EKSEKUTIF

Polisi Keselamatan Siber (PKS) Jabatan Imigresen Malaysia (JIM) dibangunkan sebagai satu platform rujukan terhadap pematuhan keselamatan maklumat atau penerangan kepada perkara-perkara yang perlu dipatuhi semasa menjalankan perkhidmatan atau berurusan dengan JIM. PKS ini merupakan dokumen penting kepada JIM dan menjadi sumber rujukan kepada warga JIM, pakar runding, pembekal dan pihak berkepentingan yang mempunyai urusan dengan perkhidmatan JIM bagi memastikan kerahsiaan, kesahihan dan ketersediaan (CIA) maklumat sentiasa terpelihara.

PKS ini mengandungi peraturan-peraturan yang mesti dibaca, difahami dan dipatuhi dalam menggunakan aset teknologi maklumat (ICT) JIM. Polisi ini dibangunkan berdasarkan Standard ISO/IEC 27001 terkini yang merangkumi 4 bidang kawalan. 4 bidang kawalan memperincikan tentang tanggungjawab tadbir urus dan semua pihak yang terlibat dalam memahami dan mematuhi peraturan-peraturan keselamatan maklumat dalam melindungi aset ICT, mengurangkan kesan atau impak insiden terhadap keselamatan ICT dan memastikan perkongsian maklumat dapat dijalankan dengan teratur.

Tajuk 4 bidang kawalan yang akan diperincikan dalam dokumen ini adalah seperti berikut:

- 1. Bidang 1 – Kawalan Organisasi**
- 2. Bidang 2 – Kawalan Manusia**
- 3. Bidang 3 – Kawalan Fizikal**
- 4. Bidang 4 – Kawalan Teknologi**

1.2 TUJUAN

PKS JIM ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga JIM, pembekal, pakar runding dan pihak berkepentingan yang mempunyai urusan dengan perkhidmatan JIM dalam melindungi maklumat di premis dan persekitaran JIM juga termasuk di dalam ruang siber.

1.3 OBJEKTIF

Objektif utama PKS JIM adalah seperti berikut:

- a) Memastikan keselamatan penyampaian perkhidmatan JIM di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi kerajaan, industri dan orang awam;
- b) Memastikan kelancaran operasi dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku; dan
- c) 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.

1.4 PERNYATAAN DASAR

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

Pernyataan ini merangkumi perlindungan semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran, dan yang dibuat salinan bagi memelihara keselamatan persekitaran dan ruang siber, dan ketersediaan maklumat kepada semua pengguna yang dibenarkan.

Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

- a) Kerahsiaan (*Confidentiality*) – Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran sahaja.
- b) Integriti (*Integrity*) – Data dan maklumat hendaklah tepat, lengkap seperti asal dan kemas kini hanya boleh diubah dengan cara yang dibenarkan.
- c) Ketersediaan (*Availability*) – Data dan maklumat hendaklah boleh diakses pada bila-bila masa oleh pengguna yang sah sahaja.
- d) Tidak Boleh Disangkal (*Non-repudiation*) – Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal.
- e) Kesahihan (*Authenticity*) – Data dan maklumat hendaklah dipastikan kesahihannya dan ketepatannya.

1.5 IMPLIKASI KETIDAKPATUHAN POLISI KESELAMATAN SIBER

Ketidakpatuhan terhadap Polisi Keselamatan Siber JIM boleh mengakibatkan pelbagai implikasi yang serius, termasuk tetapi tidak terhad kepada:

a) **Risiko Keselamatan**

Ketidakpatuhan boleh menyebabkan pendedahan data sensitif, pencerobohan sistem, atau gangguan operasi, yang boleh mengakibatkan kehilangan maklumat penting atau kerosakan kepada infrastruktur digital.

b) **Gangguan Operasi**

Ketidakpatuhan boleh menyebabkan gangguan kepada operasi harian Jabatan, termasuk masa henti sistem, kehilangan data, dan kerosakan peralatan, yang boleh memberi kesan langsung kepada penyampaian perkhidmatan.

c) **Kesan Undang-Undang**

Kegagalan mematuhi polisi ini boleh menyebabkan tindakan undang-undang diambil terhadap pihak yang terlibat, termasuk denda atau tindakan undang-undang lain yang berkaitan dengan pelanggaran peraturan dan undang-undang keselamatan siber.

d) **Kerugian Kewangan**

Ketidakpatuhan boleh membawa kepada kerugian kewangan yang besar, sama ada melalui denda, kos pemulihan, atau kehilangan kepercayaan pelanggan dan pihak berkepentingan yang boleh menjejaskan kedudukan kewangan JIM.

e) **Kerosakan Reputasi**

Insiden keselamatan siber yang disebabkan oleh ketidakpatuhan boleh merosakkan reputasi JIM, mengurangkan kepercayaan pihak berkepentingan dan masyarakat umum terhadap keupayaan JIM dalam menguruskan keselamatan maklumat.

f) **Tindakan Disiplin**

Warga JIM yang didapati tidak mematuhi PKS ini boleh dikenakan tindakan disiplin, termasuk amaran, penggantungan, atau penamatan perkhidmatan, bergantung kepada tahap pelanggaran yang dilakukan.

2.0 TADBIR URUS

- a) Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKS JIM, satu (1) struktur tadbir urus iaitu Jawatankuasa Pemandu ICT (JPICT) JIM telah diwujudkan.
- b) Keahlian JPICT ini adalah seperti berikut:
 - i. Ketua Pengarah JIM (Pengerusi)
 - ii. *Chief Digital Officer* (CDO) (Ahli)
 - iii. ICT Security Officer (ICTSO) (Ahli)
 - iv. Semua Pengarah (Ahli)
 - v. Kumpulan Pengurusan dan Profesional BTMR (Ahli)
 - vi. Pegawai Keselamatan Fizikal dan Fasiliti (Ahli)
 - vii. Pegawai Aset Jabatan (Ahli)
 - viii. Pegawai Sumber Manusia (Ahli)
 - ix. Lain-lain yang berkaitan (Ahli)
 - x. Unit Pengurusan Dasar, Pengurusan Projek dan Kualiti (Urusetia)
 - xi. Bahagian Teknologi Maklumat dan Rekod (Urusetia)
- c) Bidang rujukan JPICT adalah seperti berikut:
 - i. Pelaksanaan pensijilan ISMS ke atas perkhidmatan JIM yang dikenal pasti;
 - ii. Kelulusan atas polisi, objektif dan skop pelaksanaan ISMS;
 - iii. Keputusan dan tindakan Mesyuarat Jawatankuasa ISMS bahagian masing-masing;
 - iv. Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatan-perkhidmatan JIM yang dikenal pasti;
 - v. Polisi dan objektif ISMS diwujudkan selaras dengan hala tuju strategik JIM;
 - vi. Keperluan ISMS diterapkan dalam budaya kerja kakitangan JIM;
 - vii. Sumber yang diperlukan oleh pasukan pelaksana ISMS;
 - viii. Kepentingan pengurusan ISMS yang berkesan dan pematuhan terhadap keperluannya;
 - ix. Pencapaian sasaran ISMS yang dirancang;
 - x. Arahan dan sokongan kepada Pasukan ISMS JIM bagi memastikan ISMS dapat dilaksanakan dengan berkesan; dan
 - xi. Pelaksanaan program penambahbaikan dan peningkatan ISMS yang berterusan.

3.0 PENGURUSAN RISIKO

- a) JIM hendaklah mengenal pasti risiko yang berkaitan dengan maklumat yang terlibat. Risiko adalah kebarangkalian JIM tidak dapat melaksanakan fungsi dengan baik. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam premis dan persekitaran JIM, termasuklah ruang siber.
- b) Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya **SEKALI SETAHUN** atau apabila berlaku sebarang perubahan kepada persekitaran siber JIM.
- c) Laporan Penilaian Risiko dan Pelan Penguraian Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya **SEKALI SETAHUN** oleh Bahagian masing-masing dan dimaklumkan kepada pihak pengurusan JIM.
- d) Tindakan yang sewajarnya perlu dikenal pasti untuk menghadapi kemungkinan risiko yang berlaku. Pemilihan tindakan yang boleh diambil adalah seperti berikut:
 - i. Mengurangkan risiko (*Reduce*) – menjalankan pelaksanaan kawalan yang bersesuaian;
 - ii. Menerima risiko (*Accept*) – bersedia berhadapan dengan risiko yang akan terjadi;
 - iii. Mengelak atau mencegah risiko (*Avoid*) – mengambil tindakan yang dapat mengelak atau mencegah risiko; dan
 - iv. Memindahkan risiko (*Transfer*) – memindahkan risiko kepada pihak luaran yang berkepentingan.

4.0 PRINSIP KESELAMATAN

Prinsip-prinsip yang menjadi asas kepada PKS JIM dan perlu dipatuhi adalah seperti berikut:

a) Prinsip “Perlu-Tahu”

JIM 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.

b) Hak Istimewa Minimum

Pengguna hendaklah diberikan hak keistimewaan minimum iaitu terhadap 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 mewujudkan, menyimpan, mengemaskini, 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.

c) Pengasingan Tugas

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

d) Kawalan Capaian Berdasarkan Peranan

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

e) Peminimuman Data

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

TERHAD

POLISI KESELAMATAN SIBER JIM

5.0 BIDANG 1 – KAWALAN ORGANISASI

Terdapat 37 kawalan organisasi dalam bidang 1 yang perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di JIM. Perincian kawalan organisasi seperti di bawah.

5.1. POLISI KESELAMATAN SIBER

ID	KETERANGAN	PERANAN
5.1.1	a) Pelaksanaan polisi ini akan dijalankan oleh Ketua Pengarah JIM dengan disokong oleh Jawatankuasa Pemandu ICT (JPICT) yang terdiri daripada Ketua Pegawai Maklumat, Pegawai Keselamatan ICT, Pengarah Bahagian, dan ahli-ahli yang dilantik oleh Ketua Pengarah JIM; b) Polisi Keselamatan JIM mestilah dipatuhi oleh semua warga JIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan JIM; dan c) Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan JIM kepada warga JIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan JIM.	JPICT, CDO, ICTSO, Pengarah Bahagian
5.1.2	Kajian Semula Polisi untuk Keselamatan Maklumat a) Polisi ini perlu dikaji semula secara berkala dan apabila berlaku perubahan kepada peraturan yang sedang berkuatkuasa; dan b) Sebarang pindaan hendaklah dilaksanakan seperti berikut: - Mengenal pasti dan menentukan perubahan yang diperlukan; - Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan kepada JPICT bagi tujuan pengesahan; dan - Memaklumkan pindaan yang telah disahkan oleh JPICT kepada warga JIM, pembekal, pakar runding dan pihak yang	JPICT, CDO, ICTSO, Pengarah Bahagian

	mempunyai urusan dengan perkhidmatan JIM.	
--	---	--

5.2. PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.2.1	Peranan dan Tanggungjawab Keselamatan Maklumat a) Ketua Pengarah Peranan dan tanggungjawab adalah seperti yang berikut: - Memastikan penguatkuasaan pelaksanaan PKS JIM; - Memastikan warga JIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan JIM memahami dan mematuhi peruntukan-peruntukan di bawah PKS ini; - Memastikan semua keperluan JIM seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi; - Memastikan pengurusan risiko dan program keselamatan maklumat dilaksanakan seperti yang ditetapkan di dalam polisi ini; - Melantik CDO dan ICTSO; - Memastikan pelaksanaan organisasi Keselamatan Maklumat JIM berfungsi dengan cekap dan berkesan; dan - Mempengerusikan Mesyuarat JPICT. b) Ketua Pegawai Digital (CDO) Peranan dan tanggungjawab adalah seperti yang berikut: - Meneraju inisiatif pendigitalan di kementerian/agensi melalui penggunaan data, analisis dan teknologi digital; - Mewujudkan budaya berpacuan data dalam sektor awam yang mengamalkan pendekatan <i>principle-based</i> melalui penggunaan data dan teknologi digital;	Ketua Pengarah, CDO, ICTSO, Pengarah Bahagian, Pentadbir Sistem ICT, JPICT, CSIRT, Pengguna, Pegawai Aset, Pegawai Keselamatan

ID	KETERANGAN	PERANAN
	iii. Mentransformasi penyampaian digital di kementerian/agensi berfokuskan pengalaman pelanggan (<i>customer experience</i>) yang berteraskan konsep <i>Whole-of-Government</i> melalui inovasi melibatkan perkongsian data, data terbuka dan teknologi baru muncul; iv. Menilai, menyelaras, memperaku keperluan perkhidmatan digital, <i>Technical Service Design</i> dan bajet pembangunan serta mengurus agensi sebagai pelaksana inisiatif dan projek pendigitalan; v. Meneraju perubahan melalui Penjajaran Pelan Strategik Pendigitalan (PSP) Kementerian/Negeri/Agensi; vi. Melaporkan pelaksanaan dan kemajuan transformasi pendigitalan kepada YBhg. Ketua Setiausaha melalui Mesyuarat JPICT; dan vii. Mempengerusikan Mesyuarat JPICT JIM dengan penurunan kuasa oleh Ketua Pengarah. c) Pegawai Keselamatan ICT (ICTSO) Peranan dan tanggungjawab adalah seperti yang berikut: i. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Keselamatan Maklumat JIM; ii. Merangka pengurusan risiko dan audit keselamatan maklumat berpandukan rangka kerja, polisi, pekeliling/ garis panduan yang berkuat kuasa; iii. Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan maklumat dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;	

ID	KETERANGAN	PERANAN
	iv. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan maklumat dan memperakukan langkah-langkah baik pulih dengan segera; v. Melaksanakan pematuhan PKS oleh warga JIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JIM; vi. Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber; vii. Menyedia, merangka dan melaksanakan program-program kesedaran mengenai keselamatan siber; viii. Membantu CDO dan Pengarah Bahagian dalam melaksanakan tugas- tugas yang melibatkan keselamatan maklumat; ix. Memberi penerangan dan pendedahan berkaitan Keselamatan Siber JIM kepada semua pengguna; dan x. Memantau pelaksanaan Polisi Keselamatan Siber JIM. d) Pengarah Bahagian Peranan dan tanggungjawab adalah seperti yang berikut: i. Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru; ii. Pembelian atau peningkatan perisian dan sistem komputer; iii. Perolehan teknologi dan perkhidmatan komunikasi baru; iv. Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan; v. Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/ garis panduan dan Pelan	

ID	KETERANGAN	PERANAN
	Pengurusan Keselamatan Maklumat Kerajaan yang berkuat kuasa; vi. Memastikan kajian semula dan pelaksanaan kawalan keselamatan maklumat selaras dengan keperluan jabatan; vii. Melaporkan sebarang perkara atau penemuan mengenai keselamatan maklumat kepada ICTSO untuk tindakan; viii. Memastikan penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan maklumat dilaksanakan; dan ix. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas. e) Pentadbir Sistem ICT Peranan dan tanggungjawab adalah seperti yang berikut: i. Mengambil tindakan mengikut proses dan prosedur dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan bidang tugas; ii. Menentukan ketepatan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam polisi ini; iii. Memantau aktiviti capaian sistem aplikasi pengguna; iv. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta	

ID	KETERANGAN	PERANAN
	capaian sistem dan memaklumkan kepada ICTSO untuk tindakan lanjut; v. Menganalisis dan menyimpan rekod jejak audit; vi. Menyediakan laporan mengenai aktiviti capaian secara berkala; vii. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada personel di dalam keadaan baik; viii. Menjaga kerahsiaan kata laluan aset ICT; dan ix. Menjaga kerahsiaan konfigurasi aset ICT. f) Jawatankuasa Pemandu ICT (JPICT) Peranan dan tanggungjawab Jawatankuasa Pemandu ICT adalah seperti yang terkandung dalam Surat Pekeliling Am Bil 3 Tahun 2015 ialah merancang dan menentukan keselamatan siber. g) <i>Cyber Security Incident Response Team (CSIRT)</i> Peranan dan tanggungjawab CSIRT adalah seperti yang berikut: i. Menerima dan mengesan aduan keselamatan siber serta menilai tahap ii. dan jenis insiden; iii. Merekodkan dan menjalankan siasatan awal insiden yang diterima; iv. Menangani tindak balas (<i>response</i>) insiden keselamatan maklumat dan mengambil tindakan baik pulih minimum; v. Menasihati ICTSO/ Pentadbir Sistem untuk mengambil tindakan pemulihan dan pengukuhan; vi. Menyebarkan makluman berkaitan pengukuhan keselamatan maklumat kepada Pentadbir Sistem ICT; vii. Menjalankan penilaian untuk memastikan tahap keselamatan	

ID	KETERANGAN	PERANAN
	maklumat dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; dan viii. Menetapkan aktiviti penilaian tahap keselamatan secara dalaman sekurang-kurangnya satu (1) kali setahun dan memastikan aktiviti pengukuhan berdasarkan hasil penemuan dari penilaian tersebut. h) Pengguna Peranan dan tanggungjawab pengguna adalah seperti berikut: i. Mengetahui dan memahami implikasi keselamatan maklumat kesan daripada tindakannya; ii. Menjalani tapisan keselamatan sekiranya diperlukan atau dikehendaki berurusan dengan maklumat jenis terperingkat; iii. Mematuhi prinsip-prinsip keselamatan polisi ini dan menjaga kerahsiaan maklumat Kerajaan; iv. Melaksanakan langkah-langkah perlindungan seperti berikut: 1. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; 2. Memeriksa maklumat dan menentukan ia tepat dari semasa ke semasa; 3. Menentukan maklumat sedia boleh dicapai untuk digunakan apabila diperlukan; 4. Menjaga kerahsiaan maklumat; 5. Mematuhi polisi, piawaian dan garis panduan keselamatan siber yang ditetapkan;	

ID	KETERANGAN	PERANAN
	6. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; 7. Menjaga kerahsiaan langkah-langkah keselamatan maklumat dari diketahui umum; dan 8. Memantau kawasan persekitaran sesuai untuk diduduki dan selamat dari sebarang ancaman dan melaporkan setiap kejadian yang tidak diingini; i. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CSIRT dengan segera; ii. Menghadiri program-program kesedaran mengenai keselamatan maklumat; iii. Bersetuju dengan terma dan syarat yang terkandung di dalam polisi ini; dan iv. Membaca, memahami, mematuhi polisi ini dan menandatangani 'Surat Akuan Pematuhan Polisi Keselamatan Siber Jabatan Imigresen Malaysia' (LAMPIRAN A). i) Pegawai Aset Peranan dan tanggungjawab adalah seperti yang berikut: i. Menguruskan Mesyuarat Jawatankuasa Pengurusan Aset Alih di JIM; ii. Menguruskan aset mengikut Tatacara Pengurusan Aset Alih Kerajaan (TPA) termasuk seperti: penerimaan, pendaftaran, penggunaan, penyimpanan, pemeriksaan, pindahan dan penyelenggaraan seperti yang telah ditetapkan; iii. Menguruskan tindakan pelupusan, kehilangan dan hapus kira mengikut	

ID	KETERANGAN	PERANAN
	Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang telah ditetapkan; iv. Menguruskan Verifikasi Stor (bagi Stor Pusat/ Utama) mengikut jadual; v. Mewujudkan Pelan Perancangan Pengurusan Aset yang sistematik dan berkesan bagi mengurus aktiviti-aktiviti Pengurusan Aset Alih Dan Stor termasuk mengadakan kursus atau ceramah, pemeriksaan ke atas aset di bawah selianya; dan vi. Menyediakan laporan tahunan mengenai pengurusan aset. j) Pegawai Keselamatan Peranan dan tanggungjawab adalah seperti yang berikut: i. Bertanggungjawab ke atas semua aspek keselamatan fizikal dan persekitaran termasuklah bangunan dan harta benda JIM dan Kerajaan daripada sebarang ancaman, kecurian, kebakaran dan sebagainya dengan mengambil kira langkah-langkah melindungi selaras dengan peraturan-peraturan yang ditetapkan oleh Kerajaan; ii. Mengemukakan cadangan-cadangan untuk meningkatkan keselamatan perlindungan di JIM dari masa ke semasa mengikut kesesuaian; iii. Menubuhkan jawatankuasa keselamatan di jabatan yang berperanan untuk menyelaraskan pelaksanaan kawalan keselamatan perlindungan serta menyelesaikan isu-isu yang berkaitan dalam melaksanakan kawalan keselamatan perlindungan di jabatan; iv. Mewakili jabatan dalam menghadiri mesyuarat mengenai keselamatan dari semasa ke masa dan jika diperlukan hendaklah membentangkan laporan	

ID	KETERANGAN	PERANAN
	keselamatan jabatan serta isu-isu yang tidak dapat diselesaikan di peringkat jabatan; v. Menubuhkan jawatankuasa yang akan bermesyuarat dengan serta merta jika berlaku sebarang kejadian kecemasan yang melibatkan keselamatan dokumen dan kebocoran maklumat serta harta benda Kerajaan termasuk ancaman keselamatan, pencerobohan, kebakaran, kecurian dan sebagainya; vi. Menyediakan laporan hasil mesyuarat jawatankuasa untuk dikemukakan kepada pihak berkuasa berkenaan; vii. Mengadakan pemeriksaan dari masa ke semasa ke atas bangunan, sistem pendawaian elektrik, bilik komputer, bilik dokumen dan peralatan, kawasan pejabat dan semua perkara di bawah tanggungjawabnya bagi memastikan ia dalam keadaan yang selamat dan tidak terdedah kepada ancaman risiko; viii. Menganjurkan kursus dan taklimat kesedaran keselamatan perlindungan dengan kerjasama Pejabat Ketua Pegawai Keselamatan Kerajaan bagi memastikan setiap anggota di jabatan memahami langkah-langkah serta peraturan-peraturan keselamatan perlindungan mengikut keperluan; ix. Bekerjasama rapat dengan Pegawai Keselamatan Kerajaan untuk mendapat khidmat nasihat mengenai langkah-langkah meningkatkan sistem kawalan Keselamatan perlindungan di jabatan; x. Menyelaraskan langkah-langkah keselamatan (<i>coordinate security measures</i>) dan mengadakan hubungan dengan Pegawai Keselamatan Kerajaan,	

ID	KETERANGAN	PERANAN
	Pegawai Bomba, Pegawai Polis, serta pihak-pihak lain-lain; xi. Melaksanakan tugas-tugas lain yang ditetapkan dalam peraturan-peraturan keselamatan Kerajaan yang sedang berkuat kuasa dan yang akan dipinda dari masa ke semasa.	

5.3. PENGASINGAN TUGAS

ID	KETERANGAN	PERANAN
5.3.1	Peranan dan tanggungjawab adalah seperti yang berikut: a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b) Tugas mewujudkan, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai <i>production</i>. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; d) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya; dan e) Apabila sukar untuk mencapai pengasingan tugas, kawalan keselamatan lain harus dipertimbangkan termasuk: - Pemantauan aktiviti; - Jejak audit; dan	Pengarah Bahagian

ID	KETERANGAN	PERANAN
	iii. Penyeliaan pengurusan.	

5.4. TANGGUNGJAWAB PENGURUSAN

ID	KETERANGAN	PERANAN
5.4.1	Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut: a) Pengurusan hendaklah memastikan warga JIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan JIM supaya mengamalkan keselamatan maklumat mengikut polisi dan prosedur yang telah ditetapkan. Polisi Keselamatan Siber JIM boleh dirujuk di sistem e-Patuh; b) Memastikan kakitangan JIM diberi pendedahan mengenai pengurusan keselamatan ICT diberi kepada warga JIM, dan taklimat akan diberi kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa; dan c) Memastikan proses tindakan disiplin diwujudkan supaya boleh menjadi rujukan sekiranya berlaku pelanggaran atau ketidakpatuhan terhadap Polisi Keselamatan Siber JIM, dasar-dasar, pekeliling-pekeliling atau perundangan lain yang terlibat.	Warga JIM, Pembekal, Pakar runding, Pihak yang mempunyai urusan dengan perkhidmatan ICT JIM

5.5. HUBUNGAN DENGAN PIHAK BERKUASA

ID	KETERANGAN	PERANAN
5.5.1	Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab JIM; b) Mewujud dan mengemaskini prosedur atau senarai pihak berkuasa perundangan atau pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia dan Suruhanjaya Komunikasi	Bahagian Khidmat Pengurusan JIM, Pasukan ERT, CSIRT

	Dan Multimedia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta Bomba; c) Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden; dan d) Memastikan senarai perhubungan pihak berkuasa diedarkan kepada semua pengguna atau pengguna yang berkaitan mengikut keperluan.	
--	---	--

5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS

ID	KETERANGAN	PERANAN
5.6.1	Kumpulan berkepentingan yang khusus adalah satu kumpulan atau organisasi, atau individu yang mempunyai kepakaran dalam bidang-bidang tertentu seperti kepakaran dalam teknologi maklumat yang boleh mempengaruhi atau menyediakan penyelesaian kepada JIM contohnya JDN. Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional ataupun forum bagi: a) Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat; b) Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; c) Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan d) Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	Warga JIM (Mengikut Bidang Kepakaran)

5.7 PERISIKAN ANCAMAN

ID	KETERANGAN	PERANAN
5.7.1	Maklumat berkaitan ancaman keselamatan maklumat yang berpotensi atau memberi ancaman kepada fungsi JIM perlu diperoleh dan dianalisis untuk menghasilkan maklumat perisikan berkaitan ancaman. Maklumat tentang ancaman sedia ada atau baharu akan dikumpul dan dianalisis untuk memudahkan tindakan dan mengelakkan ancaman atau mengurangkan impak kepada aset maklumat yang terlibat. Pemilik aset maklumat hendaklah melaksanakan tindakan berikut bagi meningkatkan tahap kawalan keselamatan aset: - Mengenal pasti ancaman dengan melaksanakan penilaian risiko terhadap aset maklumat; - Mengenal pasti dan melaksanakan kawalan keselamatan yang berkaitan. Kawalan keselamatan tersebut juga dijadikan sebagai satu daripada keperluan dalam kitar hayat pembangunan sistem dan penyediaan infrastruktur ICT; dan - Menjadikan ancaman sebagai satu daripada ancaman yang perlu diambil kira dalam pelaksanaan ujian keselamatan sistem dan infrastruktur ICT.	CSIRT, Pemilik Sistem

5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK

ID	KETERANGAN	PERANAN
5.8.1	Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: - Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek JIM; - Objektif Polisi Keselamatan Siber hendaklah sentiasa diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; - Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal	Warga JIM (Pasukan Projek)

ID	KETERANGAN	PERANAN
	projek untuk mengenal pasti kawalan-kawalan yang diperlukan; d) Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam Polisi Keselamatan Siber JIM; e) Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat; f) Memastikan semua pihak yang terlibat dalam sesuatu projek maklum tentang arahan berkaitan keselamatan; dan g) Memastikan aktiviti dinyatakan secara jelas dalam jadual perancangan pelaksanaan projek bagi menjamin keselamatan maklumat.	
5.8.2	Analisis dan Spesifikasi Keperluan Keselamatan Maklumat Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada. Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut: a) Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk semasa fasa konseptualisasi perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penempatan, penyelenggaraan dan pelupusan; b) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Polisi Keselamatan Siber JIM;	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; d) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data; e) Aplikasi perlu mengandungi semakan pengesahan (<i>validation</i>) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; f) Dokumentasi sistem hendaklah disediakan bagi semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya; dan g) Semua sistem yang dibangunkan sama ada secara dalaman atau luaran hendaklah menjalani sekurang-kurangnya Ujian Penerimaan Pengguna (<i>User Acceptance Test</i> (UAT)).	

5.9 INVENTORI MAKLUMAT DAN ASET LAIN YANG BERKAITAN

ID	KETERANGAN	PERANAN
5.9.1	Inventori Aset Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT JIM. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: a) JIM hendaklah mengenal pasti Pegawai Penerima Aset setiap Bahagian untuk menguruskan penerimaan aset-aset ICT bagi projek-projek JIM; b) Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa; c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan	Pegawai Penerima Aset, Pegawai Aset, Warga JIM

ID	KETERANGAN	PERANAN
	d) Pegawai Aset hendaklah mengesahkan penempatan aset ICT.	
5.9.2	Pemilikan Aset Aset yang diselenggara hendaklah menjadi hak milik JIM. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut: a) Memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset; b) Memastikan aset telah dikelaskan dan dilindungi; c) Kenal pasti dan mengkaji semula capaian ke atas aset penting setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian pengguna sedia ada berdasarkan kepada polisi kawalan capaian yang telah dibangunkan; d) Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan e) Memastikan semua jenis aset dijaga dan dipelihara dengan baik.	Pegawai Aset, Warga JIM

5.10 PENGGUNAAN MAKLUMAT YANG BOLEH DITERIMA DAN ASET LAIN YANG BERKAITAN

ID	KETERANGAN	PERANAN
5.10.1	Penggunaan Aset yang Dibenarkan Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: a) Setiap pengguna dan pemilik aset bertanggungjawab terhadap penggunaan semua aset ICT di bawah tanggungannya; b) Pengendalian aset ICT hendaklah merujuk peraturan atau pekeliling semasa yang masih berkuat kuasa; c) Pegawai Aset di setiap Bahagian perlu memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan; dan	Warga JIM

ID	KETERANGAN	PERANAN
	d) Pegawai Aset harus memantau, merekod, atau mengaudit sekurang-kurangnya sekali setahun atau mengikut keperluan sekiranya terdapat sebarang perubahan terhadap penggunaan aset ICT, sistem dan peralatan telekomunikasi. Penyalahgunaan aset perlu dilaporkan segera kepada wakil BTMR/ ICTSO/ CSIRT.	
5.10.2	Pengendalian Aset Antara langkah-langkah keselamatan yang perlu diambil kira adalah seperti yang berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, membuat salinan, penghantaran penyampaian, pertukaran dan pemusnahan; g) Menjaga kerahsiaan langkah-langkah keselamatan maklumat daripada diketahui umum; h) Memastikan ketersediaan dan kebolehcapaian maklumat untuk digunakan apabila diperlukan; i) Memaklumkan aset ICT terperingkat kepada semua pengguna yang mengendali atau mentadbir aset berkaitan supaya kawalseliaan dan pengendalian yang sewajarnya dapat dipatuhi dan dikuatkuasakan;	Warga JIM

ID	KETERANGAN	PERANAN
	j) Menjaga kerahsiaan langkah-langkah keselamatan maklumat daripada diketahui umum; dan k) Melupuskan aset ICT mengikut garis panduan Kerajaan. Khususnya data pada cakera keras, cakera padat (CD atau DVD), cakera liut dan media <i>backup</i> yang lain mesti dikosongkan atau dimusnahkan supaya data tidak dapat diekstrak (<i>extract</i>) oleh pihak yang tidak bertanggungjawab.	

5.11 PEMULANGAN ASET

ID	KETERANGAN	PERANAN
5.11.1	Warga JIM hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan, bertukar tugas, penamatan perkhidmatan atau kontrak.	Warga JIM

5.12 PENGELASAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.12.1	Setiap maklumat hendaklah diberi perlindungan atau peringkat keselamatan yang bersesuaian berdasarkan tahap kerahsiaan terutamanya melibatkan dokumen terperingkat. Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Akta Rahsia Rasmi 1972 [Akta 88]. Pengelasan maklumat adalah seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; dan d) Terhad.	Pegawai Pengelas

5.13 PELABELAN MAKLUMAT

ID	KETERANGAN	PERANAN
----	------------	---------

5.13.1	Pelabelan maklumat perlu dilaksanakan di peringkat JIM mengikut tahap sensitiviti sesuatu maklumat menggunakan tanda atau label keselamatan mengikut pengelasan maklumat seperti: a) Rahsia Besar; b) Rahsia; c) Sulit; dan d) Terhad. Pelabelan maklumat perlu dilaksanakan untuk mengelakkan kebocoran, penyalahgunaan atau pendedahan yang tidak dibenarkan terhadap sesuatu maklumat. Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan sebagaimana yang ditetapkan di dalam Surat Pekeliling Am Bil. 1 Tahun 2020 – Permakluman Pemakaian dan Penguatkuasaan Arahan Keselamatan (Semakan dan Pindaan 2017).	Warga JIM
---------------	--	-----------

5.14 PEMINDAHAN DATA DAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.14.1	Polisi dan Prosedur Pemindahan Data dan Maklumat Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; b) Terma pemindahan data, maklumat dan perisian antara JIM dengan pihak luar hendaklah dimasukkan di dalam perjanjian; c) Media yang mengandungi maklumat perlu dilindungi; d) Memastikan maklumat yang terdapat dalam e-mel hendaklah dilindungi sebaiknya;	Pengguna, Warga JIM, Pembekal

ID	KETERANGAN	PERANAN
	e) Mengehendkan dan menentukan capaian kepada pengguna yang dibenarkan sahaja; f) Mengehendkan pengedaran data untuk tujuan rasmi dan yang dibenarkan sahaja; dan g) Penggunaan perkhidmatan luar seperti aplikasi media sosial dan perkongsian fail untuk pemindahan maklumat rasmi kerajaan perlu mendapat kelulusan Pengurusan Tertinggi JIM.	
5.14.2	Perjanjian Mengenai Pemindahan Data Maklumat JIM perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara JIM dengan pihak luar. Perkara yang perlu dipertimbangkan ialah: a) Pengarah Bahagian hendaklah mengawal penghantaran dan penerimaan maklumat JIM; b) Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat JIM; c) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat seperti pemalsuan maklumat, penyelewengan data, kehilangan data dan lain-lain lagi; d) JIM hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data; dan e) Dokumen terperingkat hendaklah dikelaskan mengikut peringkat keselamatan yang telah ditetapkan dalam Arahan Keselamatan Pindaan 2017.	CDO, Pengarah Bahagian
5.14.3	Pesanan Elektronik	Warga JIM

ID	KETERANGAN	PERANAN
	Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi adalah seperti berikut: a) Sebarang e-mel rasmi hendaklah direkod ke dalam DDMS 2.0 untuk tujuan rekod; b) Menggunakan akaun atau alamat e-mel yang diperuntukkan oleh JIM sahaja. Penggunaan akaun milik pengguna lain atau berkongsi akaun adalah dilarang sama sekali; c) Setiap e-mel yang disediakan hendaklah mematuhi format yang ditetapkan oleh JIM; d) Pengguna hendaklah menghadiri sesi kesedaran pengguna supaya dapat mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; e) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; f) Hanya e-mel rasmi yang boleh digunakan untuk urusan rasmi dan e-mel persendirian (seperti yahoo.com, gmail.com, dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; g) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan <i>mailbox</i> masing-masing; h) Setiap e-mel rasmi yang dihantar dan diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; dan i) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi kapasiti yang ditetapkan oleh JDN semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz fail adalah disarankan.	

5.15 KAWALAN CAPAIAN

ID	KETERANGAN	PERANAN
5.15.1	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 yang berikut: a) Keperluan keselamatan aplikasi; b) Hak akses dan polisi klasifikasi maklumat sistem dan rangkaian; c) Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa; d) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; e) Pengasingan peranan kawalan capaian; f) Kebenaran rasmi permohonan akses; g) Keperluan semakan hak akses berkala; h) Pembatalan hak akses; i) Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan j) Capaian <i>privilege</i>.	Pemilik Perkhidmatan Digital, Pegawai Keselamatan, Pentadbir Sistem ICT
5.15.2	Capaian kepada Rangkaian dan Perkhidmatan Rangkaian Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari JIM. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:	CDO, ICTSO, Pengarah Bahagian, Pentadbir Rangkaian

ID	KETERANGAN	PERANAN
	a) Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian JIM, rangkaian agensi lain dan rangkaian awam; b) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; d) Mengawal capaian ke atas <i>diagnostic</i> dan konfigurasi <i>port</i> yang terdapat di dalam peralatan rangkaian sama ada secara fizikal atau logikal; e) Mewujudkan pecahan dalam rangkaian (<i>segregation</i>) dengan mengelaskan setiap pecahan pengguna, maklumat sistem, pelayan (<i>server</i>), <i>mainframe</i>, DB Oracle dan lain-lain mengikut <i>network segmentation</i> tersendiri; f) Memastikan kawalan terhadap <i>routing</i> di antara jabatan, agensi luar dan awam dijaga mengikut keperluan perkhidmatan Jabatan; dan g) Memastikan pemasangan <i>switch</i>, <i>router</i>, <i>wireless access point</i> mendapat kebenaran pihak BTMR.	

5.16 PENGURUSAN IDENTITI

ID	KETERANGAN	PERANAN
5.16.1	Pendaftaran dan Pembatalan Pengguna Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi: a) Akaun yang diperuntukkan oleh JIM sahaja boleh digunakan; b) Akaun pengguna mestilah unik;	Semua Pengguna dan Warga JIM

ID	KETERANGAN	PERANAN
	c) Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada JIM terlebih dahulu; d) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; e) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan JIM; f) Kebenaran akses kepada pengguna atau pihak ketiga akan diberikan setelah permohonan diluluskan oleh Pentadbir Sistem ICT atau pegawai berkaitan. Had capaian dan tempoh masa bagi akaun pengguna pihak luar diberikan berdasarkan keperluan sahaja; g) Pembekuan dan penamatan akaun pengguna boleh dilakukan oleh Pentadbir Sistem ICT atas sebab-sebab berikut: i. Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan oleh Ketua Jabatan; ii. Pengguna yang bercuti belajar melebihi tempoh enam (6) bulan seperti mana yang diluluskan oleh Ketua Pengarah; iii. Bertukar bidang tugas kerja; iv. Bertukar ke agensi lain; v. Bersara; vi. Ditamatkan perkhidmatan serta merta pembatalan; vii. Dalam prosiding dan/ atau dikenakan tindakan tatatertib serta merta pembatalan; dan viii. Meninggal dunia. h) Pembatalan akaun (pengguna yang tamat perkhidmatan, bertukar dan melanggar polisi dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; dan i) Tertakluk kepada Prosedur Akses Pengguna/ User Access dalam Perkhidmatan JIM.	

5.17 MAKLUMAT PENGESAHAN IDENTITI

ID	KETERANGAN	PERANAN
5.17.1	Pengurusan Maklumat Pengesahan Rahsia Pengguna Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.	ICTSO, Pentadbir Sistem ICT
5.17.2	Penggunaan Maklumat Pengesahan Rahsia Peranan dan tanggungjawab pengguna adalah seperti yang berikut: a) Membaca, memahami dan mematuhi polisi ini; b) Mengetahui dan memahami implikasi keselamatan maklumat kesan dari tindakannya; c) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat JIM; d) Melaksanakan langkah-langkah perlindungan seperti yang berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan melalui pemilihan, penggunaan dan pengurusan berdasarkan amalan keselamatan yang baik; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran,	Pengguna, Pentadbir Sistem ICT, Pengarah Bahagian

ID	KETERANGAN	PERANAN
	penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan maklumat daripada diketahui umum. e) Melaporkan sebarang aktiviti yang mengancam keselamatan maklumat kepada ICTSO/ CSIRT dengan segera.	
5.17.3	Sistem Pengurusan Kata Laluan Sistem pengurusan kata laluan hendaklah interaktif dan mengambil kira kualiti kata laluan yang dicipta. Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh JIM seperti yang berikut: a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna perlu menukar kata laluan semasa <i>login</i> kali pertama atau selepas <i>reset</i> kata laluan; c) Panjang kata laluan mestilah sekurang-kurangnya <u>DUA BELAS (12) AKSARA</u> dengan gabungan antara huruf, aksara khas dan nombor (<i>alphanumeric</i>) <u>KECUALI</u> bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; d) Kata laluan hendaklah diingat dan <u>TIDAK BOLEH</u> dicatat, disimpan atau didedahkan dengan apa cara sekali pun; e) Kata laluan paparan kunci (<i>lock screen</i>) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; g) Kuat kuasakan pertukaran kata laluan semasa atau selepas <i>login</i> kali pertama atau selepas <i>reset</i> kata laluan;	Pengguna, Pentadbir Sistem, ICTSO, Pengarah Bahagian

ID	KETERANGAN	PERANAN
	h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum <u>TIGA (3) KALI</u> sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; j) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna; k) Kata laluan hendaklah ditukar apabila disyaki berlakunya kebocoran atau dikompromi; dan l) Pengurusan Kata Laluan adalah tertakluk kepada prosedur yang sedia ada di JIM.	

5.18 HAK CAPAIAN

ID	KETERANGAN	PERANAN
5.18.1	Peruntukan Akses Pengguna Satu proses penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT JIM.	Pentadbir Sistem ICT, Pengarah Bahagian
5.18.2	Kajian Semula Hak Akses Pengguna Pemilik aset hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan. Pentadbir Sistem ICT perlu 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
5.18.3	Pembatalan atau Pelarasan Hak Akses Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan atau dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian, perubahan bidang tugas atau	Pentadbir Sistem ICT, Pengarah Bahagian

	diselaraskan apabila berlaku perubahan dalaman di JIM.	
--	--	--

5.19 KESELAMATAN MAKLUMAT DALAM HUBUNGAN DENGAN PEMBEKAL

ID	KETERANGAN	PERANAN
5.19.1	Polisi Keselamatan Maklumat untuk Hubungan Pembekal Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset JIM. Perkara yang perlu dipertimbangkan adalah seperti: a) Menenal pasti dan mendokumentasi jenis pembekal mengikut kategori; b) Proses kitaran hayat (<i>lifecycle</i>) yang seragam untuk menguruskan pembekal; c) Mengawal dan memantau akses pembekal; d) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; e) Jenis-jenis obligasi kepada pembekal; f) JIM bertanggungjawab untuk mewujudkan Pelan Kontingensi (<i>Contingency Plan</i>) bagi memastikan ketersediaan kemudahan pemprosesan maklumat sekiranya berlaku insiden atau gangguan terhadap perkhidmatan JIM; g) Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber JIM kepada pembekal; h) Memastikan pembekal mematuhi Akuan Akta Rahsia Rasmi 1972 (Akta 88); i) Memastikan setiap pembekal melaksanakan tapisan keselamatan menerusi sistem yang disediakan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) iaitu Sistem e-Vetting; j) Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber Jabatan Imigresen Malaysia (LAMPIRAN A);	Pengarah Bahagian, Pemilik Projek, Pembekal

ID	KETERANGAN	PERANAN
	k) Pembekal perlu mematuhi arahan keselamatan yang berkuat kuasa.	

5.20 MENANGANI KESELAMATAN DALAM PERJANJIAN DENGAN PEMBEKAL

ID	KETERANGAN	PERANAN
5.20.1	Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak JIM selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa. Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) JIM hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; b) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; c) Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan; d) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi mengikut	Pengarah Bahagian, Syarikat Pembekal

ID	KETERANGAN	PERANAN
	skala dan standard piawaian yang telah ditetapkan; e) Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal; f) Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut: - Badan penilai pihak ketiga adalah bebas dan berintegriti; - Badan penilai pihak ketiga adalah kompeten; - Kriteria penilaian; - Parameter pengujian; dan - Andaian yang dibuat berkaitan dengan skop penilaian. g) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan JIM; dan h) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh JIM.	

5.21 MENGURUS KESELAMATAN MAKLUMAT DALAM RANTAIAN BEKALAN ICT

ID	KETERANGAN	PERANAN
5.21.1	Rantaian Bekalan Teknologi Maklumat dan Komunikasi Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk.	Pengarah Bahagian, Pembekal, Pemilik Projek

ID	KETERANGAN	PERANAN
	Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b) Melaksanakan satu kaedah pemantauan yang boleh mengesahkan pembekalan produk dan perkhidmatan mematuhi keperluan keselamatan maklumat JIM; c) Pembekal utama (<i>principal</i>) hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan d) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	

5.22 MEMANTAU, MENYEMAK DAN MENGURUS PERUBAHAN PERKHIDMATAN PEMBEKAL

ID	KETERANGAN	PERANAN
5.22.1	Memantau dan Mengkaji Semula Perkhidmatan Pembekal JIM hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan c) Memaklumkan mengenai insiden keselamatan kepada pembekal/ pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	Pengarah Bahagian, Pembekal, Pemilik Projek

ID	KETERANGAN	PERANAN
5.22.2	Menguruskan Perubahan Kepada Perkhidmatan Pembekal Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahankan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti yang berikut: a) Perubahan dalam perjanjian dengan pembekal; b) Perubahan yang dilakukan oleh JIM bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, teknologi hijau, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.	Pengarah Bahagian, Pembekal, Pemilik Projek

5.23 KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN PENGKOMPUTERAN AWAN

ID	KETERANGAN	PERANAN
5.23.1	Pengurusan perkhidmatan awan ini melibatkan pelbagai aspek teknikal dan pentadbiran untuk memastikan perkhidmatan awan digunakan secara berkesan, selamat, dan sesuai dengan keperluan organisasi. Perkara berikut perlu dipatuhi oleh semua pihak yang terlibat: a) Memastikan kepatuhan terhadap keperluan perundangan, peraturan, garis panduan dan perjanjian kontrak yang berkaitan antaranya: i. PK 2.6: Perolehan Perkhidmatan Pengkomputeran Awan (<i>Cloud</i>) Sektor Awam; ii. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 Dasar	Pentadbir Perkhidmatan, Pengkomputeran Awan, Pentadbir Sistem

ID	KETERANGAN	PERANAN
	Perkhidmatan Pengkomputeran Awan Sektor Awam; dan iii. Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan dalam Perkhidmatan Awam. b) Pengurusan perkhidmatan yang disediakan oleh pembekal yang dilantik oleh pihak Kerajaan; c) Menentukan/ mentakrifkan dan memaklumkan cara/ kaedah berkaitan pengurusan risiko bagi perkhidmatan pengkomputeran awan; d) Memastikan keperluan keselamatan maklumat yang berkaitan dengan penggunaan perkhidmatan pengkomputeran awan dilaksanakan; dan e) Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	

5.24 PERANCANGAN DAN PENYEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.24.1	Tanggungjawab dan Prosedur Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden JIM adalah berdasarkan kepada Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memberikan kesedaran berkaitan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT dan	ICTSO, Pengarah Bahagian, CSIRT, Pemilik Projek/ Sistem Aplikasi

	hebahan kepada warga JIM sekiranya ada perubahan; b) Memastikan kakitangan yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan; dan c) Memastikan tindakan pengukuhan serta maklum balas yang cepat, efektif dan teratur bagi setiap insiden keselamatan maklumat.	
--	---	--

5.25 PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.25.1	Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat berdasarkan kepada Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT yang sedang berkuat kuasa.	ICTSO, CSIRT

5.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.26.1	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. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; b) Menjalankan kajian forensik sekiranya perlu; c) Menghubungi pihak yang berkenaan dengan secepat mungkin; d) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti;	ICTSO, CSIRT

	e) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; f) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; g) Menyediakan tindakan pemulihan segera; dan h) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	
--	---	--

5.27 PENGAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.27.1	Pengetahuan yang diperoleh daripada penganalisan dan penyelesaian kejadian maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya. 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

5.28 PENGUMPULAN BAHAN BUKTI

ID	KETERANGAN	PERANAN
5.28.1	JIM 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

5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN

ID	KETERANGAN	PERANAN
5.29.1	Keselamatan maklumat semasa gangguan merujuk kepada langkah-langkah dan prosedur yang diambil untuk melindungi dan mengekalkan keselamatan maklumat, data, dan sistem ICT	Ketua Jabatan, CDO, ICTSO, CSIRT,

ID	KETERANGAN	PERANAN
	semasa terjadi gangguan, bencana atau insiden yang boleh mengancam integriti dan ketersediaan maklumat. Gangguan ini termasuk pelbagai situasi seperti serangan siber, bencana alam, kebakaran, banjir, pencurian, atau insiden teknikal yang tidak diingini. Aspek penting berkaitan dengan keselamatan maklumat semasa gangguan yang perlu diberi perhatian ialah seperti yang berikut: a) Pembangunan dan pelaksanaan Pelan Perancangan Kesyinambungan Perkhidmatan (<i>Business Continuity Planning</i>) untuk memastikan penyampaian perkhidmatan JIM berfungsi dengan minimum gangguan ketika terjadi insiden; b) Pemulihan Bencana melibatkan pelan dan tindakan untuk memulihkan sistem maklumat dan data setelah bencana atau insiden; c) Perlindungan Data melibatkan salinan data secara berkala, pengekalan data yang baik, dan pelaksanaan tindakan keselamatan yang sesuai untuk melindungi data terperingkat; d) Pencegahan Serangan Siber (<i>Cybersecurity Measures</i>) melibatkan tindakan untuk mencegah serangan siber dan melindungi data dari pada ancaman siber; e) Pemulihan Sistem Pantas (<i>Quick System Recovery</i>) untuk mengurangkan masa henti ketika terjadi gangguan; f) Kawalan Fizikal ke pusat data dan peralatan komputer terhadap kepada individu yang sah untuk mencegah capaian yang tidak dibenarkan; g) Pemulihan Data memastikan keupayaan untuk memulihkan data yang hilang atau terjejas dalam insiden; h) Kesedaran Keselamatan (<i>Security Awareness</i>) untuk mengurangkan ancaman dalaman dan mencegah insiden yang disebabkan oleh kesalahan manusia;	Pasukan PKP

ID	KETERANGAN	PERANAN
	i) Pelan Komunikasi Krisis (<i>Crisis Communication Plan</i>) yang jelas untuk mengurus krisis dan insiden dengan pantas.	

5.30 KESEDIAAN ICT BAGI KESINAMBUNGAN PERKHIDMATAN

ID	KETERANGAN	PERANAN
5.30.1	Perancangan Kesenambungan Keselamatan Maklumat JIM hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, JIM perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi JIM. JIM juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Melantik pasukan tadbir urus Pengurusan Kesenambungan Perkhidmatan (PKP) JIM; b) Menetapkan polisi Pengurusan Kesenambungan Perkhidmatan (PKP); c) Mengenal pasti perkhidmatan kritikal; d) Melaksanakan Kajian Impak Perkhidmatan (<i>Business Impact Analysis-BIA</i>) dan Penilaian Risiko terhadap perkhidmatan kritikal; e) Membangunkan Pelan Induk Pengurusan Kesenambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT; f) Melaksanakan program kesedaran latihan pasukan Pengurusan Kesenambungan Perkhidmatan (PKP) dan warga JIM;	Koordinator Pengurusan Kesenambungan Perkhidmatan, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT

ID	KETERANGAN	PERANAN
	g) Melaksanakan simulasi ke atas dokumen di item (e); dan h) Melaksanakan penyelenggaraan ke atas pelan di item (e).	
5.30.2	Pelaksanaan Kesenambungan Keselamatan Maklumat JIM 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 yang berikut: a) Melaksanakan Pengurusan Kesenambungan Perkhidmatan (PKP) apabila terdapat gangguan terhadap perkhidmatan kritikal JIM yang telah dikenal pasti berdasarkan kepada Pelan Induk Pengurusan Kesenambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak Balas Kecemasan dan Pelan Pemulihan Bencana ICT terkini; b) Melaksanakan <i>post-mortem</i> dan mengemaskini pelan-pelan Pengurusan Kesenambungan Perkhidmatan (PKP); c) Mengemaskini pelan-pelan Pengurusan Kesenambungan Perkhidmatan (PKP) jika berlaku perubahan kepada fungsi kritikal JIM; d) Mengemaskini struktur tadbir urus Pengurusan Kesenambungan Perkhidmatan (PKP) JIM jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan e) Memastikan pasukan Pengurusan Kesenambungan Perkhidmatan (PKP) mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksanakan PKP.	Koordinator Pengurusan Kesenambungan Perkhidmatan (PKP), Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pemulihan Bencana ICT
5.30.3	Mengesahkan, Mengkaji Semula dan Menilai Kesenambungan Keselamatan Maklumat	Pengurusan Atasan JIM,

ID	KETERANGAN	PERANAN
	JIM hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: - Menyenaraikan senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; - Senarai kakitangan JIM dan pembekal berserta nombor yang boleh dihubungi (telefon dan e-mel). Senarai kakitangan kedua juga hendaklah disediakan sebagai menggantikan kakitangan utama yang tidak dapat hadir untuk menangani insiden; - Senarai lengkap maklumat yang memerlukan <i>backup</i> dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; - Menetapkan arahan pemulihan maklumat dan kemudahan yang berkaitan; - Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; - Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan; - Salinan Pelan Pengurusan Kesinambungan Perkhidmatan perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama; dan - Pelan Pengurusan Kesinambungan Perkhidmatan hendaklah diuji sekurang-kurangnya SETAHUN SEKALI atau apabila terdapat perubahan dalam persekitaran atau fungsi perkhidmatan untuk memastikan ia sentiasa kekal berkesan.	Koordinator Pengurusan Kecinambungan Perkhidmatan (PKP), Pasukan Tindak Balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT, Pemilik Perkhidmatan Kritikal JIM dalam Pengurusan Kecinambungan Perkhidmatan (PKP), Warga JIM

5.31 KEPERLUAN PERUNDANGAN DAN KONTRAK

ID	KETERANGAN	PERANAN
5.31.1	Pengenalpastian Keperluan Undang Undang dan Kontrak Yang Terpakai Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga JIM, pembekal, pakar runding dan pihak berkepentingan yang mempunyai urusan dengan perkhidmatan ICT JIM. Senarai keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh warga JIM, pembekal, pakar runding dan pihak berkepentingan adalah seperti di LAMPIRAN B.	Warga JIM, Pembekal, Pakar Runding, Pihak Berkepentingan yang mempunyai urusan dengan ICT JIM

5.32 HAK HARTA INTELEK

ID	KETERANGAN	PERANAN
5.32.1	Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan pelesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Pematuhan terhadap hak cipta yang berkaitan dengan perisian hak milik (<i>proprietary</i>), dan reka bentuk yang diperolehi oleh JIM; b) Pematuhan terhadap pelesenan menghadkan penggunaan produk, perisian, reka bentuk dan bahan-bahan lain yang diperolehi oleh JIM; c) Pematuhan yang berterusan terhadap hak cipta produk dan keperluan pelesenan; dan d) Perisian atau sistem maklumat yang dibangunkan oleh JIM adalah menjadi harta intelek JIM.	Warga JIM, Pembekal, Pakar Runding, Pihak Berkepentingan yang mempunyai urusan dengan perkhidmatan ICT JIM

ID	KETERANGAN	PERANAN

5.33 PERLINDUNGAN REKOD

ID	KETERANGAN	PERANAN
5.33.1	Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Pengekalan, penyimpanan, pengendalian dan pelupusan rekod dan maklumat (Rujuk Dasar Pengurusan Rekod dan Arkib Elektronik 2003); b) Jadual pelupusan rekod perlu dikenal pasti; dan c) Inventori rekod.	Warga JIM, Pembekal, Pakar Runding, Pihak Berkepentingan yang mempunyai urusan dengan perkhidmatan ICT JIM

5.34 PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI

ID	KETERANGAN	PERANAN
5.34.1	JIM hendaklah memberi jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Tidak mendedahkan maklumat peribadi pengguna kepada mana-mana pihak yang tidak berkaitan; b) Memastikan kawalan penyimpanan rekod maklumat peribadi pengguna di tempat yang selamat; dan c) Maklumat peribadi pengguna hanya boleh digunakan untuk tujuan rasmi dan dengan kebenaran.	Warga JIM, Pembekal, Pakar Runding, Pihak Berkepentingan yang mempunyai urusan dengan perkhidmatan ICT JIM

5.35 KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI

ID	KETERANGAN	PERANAN
5.35.1	Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	Pengarah Bahagian, Pemilik Perkhidmatan

5.36 PEMATUHAN DASAR, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.36.1	Pematuhan Polisi dan Standard Keselamatan JIM 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. Perkara yang perlu dipatuhi adalah seperti berikut: a) Pemilik perkhidmatan perlu memastikan kajian ke atas pematuhan dan prosedur pemprosesan maklumat di dalam bidang tanggungjawab mereka selaras dengan Polisi Keselamatan Siber atau lain-lain keperluan keselamatan; b) Mengenal pasti punca-punca ketidakpatuhan; c) Menilai keperluan tindakan untuk mencapai pematuhan tindakan pembetulan hendaklah dilaksanakan; dan d) Mengkaji semula tindakan pembetulan yang diambil untuk mengesahkan keberkesanannya dan mengenal pasti kekurangan dan kelemahannya.	Pengarah Bahagian, Pemilik Perkhidmatan
5.36.2	Kajian Semula Pematuhan Teknikal JIM hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung	Pengarah Bahagian, Pemilik Perkhidmatan

ID	KETERANGAN	PERANAN
	di dalam polisi, piawaian dan keperluan komputer. Perkara yang perlu dipatuhi adalah seperti berikut: a) Sistem maklumat hendaklah dikaji sekurang-kurangnya setahun sekali atau mengikut keperluan; b) Menyelaraskan kesemua pematuhan polisi dan piawaian keselamatan maklumat JIM seperti <i>Security Posture Assessment</i>; dan c) Sebarang semakan pematuhan teknikal perlulah dilakukan oleh syarikat yang kompetan dilantik oleh JIM.	

5.37 DOKUMENTASI PROSEDUR OPERASI STANDARD

ID	KETERANGAN	PERANAN
5.37.1	Prosedur Operasi yang Didokumenkan Penyediaan dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut: a) Semua prosedur keselamatan ICT yang di wujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; c) Semua proses hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan; d) Setiap perubahan kepada prosedur operasi mestilah dikawal; dan	Pengarah Bahagian, Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	e) Tugas dan tanggungjawab perlu diasingkan bagi mengurangkan risiko kecuaiian dan penyalahgunaan aset JIM.	

6.0 BIDANG 2 – KAWALAN SUMBER MANUSIA

Terdapat 8 kawalan sumber manusia yang perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di JIM. Perincian kawalan sumber manusia seperti di bawah.

6.1 TAPISAN KESELAMATAN

ID	KETERANGAN	PERANAN
6.1.1	Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga JIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JIM yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan b) Menjalankan tapisan keselamatan contohnya e-vetting untuk warga JIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JIM yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Warga JIM, Pembekal, Pakar runding, Pihak yang mempunyai urusan dengan perkhidmatan ICT JIM

6.2 TERMA DAN SYARAT PERKHIDMATAN

ID	KETERANGAN	PERANAN
6.2.1	Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut: a) Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga JIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JIM yang terlibat dalam menjamin keselamatan aset ICT; dan b) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Warga JIM, Pembekal, Pakar runding, Pihak yang mempunyai urusan dengan perkhidmatan JIM

--	--	--

6.3 KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
6.3.1	Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber JIM dan latihan teknikal yang berkaitan dengan produk/ fungsi/ aplikasi/ sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; b) Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber JIM perlu diberi kepada Pihak Ketiga yang berkepentingan dari semasa ke semasa; c) Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat; dan d) Memastikan program menangani insiden dijalankan dari semasa ke semasa sebagai langkah proaktif untuk mengurangkan impak terhadap keselamatan maklumat dan kerajaan.	Bahagian Sumber Manusia, Warga JIM, Pembekal, Pakar runding, Pihak yang mempunyai urusan dengan perkhidmatan JIM

6.4 PROSES TATATERTIB

ID	KETERANGAN	PERANAN
6.4.1	Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Memastikan adanya proses tindakan disiplin dan/ atau undang-undang ke atas warga JIM sekiranya berlaku pelanggaran terhadap perundangan dan peraturan yang ditetapkan oleh JIM; dan b) Warga JIM yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung	Bahagian Khidmat Pengurusan

	daripada mendapat capaian kepada kemudahan ICT JIM.	
--	---	--

6.5 TANGGUNGJAWAB SELEPAS PENAMATAN PERANAN ATAU JAWATAN

ID	KETERANGAN	PERANAN
6.5.1	Penamatan atau Pertukaran Tanggungjawab Perkhidmatan a) Warga JIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JIM yang telah tamat perkhidmatan perlu mematuhi perkara-perkara berikut: i. Memastikan semua aset ICT dikembalikan kepada JIM 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 JIM dan/ atau terma perkhidmatan yang ditetapkan; iii. Maklumat rasmi JIM dalam peranti tidak dibenarkan dibawa keluar dari JIM; dan iv. Menguruskan urusan keluar, berhenti, perubahan peranan dan tanggungjawab warga JIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JIM sekiranya berlaku pertukaran atau penamatan tugas dan bidang kerja. b) Warga JIM yang telah bertukar perkhidmatan hendaklah: i. Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada JIM mengikut peraturan dan/ atau terma perkhidmatan yang ditetapkan; dan	Ketua Pembantu Tadbir

	ii. Menyediakan dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.	
--	--	--

6.6 PERJANJIAN KERAHSIAAN ATAU KETAKDEDAHAN

ID	KETERANGAN	PERANAN
6.6.1	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mewujudkan perjanjian kerahsiaan atau <i>non-disclosure agreement</i> (NDA) dengan pihak ketiga; b) Mengambil kira keperluan kerahsiaan maklumat organisasi dalam perjanjian; c) Mengkaji dan menyemak perjanjian dari semasa ke semasa serta mendokumentasikan perjanjian; dan d) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan ICT yang relevan.	ICTSO, Pengarah Bahagian, Pentadbir Sistem ICT, Pengguna, Pembekal

6.7 BEKERJA SECARA JARAK JAUH

ID	KETERANGAN	PERANAN
6.7.1	Polisi dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi apabila bekerja secara jarak jauh. Peralatan yang digunakan semasa bekerja secara jarak jauh adalah seperti komputer atau peralatan mudah alih termasuk komputer riba, <i>tablets</i>, telefon bimbit dan telefon pintar. Empat (4) perkara yang perlu diambil kira dan dipatuhi semasa melakukan telekerja atau kerja jarak jauh adalah seperti yang berikut: a) Keselamatan peralatan:	Warga JIM

ID	KETERANGAN	PERANAN
	i. Komputer mestilah dilindungi dengan perisian antivirus/ <i>antimalware</i> yang dikemaskini; ii. Memastikan perisian pada komputer dan peralatan mudah alih dilindungi dengan <i>security updates</i> yang terkini; iii. Peralatan mestilah dilindungi dengan kata laluan yang kukuh; iv. Peralatan tidak ditinggalkan tanpa pengawasan sehingga membolehkan maklumat rasmi JIM terdedah, dipinda atau dihapus secara sengaja atau tidak sengaja; dan v. Peralatan milik JIM yang dibawa keluar perlu dilindungi daripada kehilangan, kerosakan, kecurian, salah guna atau gangguan ke atas peralatan berkenaan. b) Penggunaan rangkaian: i. Menggunakan <i>mobile data</i> atau rangkaian di rumah (yang mempunyai kawalan keselamatan) semasa telekerja; dan ii. Penggunaan perkhidmatan WiFi awam tanpa kata laluan tidak digalakkan. c) Keselamatan Maklumat: dan i. Sentiasa log keluar daripada aplikasi setelah selesai urusan. Contohnya aplikasi <i>web portal</i>, e-mel rasmi; dan ii. Pengguna digalakkan mencapai dokumen secara dalam talian. Sekiranya perlu membuat cetakan, memastikan cetakan yang melibatkan dokumen rahsia rasmi sentiasa mengikut tatacara pengurusan dokumen mengikut klasifikasi maklumat. Sekiranya dokumen dibawa keluar dari JIM, pengguna perlu memastikan dokumen dibawa semula atau dikembalikan ke JIM untuk simpanan.	

ID	KETERANGAN	PERANAN
	d) Lokasi tempat kerja: i. Lokasi yang dipilih untuk telekerja mestilah bersesuaian dan terlindung daripada gangguan dan ancaman keselamatan	

6.8 PELAPORAN INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
6.8.1	Pelaporan Kejadian Keselamatan Maklumat Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT. CSIRT kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. a) Perkara yang perlu dipertimbangkan adalah seperti yang berikut: i. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang; ii. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; iii. Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan; iv. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan v. Berlaku percubaan mencerooboh, penyelewengan dan insiden yang tidak dijangka. b) Pelaporan kejadian keselamatan maklumat perlu menerangkan secara terperinci mengenai proses yang dijalankan serta merujuk <i>Service Level Agreement</i> (SLA)	ICTSO, Pengarah Bahagian, CSIRT

ID	KETERANGAN	PERANAN
	matriks yang telah ditandatangani (sekiranya berkaitan) contohnya: i. Kebiasaannya SLA yang terkandung dalam kontrak menerangkan tahap perkhidmatan yang dipersetujui melalui faktor (<i>attributes</i>) seperti ketersediaan, prestasi atau kebolekhidmatan (<i>serviceability</i>); dan ii. SLA hendaklah menjelaskan <i>threshold matrix</i> bersama dengan penalti kewangan sekiranya berlaku gangguan perkhidmatan atau pelanggaran kontrak. c) Prosedur pelaporan insiden keselamatan siber berdasarkan: i. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; ii. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam; dan iii. Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT.	
6.8.2	Pelaporan Kelemahan Maklumat Warga JIM dan pembekal yang menggunakan sistem dan perkhidmatan maklumat JIM dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT kepada ICTSO atau CSIRT.	Warga JIM, Pembekal, Pakar Runding, Pihak Berkepentingan yang mempunyai urusan dengan ICT JIM

7.0 BIDANG 3 – KAWALAN FIZIKAL

Terdapat 14 kawalan fizikal yang perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di JIM. Perincian kawalan fizikal seperti di bawah.

7.1 PERIMETER KESELAMATAN FIZIKAL

ID	KETERANGAN	PERANAN
7.1.1	Perimeter keselamatan fizikal bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan aset ICT JIM. Perkara- perkara yang perlu dipatuhi termasuk tetapi tidak terhad kepada yang berikut: a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; c) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; d) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia; e) Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; f) Mengadakan kaunter kawalan di pintu masuk yang untuk tujuan rekod kehadiran; g) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya;	Pejabat Ketua Pegawai Keselamatan Kerajaan, CDO, Bahagian Khidmat Pengurusan (Pegawai Keselamatan Fizikal dan Fasiliti JIM)

ID	KETERANGAN	PERANAN
	h) Memasang alat penggera, kamera keselamatan atau alat-alat keselamatan lain yang bersesuaian mengikut lokasi; dan i) Mengenal pasti kawasan keselamatan fizikal dengan jelas. Lokasi dan tahap keselamatan fizikal bergantung kepada keperluan untuk melindungi aset dan penilaian risiko.	

7.2 KEMASUKAN FIZIKAL

ID	KETERANGAN	PERANAN
7.2.1	Kawalan Kemasukan Fizikal Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis JIM. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Setiap pegawai dan kakitangan JIM hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada JIM apabila kakitangan bertukar, tamat perkhidmatan atau bersara; b) Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan; c) Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT JIM; d) Kehilangan pas hendaklah dilaporkan dahulu kepada pihak polis dengan segera disusuli dengan laporan kepada Pegawai Keselamatan Fizikal dan Fasiliti JIM; dan e) Setiap pegawai dan kakitangan JIM yang memasuki premis hendaklah memastikan tiada pihak luar yang tidak mempunyai akses mengekori (<i>tailgate</i>) untuk masuk bersama ke dalam premis kerja tanpa akses dan kesedaran warga JIM.	Warga JIM, Pembekal, Pakar runding, Pihak yang mempunyai urusan dengan perkhidmatan ICT JIM
7.2.2	Kawasan Penyerahan dan Pemunggahan	Warga JIM, Pembekal,

ID	KETERANGAN	PERANAN
	Titik kemasukan (<i>access point</i>) seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan. JIM hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.	Pakar perunding, Pihak yang mempunyai urusan dengan perkhidmatan ICT JIM

7.3. KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN

ID	KETERANGAN	PERANAN
7.3.1	Keselamatan Pejabat, Bilik Dan Fasiliti Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik kebal, bilik perbincangan, bilik fail, bilik kawalan CCTV dan pusat data perlu dihadkan daripada diakses tanpa kebenaran; b) Kawasan tempat bekerja, bilik dan tempat operasi maklumat perlu dihadkan daripada diakses oleh orang luar; dan c) Penunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan.	Warga JIM, Pembekal, Pakar runding, Pihak yang berkepentingan mempunyai urusan dengan perkhidmatan ICT JIM

7.4 PEMANTAUAN KESELAMATAN FIZIKAL

ID	KETERANGAN	PERANAN
7.4.1	a) Premis fizikal harus dipantau oleh sistem pengawasan termasuk pengawal, sistem pemantauan video seperti CCTV dan perisian pengurusan maklumat keselamatan fizikal	Bahagian Khidmat Pengurusan, Pentadbir Pusat Data, Warga JIM

ID	KETERANGAN	PERANAN
	sama ada diurus secara dalaman atau oleh penyedia perkhidmatan pemantauan; b) Sistem pemantauan harus dilindungi daripada capaian yang tidak dibenarkan untuk mengelakkan maklumat pengawasan, seperti suapan video, daripada dicapai oleh orang yang tidak dibenarkan atau sistem diceroboh secara jarak jauh; c) Melaksanakan pemantauan secara berterusan di premis bagi mengelakkan capaian secara fizikal yang tidak dibenarkan; dan d) Capaian kepada bangunan yang menempatkan sistem kritikal harus dipantau secara berterusan untuk mengesan capaian yang tidak dibenarkan atau tingkah laku yang mencurigakan dengan memasang sistem pemantauan video seperti CCTV untuk melihat dan merakam capaian ke kawasan sensitif di dalam dan di luar premis JIM.	

7.5 PERLINDUNGAN DARIPADA ANCAMAN FIZIKAL DAN PERSEKITARAN

ID	KETERANGAN	PERANAN
7.5.1	Perlindungan Daripada Ancaman Luar dan Persekitaran Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirancang dan dilaksanakan. JIM perlu mereka bentuk dan melaksanakan perlindungan fizikal terhadap aset daripada kebakaran, banjir, letupan, huru-hara dan bencana. a) Antara aset yang perlu dilindungi adalah: - Maklumat atau Data; - Perisian; - Perkakasan; - Sistem Sokongan atau Infrastruktur atau Utiliti; dan - Manusia.	Pentadbir Pusat Data, Bahagian Khidmat Pengurusan

ID	KETERANGAN	PERANAN
	b) Perkara yang perlu dipatuhi adalah seperti berikut: i. Merancang dan menyediakan pelan keseluruhan susun atur premis (peralatan komputer, ruang atur pejabat, bilik percetakan dan sebagainya) dengan teliti; ii. Semua ruang di pejabat khususnya yang mempunyai kemudahan maklumat hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan, seperti alat pencegahan kebakaran, pintu kalis api dan pintu kecemasan; iii. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan seperti dalam dokumen Pelan Kesyinambungan Perniagaan yang sedia ada di JIM; iv. Bahan mudah terbakar hendaklah disimpan di luar kawasan penyimpanan aset ICT; v. Pengguna dilarang merokok atau menggunakan peralatan memasak berhampiran peralatan komputer; dan vi. Semua peralatan perlindungan keselamatan dan kebakaran hendaklah diselenggara bagi memastikan ia dapat berfungsi dengan baik.	

7.6 BEKERJA DI KAWASAN SELAMAT

ID	KETERANGAN	PERANAN
7.6.1	Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga JIM yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis JIM termasuklah Pusat Data.	Pentadbir Pusat Data, Bahagian Khidmat Pengurusan

ID	KETERANGAN	PERANAN
	Kawasan ini mestilah dilindungi daripada ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut: a) Sumber data atau <i>server</i>, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik <i>server</i> atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; b) Akses adalah terhad kepada warga JIM yang telah diberi kuasa sahaja dan dipantau pada setiap masa; c) Pemantauan dibuat menggunakan <i>Closed-Circuit Television</i> (CCTV) kamera atau lain-lain peralatan yang sesuai; d) Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual; e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; f) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh lokasi berkaitan; g) Lokasi premis maklumat hendaklah tidak berhampiran dengan kawasan pemunggaran, saluran air dan laluan awam; h) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; i) Memperkukuh dinding dan siling; j) Mengehadkan jalan keluar masuk; dan k) Fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa melainkan mendapat kebenaran.	

7.7 POLISI MEJA KOSONG DAN SKRIN KOSONG

ID	KETERANGAN	PERANAN
7.7.1	Dasar meja kosong untuk kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. Semua maklumat dalam	Warga JIM, Pembekal, Pakar runding,

ID	KETERANGAN	PERANAN
	apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Meja kosong bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Pengecualian Polisi Skrin Kosong (<i>Clear Screen</i>) adalah bagi Pentadbir Sistem yang terlibat dengan pemantauan masa nyata terhadap prestasi sistem kritikal yang menggunakan paparan di dalam Tempat Larangan. Langkah-langkah yang perlu diambil termasuklah seperti yang berikut: - Menggunakan kemudahan <i>password screen saver</i> atau <i>logout</i> apabila meninggalkan komputer; - Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; - Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat; - E-mel masuk dan keluar hendaklah dikawal; dan - Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	Pihak yang mempunyai urusan dengan perkhidmatan ICT JIM
7.7.2	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:	Warga JIM, Pembekal, Pakar runding, Pihak yang mempunyai urusan dengan perkhidmatan ICT JIM

ID	KETERANGAN	PERANAN
	a) <i>Log-out</i> daripada sistem apabila selesai tugas; b) <i>Log-off</i> komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; c) Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan; dan d) Mengaktifkan mekanisme penguncian atau kawalan yang bersesuaian contohnya <i>password</i> dan <i>protected screen saver</i> .	

7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT

ID	KETERANGAN	PERANAN
7.8.1	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 yang berikut: a) Sekurang-kurangnya penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; e) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (<i>activated</i>) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;	Warga JIM, Pembekal, Pakar runding, Pihak yang mempunyai urusan dengan perkhidmatan ICT JIM

ID	KETERANGAN	PERANAN
	f) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna; g) Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; h) Peralatan-peralatan kritikal perlu disokong oleh <i>Uninterruptable Power Supply</i> (UPS) dan <i>Generator Set</i> (Gen-Set); i) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih, dan mempunyai ciri-ciri keselamatan; j) Peralatan-peralatan seperti suis, penghala, hub dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci; k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (<i>air ventilation</i>) yang sesuai; l) Peralatan ICT yang hendak dibawa keluar premis JIM, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan; m) Peralatan ICT yang hilang di pejabat hendaklah dikendalikan mengikut Tatacara Pengurusan Aset Alih Kerajaan KP 2.7/2013: Kehilangan dan Hapus Kira; n) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pentadbir Sistem ICT; p) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih; q) Sebarang pelekat selain bagi tujuan rasmi, hiasan, atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak	

ID	KETERANGAN	PERANAN
	dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; r) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal; s) Pengguna dilarang menggunakan kata laluan bagi pentadbir (<i>administrator password</i>) atau <i>default password</i> yang telah ditetapkan oleh Pentadbir Sistem ICT; t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat yang bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan JIM sahaja; dan u) Sebarang pelaksanaan <i>rogue device</i> adalah dilarang.	

7.9 KESELAMATAN ASET DI LUAR PREMIS

ID	KETERANGAN	PERANAN
7.9.1	Keselamatan Peralatan dan Aset di Luar Premis Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis JIM. Peralatan yang dibawa keluar dari premis JIM adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut: a) Peralatan perlu dilindungi dan dikawal sepanjang masa; b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; c) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan; d) Memeriksa dan memastikan peralatan yang dibawa keluar tidak mengandungi maklumat terutamanya maklumat sensitif atau terperingkat, maklumat tersebut perlu dihapuskan dari peralatan tersebut setelah disalin ke media storan sekunder;	Warga JIM, Pembekal, Pakar perunding, Pihak yang mempunyai urusan dengan perkhidmatan ICT JIM

	e) Aset ICT yang hendak dibawa keluar dari JIM perlu mendapat kebenaran dari Ketua Pengarah/ Pengarah Bahagian atau pegawai yang diturunkan kuasa untuk meluluskan pergerakan keluar aset ICT; dan f) JIM perlu mengikut Tatacara Pengurusan Aset Alih Kerajaan yang berkuatkuasa bagi menangani insiden aset yang dibawa keluar dan hilang.	
--	--	--

7.10 MEDIA STORAN

ID	KETERANGAN	PERANAN
7.10.1	Pengurusan Media Boleh Alih Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengelasan yang diguna pakai oleh JIM. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut: a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Mengehendkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) Mengehendkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; e) Menyimpan maklumat rasmi yang dibenarkan sahaja di dalam media mudah alih yang dibekalkan oleh JIM; f) Memastikan media mudah alih disimpan di ruang yang mempunyai ciri-ciri keselamatan yang baik dan sesuai untuk penyimpanan maklumat; g) Merekodkan sebarang pergerakan media mudah alih atau capaian kepada maklumat JIM; h) Mengadakan salinan atau pendua untuk maklumat di dalam media mudah alih bagi	Pentadbir Sistem ICT, Pegawai Aset, Pengguna

ID	KETERANGAN	PERANAN
	mengelakkan kehilangan maklumat atau sebarang gangguan kepada keselamatan maklumat; i) Melupuskan kandungan maklumat sekiranya media tidak lagi digunakan bagi mengelakkan salinan semula maklumat yang tidak sah; dan j) Membenarkan penggunaan pemacu media sekiranya terdapat keperluan dalam perkhidmatan.	
7.10.2	Pelupusan Media a) Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan seperti Garis Panduan Sanitasi Media Elektronik dalam Perkhidmatan Awam; b) Media yang mengandungi maklumat terperingkat hendaklah disanitisasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa; dan c) Pemilik maklumat perlu memberi kebenaran terlebih dahulu sebelum pelupusan kandungan media dapat dijalankan.	Pentadbir Sistem ICT, Pegawai Aset, Jawatankuasa yang dilantik untuk pelupusan aset
7.10.3	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 yang berikut: a) Peralatan ICT yang hendak dibawa keluar dari premis JIM untuk tujuan rasmi, perlulah mendapat kelulusan Pengarah Bahagian JIM atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; b) Aktiviti peminjaman dan pemulangan perkakasan maklumat mestilah direkodkan oleh pegawai yang berkenaan; dan	Pengguna, Pegawai Aset

ID	KETERANGAN	PERANAN
	c) Memeriksa peralatan yang dipulangkan berada dalam keadaan baik.	
7.10.4	Pemindahan Media Fizikal a) Memastikan penghantaran atau pemindahan media fizikal ke luar pejabat mengikut kepada Arahan Keselamatan; dan b) Melindungi media yang mengandungi maklumat terperingkat daripada capaian yang tidak dibenarkan semasa proses pemindahan media fizikal.	Pentadbir Sistem ICT, Pegawai Aset
7.10.5	Media Mudah Alih Persendirian Penggunaan media mudah alih persendirian tertakluk kepada peraturan konsep <i>Bring Your Own Device</i> (BYOD) yang diwujudkan. Penggunaan peralatan mudah alih di tempat kerja boleh menimbulkan risiko besar kepada keselamatan maklumat. Oleh itu, peraturan diwujudkan sekiranya terdapat keperluan bagi warga JIM, pembekal, pakar runding dan pihak-pihak lain dan peraturan perlu difahami dan dipatuhi untuk menangani ancaman atau menguruskan risiko dengan sebaiknya. Peraturan BYOD yang perlu dipatuhi setiap pengguna adalah seperti berikut: a) Sebarang bahan rasmi yang dimuat naik/ edar/ kongsi hendaklah mendapat kebenaran Ketua Jabatan; b) Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber dan Akta Rahsia Rasmi 1972 [Akta 88]; c) Memastikan peranti yang digunakan mempunyai kawalan keselamatan seperti berikut: - Menetapkan mekanisme kawalan akses bagi BYOD dan akan mengunci secara automatik apabila tidak digunakan; - Melaksanakan penyulitan dan/ atau perlindungan ke atas fail yang	Warga JIM, Pihak Luar, Pegawai Keselamatan

ID	KETERANGAN	PERANAN
	mempunyai maklumat rasmi Kerajaan yang disimpan di dalam peranti BYOD; dan iii. Memastikan BYOD mempunyai ciri-ciri piawaian keselamatan seperti antivirus, <i>patching</i> terkini dan <i>anti-theft</i>. d) Pengguna adalah dilarang daripada melakukan perkara berikut: i. Menyimpan Maklumat Rasmi di dalam BYOD; ii. Menggunakan BYOD untuk mencapai, menyimpan dan menyebarkan maklumat rasmi dan terperingkat kepada pihak yang tidak dibenarkan; iii. Menjadikan BYOD sebagai medium sandaran (<i>backup</i>) bagi maklumat rasmi; iv. Merakam komunikasi dan dokumen rasmi untuk tujuan peribadi; v. Menjadikan BYOD sebagai <i>access point</i> kepada aset ICT Jabatan untuk capaian ke internet tanpa kebenaran; dan vi. Tidak boleh mengakses peranti <i>jailbreak</i> dan <i>di-root</i>. e) Pengguna adalah tertakluk kepada perkara seperti berikut: i. Menggunakan BYOD secara berhemah sepanjang masa dan mematuhi mana-mana peraturan/ dasar yang berkuat kuasa; ii. Memadamkan segala maklumat yang berkaitan dengan urusan rasmi jabatan sekiranya bertukar/ ditamatkan perkhidmatan/ bersara ATAU sewaktu dihantar ke pusat servis untuk penyelenggaraan; iii. Bertanggungjawab dan boleh dikenakan tindakan tatatertib sekiranya didapati menyalahgunakan BYOD yang menyebabkan kehilangan/ kerosakan/ pendedahan maklumat rasmi Kerajaan;	

ID	KETERANGAN	PERANAN
	iv. Merampas mana-mana BYOD pengguna sekiranya didapati atau disyaki tidak mematuhi peraturan yang telah ditetapkan; dan v. Sekiranya peranti mudah alih pengguna hilang atau dicuri, tetapkan semula atau hapus kata laluan peranti dari jauh untuk mengelakkan akses tidak sah ke data sensitif organisasi. Pastikan aplikasi kata laluan peranti dari jauh dipasang terlebih dahulu untuk mengakses dari jarak jauh. f) Bertanggungjawab atas kehilangan, kerosakan data atau aplikasi dalam BYOD yang digunakan untuk tujuan urusan rasmi jabatan; g) Melaksanakan VPN yang menggunakan SSL untuk menyediakan akses jauh yang selamat; h) Pastikan peranti pengguna sentiasa diperbaharui dengan sistem operasi (<i>Operating System</i>) terkini dan perisian terkini, yang dapat mengelakkan dari penembusan kelemahan keselamatan peranti; dan i) Mengenakan akses WLAN JIM ketika berada di lokasi.	

7.11 UTILITI SOKONGAN

ID	KETERANGAN	PERANAN
7.11.1	Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Semua aset ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; b) Peralatan-peralatan kritikal perlu disokong oleh <i>Uninterruptible Power Supply</i> (UPS);	Warga JIM, Pembekal, Pakar runding, Pihak yang mempunyai urusan dengan perkhidmatan ICT JIM

	c) Peralatan sokongan seperti UPS dan penjana kuasa (<i>generator</i>) boleh digunakan bagi perkhidmatan kritikal seperti bilik server supaya mendapat bekalan kuasa berterusan; dan d) Semua alat sokongan perlu disemak dan diselenggara dari semasa ke semasa sekurang-kurangnya SETAHUN SEKALI atau apabila terdapat keperluan.	
--	---	--

7.12 KESELAMATAN KABEL

ID	KETERANGAN	PERANAN
7.12.1	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 yang berikut: a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan dengan bilangan yang mencukupi; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan <i>wiretapping</i>; d) Semua kabel perlu dilabelkan dengan jelas mengikut spesifikasi dan prosedur yang telah ditetapkan, dan mestilah melalui <i>trunking</i> bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat; dan e) Kawalan akses terhadap <i>patch panel</i> dan bilik kabel.	Pentadbir Sistem ICT

7.13 PENYELENGGARAAN PERALATAN

ID	KETERANGAN	PERANAN
7.13.1	Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: a) Bertanggungjawab terhadap setiap perkakasan maklumat bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; b) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; c) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pegawai Aset.	Pegawai Aset, Pentadbir Sistem ICT

7.14 PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN

ID	KETERANGAN	PERANAN
7.14.1	Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (<i>overwrite</i>) sebelum dilupuskan atau diguna semula. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada	Pegawai Aset, Pentadbir Sistem, Warga JIM

ID	KETERANGAN	PERANAN
	harta modal atau inventori yang dibekalkan oleh JIM dan ditempatkan di JIM. Peralatan ICT yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada JIM. Langkah-langkah seperti yang berikut hendaklah diambil: - Bagi peralatan ICT yang akan dilupuskan sebelum pindah milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat seperti melakukan <i>shredding</i>, <i>grinding</i>, <i>degaussing</i> atau pembakaran; - Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; - Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; - Pelupusan peralatan maklumat hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; - Pengguna maklumat adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut: - Menyimpan mana-mana peralatan maklumat yang hendak dilupuskan untuk milik peribadi; - Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman <i>CPU</i> seperti <i>RAM</i>, <i>Hard disk</i>, <i>Motherboard</i> dan sebagainya; - Menyimpan dan memindahkan perkakasan luaran komputer seperti <i>AVR</i>, <i>speaker</i> dan mana-mana peralatan	

ID	KETERANGAN	PERANAN
	yang berkaitan ke mana-mana bahagian di JIM; iv. Memindah keluar dari pejabat bagi mana-mana peralatan maklumat yang hendak dilupuskan; dan v. Melupuskan sendiri peralatan maklumat kerana kerja-kerja pelupusan di bawah tanggungjawab JIM. f) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau <i>thumbdrive</i> sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; g) 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; h) Penggunaan semula perkakasan hendaklah mendapat kebenaran daripada pemilik dan hendaklah melalui proses penghapusan maklumat menggunakan kaedah yang bersesuaian untuk membendung kebocoran atau penyalahgunaan maklumat; i) Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan (TPA)" yang berkuat kuasa; dan j) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan Tatacara Jabatan Arkib Negara.	

8.0 BIDANG 4 – KAWALAN TEKNOLOGI

Terdapat 34 kawalan teknologi yang perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di JIM. Perincian kawalan teknologi seperti di bawah.

8.1 POLISI PERANTI MUDAH ALIH

ID	KETERANGAN	PERANAN
8.1.1	Membangun serta menyebarkan polisi dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih. Perkara-perkara yang perlu dipatuhi: a) Pendaftaran ke atas peralatan mudah alih; b) Keperluan ke atas perlindungan secara fizikal; c) Kawalan ke atas pemasangan perisian peralatan mudah alih; d) Kawalan ke atas versi dan <i>patches</i> perisian; e) Sekatan ke atas akses perkhidmatan maklumat secara dalam talian; f) Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi; dan g) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Sokongan Teknikal JIM, Warga JIM

8.2 PENGURUSAN HAK AKSES ISTIMEWA

ID	KETERANGAN	PERANAN
8.2.1	Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas merujuk kepada prosedur yang berkuat kuasa di JIM.	Pentadbir Sistem ICT

8.3 SEKATAN CAPAIAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.3.1	Sekatan Akses Maklumat Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut polisi kawalan capaian seperti yang sedia ada atau yang telah dibangunkan di JIM.	Pengguna, Pentadbir Sistem, ICTSO, Pengarah Bahagian

8.4 KAWALAN CAPAIAN KEPADA KOD SUMBER

ID	KETERANGAN	PERANAN
8.4.1	Kawalan Akses Kepada Kod Sumber Program Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Log audit perlu dikekalkan kepada semua akses kepada kod sumber; b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; c) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik JIM; d) Pemantauan dan penyeliaan pembangunan kod sumber program oleh pemilik sistem; e) Penyimpanan kod sumber program dengan teratur dan selamat; dan f) Memberi capaian baca dan tulis kepada kod sumber berdasarkan keperluan dan berupaya mengawal risiko mengubah atau menyalah guna kod sumber.	Pengarah Projek, Pengurus Projek, Pentadbir Sistem ICT

8.5 PENGESAHAN IDENTITI YANG SELAMAT

ID	KETERANGAN	PERANAN
8.5.1	Prosedur Log Masuk yang Selamat Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan.	Pentadbir Sistem, ICTSO, Pengarah Bahagian

ID	KETERANGAN	PERANAN
	Langkah dan kaedah kawalan yang digunakan adalah seperti yang berikut: a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan JIM; b) Menjana amaran (<i>alert</i>) sekiranya berlaku pelanggaran semasa proses log masuk terhadap aplikasi sistem; c) Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin; d) Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna; e) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; dan f) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	

8.6 PENGURUSAN KAPASITI

ID	KETERANGAN	PERANAN
8.6.1	Kapasiti sistem maklumat hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan, kegunaan sistem ICT pada	Pemilik Sistem, Pentadbir Sistem

ID	KETERANGAN	PERANAN
	masa akan datang dan mencapai tahap perkhidmatan yang disasarkan; c) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang; d) Kos naik taraf hendaklah dibandingkan dengan kos gantian serta tempoh sokongan (<i>support</i>) perkakasan oleh pembekal sebelum sesuatu keputusan dibuat; dan e) Kapasiti sumber manusia hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluan ruang kerja adalah mencukupi dan kondusif untuk pada masa akan datang.	

8.7 PERLINDUNGAN DARIPADA PERISIAN HASAD

ID	KETERANGAN	PERANAN
8.7.1	Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan <i>malware</i> 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: a) Memasang sistem keselamatan untuk mengesan perisian atau program <i>malware</i> seperti antivirus, <i>Intrusion Detection System</i> (IDS), <i>Intrusion Prevention System</i> (IPS) atau <i>web application firewall</i> serta mengikuti prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah	Pentadbir Sistem ICT, Pengguna, CSIRT

ID	KETERANGAN	PERANAN
	mana-mana undang-undang bertulis yang berkuat kuasa; c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d) Mengemaskini antivirus dengan <i>signature/pattern</i> antivirus yang terkini; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) 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; h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus; j) Melaksanakan Program Kesedaran Pengguna yang bersesuaian; k) Penggunaan <i>mobile code</i> yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan; l) <i>Mobile code</i> yang memenuhi ciri-ciri keselamatan dan diluluskan oleh CSIRT sahaja boleh digunakan; m) Pelaksanaan Sistem Pengurusan dan Analisa Log Keselamatan (SIEM) di JIM untuk mengenal pasti, menganalisis, merekod bagi tujuan pengurusan insiden keselamatan maklumat; dan	

ID	KETERANGAN	PERANAN
	n) Laporan daripada SIEM untuk setiap aset yang terlibat termasuklah aktiviti atau kehilangan <i>security patches</i> .	
8.7.2	Perlindungan Dari Mobile Code Penggunaan <i>mobile code</i> yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan. Dalam keadaan di mana <i>mobile code</i> dibenarkan, memastikan konfigurasinya beroperasi berdasarkan kepada garis panduan atau prosedur. Penggunaan <i>mobile code</i> tidak boleh digunakan atas tujuan salah laku seperti berikut: a) Mencapai maklumat yang bukan hak miliknya; b) Akses ke sistem di mana tiada hak capaian ke atasnya; c) Menyebabkan kesesakan trafik rangkaian; d) <i>Packet Spoofing</i>; dan e) Melancarkan serangan <i>Denial-of-Service</i>, virus atau <i>malware</i>.	Pengguna

8.8 PENGURUSAN KERENTANAN TEKNIKAL

ID	KETERANGAN	PERANAN
8.8.1	Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem aplikasi dan operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;	Pentadbir Sistem ICT, CSIRT

	b) Mengenal pasti dan menganalisis tahap pendedahan dan risiko kerentanan; c) Mengambil tindakan pengolahan dan kawalan risiko; dan d) Pelaksanaan ujian penembusan ke atas aset atau sistem yang terlibat perlu dilakukan sekurang-kurangnya SETAHUN SEKALI dan sebarang penemuan kelemahan kerentanan teknikal perlu dihapuskan bagi melindungi aset dan maklumat sensitif JIM.	
--	---	--

8.9 PENGURUSAN KONFIGURASI

ID	KETERANGAN	PERANAN
8.9.1	Pengurusan konfigurasi perlu dilaksanakan untuk memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul berserta dengan keperluan keselamatan. Konfigurasi tidak diubah tanpa kebenaran berdasarkan prosedur yang ditetapkan. Perkara yang perlu dipatuhi ialah seperti yang berikut: a) Melindungi capaian terhadap fail konfigurasi mengikut kawalan yang ditetapkan; b) Merekod dan menyimpan sebarang perubahan konfigurasi dengan selamat; dan c) Memantau konfigurasi untuk mengesahkan tetapan konfigurasi dan menilai kawalan keselamatan melalui aktiviti <i>Security Posture Assessment</i> (SPA).	Pentadbir Sistem, Pentadbir Pelayan, Pentadbir Rangkaian

8.10 PENGHAPUSAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.10.1	Maklumat terperingkat yang disimpan dalam aset maklumat hendaklah dilupuskan mengikut prosedur yang ditetapkan. Perkara yang perlu dipatuhi ialah seperti berikut: a) Menentukan kaedah penghapusan maklumat yang sesuai selaras dengan keperluan JIM; b) Merekod keputusan sebagai bukti penghapusan maklumat; dan c) Mendapatkan bukti penghapusan maklumat jika menggunakan perkhidmatan pembekal.	Pemilik Maklumat, Pemilik Aset, Pegawai Aset

8.11 PENYEMBUNYIAN DATA (DATA MASKING)

ID	KETERANGAN	PERANAN
8.11.1	Penyembunyian data dilaksanakan bagi melindungi data sensitif seperti data <i>Personal Identifiable Information</i> (PII), dan data terperingkat dengan mengambil kira keperluan	Pemilik Maklumat, Pentadbir Sistem

ID	KETERANGAN	PERANAN
	perkhidmatan dan polisi kawalan capaian serta polisi lain yang berkaitan tertakluk kepada keperluan perundangan dan peraturan yang berkuat kuasa. Pelaksanaan penyembunyian data ialah berdasarkan proses penyembunyian yang ditetapkan. Penyembunyian data diperlukan bagi melindungi data PII dan data sensitif daripada terdedah atau bocor kepada pihak yang tidak bertanggung jawab yang akan menyebabkan imej JIM terjejas. Perkara yang perlu dipatuhi ialah seperti yang berikut: a) Mengetahui pasti klasifikasi data yang perlu dikongsi dengan pihak ketiga; b) Mengetahui pasti teknik yang sesuai selaras dengan sensitiviti data; dan c) Memastikan pengguna hanya dapat mencapai data yang minimum yang dibenarkan sahaja.	

8.12 PENCEGAHAN KETIRISAN DATA (*DATA LEAKAGE PREVENTION*)

ID	KETERANGAN	PERANAN
8.12.1	Data dalam sistem, rangkaian dan peralatan lain perlu dilindungi daripada pendedahan dan pengekstrakan data yang tidak sah oleh individu atau sistem. Perkara yang perlu dipatuhi ialah seperti berikut: a) Mengetahui pasti dan mengelaskan maklumat untuk dilindungi daripada ketirisan; b) Memantau saluran transaksi dan perkongsian data (contohnya e-mel, pemindahan fail, perkhidmatan peranti atau media mudah alih; dan c) Melaksanakan tindakan pengukuhan untuk mengelakkan ketirisan maklumat.	Pemilik Maklumat, Pentadbir Sistem, Pentadbir Rangkaian dan Keselamatan

TERHAD

POLISI KESELAMATAN SIBER JIM

8.13 SANDARAN MAKLUMAT (INFORMATION BACKUP)

ID	KETERANGAN	PERANAN
8.13.1	Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui oleh pihak-pihak yang berkepentingan. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan mengikut kekerapan yang telah ditetapkan dan dipersetujui oleh semua pihak berkepentingan selari dengan keperluan perkhidmatan seperti dalam SOP sedia ada di JIM. Sandaran hendaklah direkodkan dan disimpan di <i>off site</i>. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi; c) Menguji sistem sandaran sedia ada bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana seperti dalam dokumen <i>Disaster Recovery Plan</i> JIM; d) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara <u>harian, mingguan, bulanan atau tahunan</u>. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang- kurangnya <u>Tiga (3) Generasi</u>; dan e) Merekod dan menyimpan salinan sandaran di lokasi yang berlainan dan selamat.	Pentadbir Sistem ICT

8.14 LEWAHAN (*REDUNDANCY*) BAGI KEMUDAHAN PEMROSESAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.14.1	Ketersediaan Kemudahan Pemprosesan Maklumat Kemudahan Pemprosesan maklumat JIM perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (<i>failover test</i>) keberkesannya dari semasa ke semasa seperti dalam prosedur sedia ada di JIM.	Pentadbir Pusat Data, Pemilik Perkhidmatan, Pentadbir Sistem ICT

8.15 PENGELOGAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.15.1	Pengelogan Kejadian Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalan terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan. Log hendaklah disimpan dan direkodkan selaras dengan arahan/ pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. a) Jenis fail log bagi <i>server</i> dan aplikasi yang perlu diaktifkan adalah seperti yang berikut: - Fail log sistem; - Fail log servis (contoh: web, e-mel); - Fail log aplikasi (jejak audit); dan - Fail log rangkaian (contoh: <i>switch</i>, <i>firewall</i>, IPS).	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	b) ICTSO dan Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: i. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; ii. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; iii. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada pasukan CSIRT; iv. Mewujudkan prosedur untuk memantau penggunaan kemudahan memproses maklumat dan dipantau secara berkala; v. Melindungi kemudahan merekod dan maklumat log daripada pengubahsuaian atau sebarang capaian yang tidak dibenarkan; dan vi. Memastikan waktu yang berkaitan dengan sistem pemprosesan maklumat diseragamkan dengan satu sumber waktu yang ditetapkan oleh <i>National Metrology Institute of Malaysia</i> (NMIM)/SIRIM.	
8.15.2	Perlindungan Maklumat Log Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin.	Pentadbir Sistem ICT
8.15.3	Log Pentadbir dan Pengendali Aktiviti Pentadbir Sistem dan Pengendali Sistem hendaklah direkodkan dan log aktiviti tersebut	Pentadbir Sistem ICT, CSIRT

ID	KETERANGAN	PERANAN
	hendaklah dilindungi dan dikaji semula secara tetap: a) Memantau penggunaan kemudahan memproses maklumat secara berkala; b) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak disemak dari semasa ke semasa dan menyediakan laporan jika perlu; c) Kesalahan, kesilapan dan/ atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; d) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; e) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian, pemalsuan dan pencerobohan maklumat, Pentadbir Sistem ICT hendaklah melaporkan kepada pasukan CSIRT; dan f) Mewujudkan prosedur untuk memantau penggunaan kemudahan memproses maklumat.	

8.16 AKTIVITI PEMANTAUAN

ID	KETERANGAN	PERANAN
8.16.1	Rangkaian, sistem dan aplikasi harus dipantau dan tindakan sewajarnya diambil untuk menilai kemungkinan insiden keselamatan maklumat. Pentadbir Sistem perlu memantau untuk mengesan tingkah laku tidak normal (anomali) dan kemungkinan berlaku insiden keselamatan maklumat. Aktiviti pemantauan perlu merangkumi perkara seperti yang berikut: a) Trafik keluar (<i>outbound</i>) dan masuk (<i>inbound</i>) bagi rangkaian, sistem dan aplikasi;	Pentadbir Sistem, Pentadbir Rangkaian, Pentadbir Pelayan, CSIRT

ID	KETERANGAN	PERANAN
	b) Capaian kepada sistem, pelayan, peralatan rangkaian, sistem pemantauan, aplikasi kritikal; c) Log daripada peralatan keselamatan (contohnya antivirus, IDS, sistem pencegahan pencerobohan (IPS), penapis web, <i>firewall</i>, pencegahan kebocoran data); d) Log peristiwa yang berkaitan dengan sistem dan aktiviti rangkaian; e) Memastikan supaya kod sumber yang dilaksanakan telah diberi kebenaran untuk dilaksanakan dan tidak diubah tanpa kebenaran; dan f) Penggunaan dan prestasi sumber.	

8.17 PENYERAGAMAN JAM

ID	KETERANGAN	PERANAN
8.17.1	Jam bagi semua pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam JIM atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh <i>National Metrology Institute of Malaysia</i> (NMIM)/SIRIM.	Pentadbir Pusat Data, Pentadbir Rangkaian dan Keselamatan

8.18 PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA

ID	KETERANGAN	PERANAN
8.18.1	Program utiliti adalah aplikasi sistem yang melaksanakan tugas tertentu, secara amnya berkaitan dengan penyelenggaraan atau operasi sumber sistem yang optimum. Penggunaan	Pentadbir Sistem ICT, Pengarah Bahagian

	program utiliti seperti antivirus hendaklah dikawal bagi mengelakkan <i>overiding</i> sistem. Perkara yang perlu dipatuhi adalah seperti berikut: a) Hanya program atau perisian khas utiliti yang dipastikan selamat sahaja digunakan; b) Hadkan penggunaan program atau perisian khas utiliti yang membebankan kapasiti (<i>bandwidth</i>) rangkaian; c) Penggunaan program utiliti yang mempunyai hak istimewa mestilah mendapatkan kebenaran Bahagian Teknologi Maklumat dan Rekod.	
--	--	--

8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI

ID	KETERANGAN	PERANAN
8.19.1	Pemasangan Perisian pada Sistem yang Beroperasi Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan Ketua Unit Aplikasi adalah seperti yang berikut: a) Strategi <i>backup</i> perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; b) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperakui berjaya; c) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur; dan d) Pengemaskinian perisian operasi, aplikasi dan program <i>libraries</i> hanya boleh dilakukan oleh Pentadbir Sistem yang terlatih setelah mendapat kelulusan Ketua Unit.	Ketua Unit Aplikasi, Pentadbir Sistem ICT

8.20 KESELAMATAN RANGKAIAN

ID	KETERANGAN	PERANAN
8.20.1	Kawalan Rangkaian Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti yang berikut: - Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; - Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk; - Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; - Semua peralatan rangkaian hendaklah melalui proses <i>Factory Acceptance Check</i> (FAC) semasa pemasangan dan konfigurasi; - Melakukan verifikasi terhadap peralatan rangkaian yang diterima; - Semua peralatan rangkaian yang diterima akan melalui proses <i>Burn Test</i>; <i>Firewall</i> hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian dan Keselamatan; - Semua trafik keluar dan masuk rangkaian hendaklah melalui <i>firewall</i> di bawah kawalan JIM; - Semua perisian <i>sniffer</i> atau <i>network analyzer</i> adalah dilarang dipasang pada komputer pengguna KECUALI mendapat kebenaran daripada Pegawai Keselamatan Teknologi Maklumat (ICTSO); - Memasang perisian <i>Intrusion Prevention System</i> (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain	Pentadbir Sistem ICT, Pentadbir Rangkaian dan Keselamatan

ID	KETERANGAN	PERANAN
	yang boleh mengancam data dan maklumat JIM; k) Memasang <i>Web Content Filtering</i> pada <i>Internet Gateway</i> untuk menyekat aktiviti yang dilarang; l) Sebarang penyambungan rangkaian yang bukan di bawah kawalan BTMR JIM dan aktiviti penyaluran maklumat secara saluran terselindung (<i>covert channel</i>, <i>side channel</i>, <i>steganography</i> dan lain-lain) adalah tidak dibenarkan; m) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di JIM sahaja dan penggunaan modem adalah dilarang sama sekali; n) Kemudahan bagi LAN tanpa wayar hendaklah dipantau dan dikawal penggunaannya; o) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi <i>Service Level Assurance</i> (SLA) yang telah ditetapkan; p) Menempatkan atau memasang antara muka (<i>interfaces</i>) yang bersesuaian di antara rangkaian JIM, rangkaian agensi lain dan rangkaian awam; q) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; r) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; s) Mengawal capaian fizikal dan logikal ke atas kemudahan <i>port</i> diagnostik dan konfigurasi jarak jauh; t) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan JIM; dan	

ID	KETERANGAN	PERANAN
	u) Mewujud dan melaksana kawalan pengalihan laluan (<i>routing control</i>) bagi memastikan pematuhan terhadap peraturan JIM.	

8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN

ID	KETERANGAN	PERANAN
8.21.1	Pengurusan bagi semua perkhidmatan rangkaian (dalam atau <i>outsourced</i>) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian. JIM perlu mengambil kira keselamatan ICT organisasi atau menandatangani perjanjian bertulis apabila berlaku pemindahan maklumat organisasi antara JIM dengan pihak luar. Perkara yang perlu dipertimbangkan adalah: a) Mekanisme keselamatan, tahap kesediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan yang disediakan secara dalaman ataupun menggunakan sumber luar; b) Semua trafik keluar dan masuk hendaklah ditapis oleh peralatan keselamatan di bawah kawalan JIM; c) Tanggungjawab dan liabiliti sekiranya berlaku insiden keselamatan ICT seperti kehilangan data; dan d) Sebarang aktiviti yang dilarang seperti yang termaktub dalam Pekeliling Kemajuan Pentadbiran Awam (PKPA) yang berkuat kuasa perlu disekat melalui penggunaan <i>Web Content Filtering</i>.	ICTSO, Pengarah Bahagian, Pentadbir Sistem ICT, Pentadbir Rangkaian dan Keselamatan, Pembekal

8.22 PENGASINGAN RANGKAIAN

ID	KETERANGAN	PERANAN
8.22.1	Pengasingan dalam Rangkaian Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian JIM selain meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menenal pasti fungsi dan tanggungjawab pengguna; b) Mengkonfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d) Mengemaskini hak capaian pengguna dari semasa ke semasa mengikut keperluan; dan e) Operasi rangkaian mestilah diasingkan untuk meminimumkan risiko capaian yang tidak dibenarkan.	ICTSO, Pengarah Bahagian, Pentadbir Sistem ICT, Pentadbir Rangkaian dan Keselamatan

8.23 PENAPISAN WEB (WEB FILTERING)

ID	KETERANGAN	PERANAN
8.23.1	Kawalan penapisan web dalam bentuk perisian atau sebagainya perlu dilaksanakan bagi mengesan dan menyekat ke laman web yang dianggap tidak selamat dan tidak sesuai. Ini bagi melindungi sistem maklumat daripada sebarang ancaman keselamatan laman web luaran. JIM hendaklah mengurangkan risiko mencapai laman web yang mengandungi maklumat yang dilarang atau diketahui mengandungi virus atau data pancingan (<i>phishing</i>) data oleh pengguna. JIM hendaklah mengenal pasti jenis laman web yang patut atau tidak boleh dicapai oleh warga JIM. JIM hendaklah mempertimbangkan untuk menyekat capaian kepada jenis laman web yang berikut: a) Laman web yang mempunyai fungsi muat naik maklumat melainkan dibenarkan atas sebab perkhidmatan yang sah; b) Tapak web yang diketahui atau disyaki berniat jahat; c) Pelayan arahan dan kawalan (<i>command and control</i>); d) Laman web berniat jahat yang diperoleh daripada risikan ancaman; dan e) Laman web yang berkongsi kandungan haram.	Pentadbir Rangkaian dan Keselamatan

8.24 PENGGUNAAN KRIPTOGRAFI

ID	KETERANGAN	PERANAN
8.24.1	Polisi Penggunaan Kawalan Kriptografi Kriptografi merupakan proses penukaran format maklumat asal kepada format maklumat yang hanya boleh difahami menggunakan fungsi tertentu. Kriptografi merangkumi kaedah-kaedah seperti yang berikut: a) Enkripsi; dan	Pengarah Projek, ICTSO, Pentadbir Rangkaian dan Keselamatan, Pentadbir Sistem (Sub Modul

ID	KETERANGAN	PERANAN
	Sistem aplikasi yang melibatkan maklumat terperingkat seperti Rahsia Besar, Rahsia, Sulit dan Terhad hendaklah dibuat enkripsi (<i>encryption</i>). b) Tandatangan Digital. Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. Kemudahan tandatangan digital yang digunakan hendaklah mematuhi dasar dan peraturan yang berkuat kuasa seperti Akta Tandatangan Digital 1997. Antara perkara yang perlu dipatuhi adalah seperti berikut: i. Pihak yang dilantik atau diberi kuasa untuk menggunakan tandatangan digital mestilah bertanggungjawab sepenuhnya ke atas tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; dan ii. Sebarang insiden yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Dokumen Perjalanan), Pentadbir Emel (TLS)
8.24.2	Pengurusan Kunci Awam Pengurusan ke atas pengurusan Infrastruktur Kunci Awam (<i>Public Key Infrastructure</i> (PKI)) hendaklah dilakukan dengan berkesan dan selamat, dengan merujuk kepada manual yang berkaitan di JIM bagi melindungi kunci berkenaan daripada diubah, di musnah dan didedahkan sepanjang tempoh sah kunci tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pengarah Bahagian Keselamatan dan Pasport, Pentadbir Sistem (Sub Modul Dokumen Perjalanan)

ID	KETERANGAN	PERANAN
	a) Sebarang transaksi melalui aplikasi atau sistem tertentu perlu dilindungi dengan penggunaan kekunci awam bagi memastikan keselamatan data terjamin; b) Kekunci awam yang diguna pakai dalam sebarang aplikasi atau sistem hendaklah diakui sah oleh standard tempatan dan antarabangsa. c) Kekunci awam hendaklah disimpan di tempat yang selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; d) Perkongsian kekunci awam adalah DILARANG SAMA SEKALI; dan e) Sebarang perubahan atau kehilangan kekunci awam perlu dilaporkan kepada Pentadbir ICT.	
8.24.3	Pengurusan Penggunaan Kriptografi Kata kunci mestilah dilindungi menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Kata kunci mestilah dihindari daripada pengubahsuaian, pemusnahan dan penyebaran tanpa kebenaran. Penggunaan kawalan kriptografi adalah perlu terutamanya bagi melindungi maklumat terperinci dan sensitif seperti berikut: a) Maklumat perlu diklasifikasi mengikut tahap peringkat maklumat seperti Rahsia Besar, Rahsia, Sulit dan Terbuka; b) Semua maklumat terperinci perlu disulitkan (<i>encrypt</i>) sebelum dihantar keluar. Pengguna boleh melaksanakan proses penyulitan dengan menggunakan sekurang-kurangnya kata laluan pada dokumen yang perlu dihantar; c) Komputer riba yang menyimpan maklumat terperinci perlu dilaksanakan penetapan kata laluan yang kukuh terutamanya jika	Pengarah Bahagian Keselamatan dan Pasport, Pentadbir Sistem (Sub Modul Dokumen Perjalanan), Pentadbir Rangkaian dan Keselamatan

ID	KETERANGAN	PERANAN
	berada di luar premis bagi mengelakkan pencerobohan maklumat; d) Sekiranya didapati berlakunya sebarang kebocoran dan penyalahgunaan maklumat, pengguna perlu melaporkan insiden kepada CSIRT, membuat permohonan pembatalan sijil dan permohonan bagi mendapatkan sijil digital yang baru; e) Capaian jauh (<i>remote access</i>) perlu menggunakan kaedah yang selamat; dan f) Penggunaan SSL adalah diwajibkan bagi semua sistem berasaskan web yang membenarkan pertukaran maklumat.	

8.25 KITAR HAYAT PEMBANGUNAN SISTEM YANG SELAMAT

ID	KETERANGAN	PERANAN
8.25.1	Dasar Pembangunan Selamat Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti berikut: a) Keselamatan persekitaran pembangunan; b) Keselamatan pangkalan data; c) Keperluan keselamatan dalam fasa reka bentuk; d) Panduan keselamatan dalam kitar hayat pembangunan (<i>development lifecycle</i>) perisian; e) Keperluan <i>check point</i> keselamatan dalam carta perbatuan projek; f) Keperluan pengetahuan ke atas keselamatan aplikasi; g) Keselamatan repositori; h) Keselamatan dalam kawalan versi; i) Bagi pembangunan secara penyumberluaran (<i>outsourcing</i>), pembekal yang dilantik berkebolehan untuk mengenal pasti dan	ICTSO, Pengarah Bahagian, Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	menambah baik kelemahan dalam pembangunan sistem; dan j) Kod sumber perlu selamat dan bebas daripada sebarang ancaman dan pencerobohan seperti melalui SPA.	
8.25.2	Persekitaran Pembangunan Selamat Persekitaran bagi pembangunan sistem hendaklah selamat untuk melindungi keseluruhan proses pembangunan sistem (<i>development lifecycle</i>). Secara umumnya, persekitaran sistem perlu diwujudkan iaitu Persekitaran Pembangunan (<i>Development Environment</i>) dan Persekitaran Staging (<i>Staging Environment</i>) bagi memastikan kelancaran operasi pembangunan. Oleh itu, organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. JIM perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; e) Pengawal yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	Pentadbir Sistem ICT, Pengarah Bahagian

ID	KETERANGAN	PERANAN

8.26 KEPERLUAN KESELAMATAN APLIKASI

ID	KETERANGAN	PERANAN
8.26.1	Melindungi Perkhidmatan Aplikasi dalam Rangkaian Awam Maklumat aplikasi yang menggunakan rangkaian awam mestilah dilindungi daripada aktiviti yang tidak sah seperti penipuan, pendedahan maklumat, pengubahsuaian maklumat yang tidak dibenarkan yang boleh menyebabkan pertikaian kontrak. Perkara yang perlu dipertimbangkan adalah seperti berikut: a) Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi JIM. Contoh perkhidmatan sumber luaran adalah: - Perisian Sebagai Satu Perkhidmatan; - Platform Sebagai Satu Perkhidmatan; - Infrastruktur Sebagai Satu Perkhidmatan; - Storan Pengkomputeran Awan (MyGovUC); dan - Pemantauan Keselamatan. b) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala; c) Identiti pengguna perlu dikenal pasti dan disahkan bagi menentukan tahap capaian maklumat yang dibenarkan, misalnya melalui pengesahan (<i>authentication</i>);	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	d) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan penerbitan atau menandatangani dokumen transaksi; e) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan maklumat, peranan dan tanggungjawab mengikut skop yang telah ditetapkan; f) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak; g) Tanggungjawab dan liabiliti yang berkaitan dengan mana-mana kes transaksi <i>fraud</i>; h) Memastikan tiada kehilangan atau penduaan maklumat semasa proses pemindahan dilaksanakan; dan i) Memastikan pihak ketiga menandatangani akuan pematuhan, mematuhi kontrak dan peraturan keselamatan yang ditetapkan.	
8.26.2	Melindungi Transaksi Perkhidmatan Aplikasi Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti berikut: a) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi; b) Memastikan semua aspek transaksi dipatuhi: - Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan; - Mengekalkan kerahsiaan maklumat; - Mengekalkan privasi pihak yang terlibat;	ICTSO, Pengarah Bahagian, Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	iv. Komunikasi antara semua pihak yang terlibat dirahsiakan; dan v. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi; c) Pihak yang mengeluarkan dan mengekalkan tandatangan digital ialah yang dilantik oleh Kerajaan atau JIM.	

8.27 PRINSIP REKA BENTUK DAN KEJURUTERAAN SISTEM YANG SELAMAT

ID	KETERANGAN	PERANAN
8.27.1	Prinsip Kejuruteraan Sistem yang Selamat Prinsip Kejuruteraan sistem yang selamat hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada Garis Panduan dan Pelaksanaan <i>Independent Verification and Validation</i> (IV&V) sektor awam yang terkini. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan keselamatan seperti ancaman daripada bencana alam dan manusia diambil kira; b) Perlindungan maklumat dalam pembangunan sistem semasa pemprosesan, pemindahan dan penyimpanan; c) Mengambil kira kriteria di bawah dalam prinsip kejuruteraan pembangunan sistem: i. <i>Business layer</i> – berdasarkan tahap pengesahan pengguna, hanya pengguna tertentu boleh melihat data peribadi;	Pentadbir Sistem ICT, Pengarah Bahagian

ID	KETERANGAN	PERANAN
	ii. <i>Data layer</i> – hanya log masuk dengan kata laluan pangkalan data yang selamat untuk aktiviti penyenggaraan pangkalan data dibenarkan; iii. <i>Application layer</i> – penggunaan enkripsi untuk penghantaran maklumat; dan iv. <i>Technology layer</i> – penggunaan perisian sumber terbuka dan infrastruktur rangkaian.	

8.28 PENGEKODAN SELAMAT

ID	KETERANGAN	PERANAN
8.28.1	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kaedah pengkodan yang selamat perlu sentiasa dipraktiskan dengan memasukkannya sebagai satu keperluan dalam setiap fasa pembangunan aplikasi; b) Amalan pengkodan selamat boleh mengelakkan dari risiko rentanan aplikasi yang menjurus kepada ketirisan maklumat sensitif.	

8.29 PENGUJIAN DAN PENERIMAAN KESELAMATAN SISTEM

ID	KETERANGAN	PERANAN
8.29.1	Pengujian Keselamatan Sistem Pengujian fungsian keselamatan hendaklah dijalankan ke atas tiga (3) peringkat pemprosesan maklumat iaitu peringkat kemasukan data (<i>input</i>), peringkat pemprosesan data (<i>process</i>) dan peringkat penjaan laporan (<i>output</i>). Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi proses dan ketepatan maklumat;	Pentadbir Sistem ICT, ICTSO

ID	KETERANGAN	PERANAN
	b) Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; c) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan; d) Pengujian fungsi keselamatan sistem hendaklah dilaksanakan semasa fasa pembangunan; e) Semua sistem baru atau penambahbaikan sistem hendaklah menjalani ujian <i>Security Posture Assessment</i> (SPA) termasuk penyediaan jadual terperinci aktiviti, ujian <i>input</i> dan <i>output</i> (<i>input and output validation</i>); f) Mengenal pasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan perlindungan integriti data; g) Merancang dan melaksanakan penilaian risiko mengikut keperluan bagi mengenal pasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam aplikasi; dan h) Menjalankan proses semak ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan dan kesesuaian. Maklumat lanjut berkaitan pengujian keselamatan sistem boleh merujuk kepada dokumen ISO/IEC/IEEE 29119 <i>Software Testing Standard</i> dan ISO/IEC 27007 <i>Security Techniques (Guidelines for information security management systems auditing)</i>.	
8.29.2	Pengujian Penerimaan Sistem Program pengujian penerimaan sistem Ujian Penerimaan Pengguna (UAT) dan Ujian Integrasi Sistem (SIT) dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat	Pengguna, Pentadbir Sistem ICT, ICTSO

ID	KETERANGAN	PERANAN
	yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat dan kepatuhan kepada Polisi Pembangunan Selamat; b) Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem diguna pakai; c) Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan (<i>vulnerability scanner</i>); d) Memastikan proses kerja sistem memenuhi keperluan pengguna; e) Melaksanakan ujian fungsi ke atas sistem menggunakan <i>dummy input</i>, dan f) Melibatkan ujian prestasi (<i>performance test</i>), ujian tekanan (<i>stress test</i>) dan ujian bebanan (<i>load test</i>). Maklumat lanjut berkaitan boleh merujuk kepada dokumen ISO/IEC/IEEE 29119 Software Testing Standard.	

8.30 PEMBANGUNAN SISTEM OLEH SUMBER LUAR

ID	KETERANGAN	PERANAN
8.30.1	Pembangunan oleh Khidmat Luaran JIM hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara <i>outsource</i> oleh pihak luar. <i>Intellectual Property Rights</i> (IPR) dan kod sumber (<i>source code</i>) hendaklah menjadi HAK MILIK JIM. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Perkiraan pelesenan, kod sumber ialah HAK MILIK JIM dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara <i>outsource</i>; b) 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”; c) Keperluan kontrak untuk reka bentuk selamat, pengkodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik; d) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem; e) Mengguna pakai prinsip dan tatacara <i>escrow</i>; f) Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian; g) Maklumat, prosedur, dan dokumen yang digunakan semasa pembangunan secara <i>outsource</i> adalah menjadi rahsia Kerajaan yang tidak boleh disebar dan didedahkan; dan h) Setiap sistem perlu mendapatkan pengesahan JPICT sebelum pelancaran projek.	Pentadbir Sistem ICT, Pengarah Bahagian, ICTSO

TERHAD

POLISI KESELAMATAN SIBER JIM

8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PRODUKSI

ID	KETERANGAN	PERANAN
8.31.1	Pengasingan Persekitaran Pembangunan, Pengujian, Staging, Operasi dan Latihan Persekitaran pembangunan pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan pada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (<i>production</i>); b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; c) Data yang mengandungi maklumat rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat; d) Mewujudkan prosedur keperluan sumber bagi penyediaan persekitaran untuk pembangunan, pengujian dan operasi; e) Merekodkan semua penggunaan sumber yang dilaksanakan; dan f) Memantau pelaksanaan penggunaan sumber bagi tujuan perancangan kapasiti.	Pentadbir Sistem ICT
8.31.2	Persekitaran Pembangunan Selamat Persekitaran bagi pembangunan sistem hendaklah selamat untuk melindungi keseluruhan proses pembangunan sistem (<i>development lifecycle</i>). Secara umumnya, persekitaran sistem perlu diwujudkan iaitu Persekitaran Pembangunan (<i>Development</i>	Pentadbir Sistem ICT, Pengarah Bahagian

ID	KETERANGAN	PERANAN
	<i>Environment</i>) dan Persekitaran Staging (<i>Staging Environment</i>) bagi memastikan kelancaran operasi pembangunan. Oleh itu, organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. JIM perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; e) Pengawal yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	

8.32 PENGURUSAN PERUBAHAN

ID	KETERANGAN	PERANAN
8.32.1	Perubahan dalam organisasi, proses perkhidmatan, kemudahan pemprosesan maklumat, dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Pengurusan ke atas perubahan perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta melakukan penilaian semula terhadap risiko. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara berikut:	Pentadbir Sistem ICT, Pemilik Aset ICT

ID	KETERANGAN	PERANAN
	a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara menghapus dan mengemaskini mana-mana komponen sistem maklumat hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c) Semua aktiviti pengubahsuaian komponen sistem maklumat hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; d) Semua aktiviti perubahan atau pengubahsuaian hendaklah diuji jika berkenaan, disahkan, direkod, dikawal dan dipantau bagi mengelakkan berlakunya ralat sama ada secara sengaja ataupun tidak sengaja; e) Menghalang sebarang peluang untuk membocor dan memanipulasi maklumat; f) Pegawai yang telah dipertanggungjawabkan dan ditetapkan hendaklah memantau penambahbaikan, pembetulan atau perubahan yang dilakukan oleh pihak ketiga; g) Akses kepada kod sumber (<i>source code</i>) aplikasi hendaklah dihadkan kepada pegawai yang dibenarkan; dan h) Mewujudkan prosedur pengurusan perubahan.	
8.32.2	Prosedur Kawalan Perubahan Sistem Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem	Pengarah Bahagian, Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti berikut: a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan buruk terhadap operasi dan keselamatan agensi, individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh <i>vendor</i>; c) Mengawal perubahan dan/ atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; d) Capaian kepada kod sumber (<i>source code</i>) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja; dan e) Setiap permohonan perubahan/ penambahbaikan sistem menggunakan Borang Permohonan Penambahbaikan Sistem (<i>Change Request</i>) untuk memantau perubahan/ penambahbaikan yang dilaksanakan oleh pengaturcara.	
8.32.3	Kajian Semula Teknikal bagi Aplikasi Selepas Perubahan Platform Operasi Apabila platform operasi contohnya sistem operasi, pangkalan data atau platform perisian berubah, aplikasi penting perkhidmatan hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi. Perkara yang perlu dipatuhi adalah seperti yang berikut:	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	a) Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; b) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; c) Memastikan perubahan yang sesuai dibuat kepada JPICT JIM dan Pelan Kesenambungan Perkhidmatan yang berkaitan; dan d) Memastikan sistem aplikasi, integriti maklumat dan kawalan capaian disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilaksanakan.	
8.32.4	Sekatan Ke atas Perubahan Dalam Pakej Perisian Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal ketat. Jika pakej perisian perlu diubah suai, perkara berikut perlu diambil kira: a) Akses kepada kod sumber aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja; b) Melaksanakan pengujian ke atas pakej perisian yang terkini sebelum dimaklumkan kepada semua pengguna mengenai perubahan pakej perisian; dan c) Memastikan perubahan pakej perisian tidak menjejaskan perkhidmatan operasi sistem maklumat.	Pentadbir Sistem ICT, Pengarah Bahagian

8.33 DATA PENGUJIAN

ID	KETERANGAN	PERANAN
8.33.1	Perlindungan Data Ujian Data ujian yang hendak digunakan perlu dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; b) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; c) Pengujian hendaklah dibuat ke atas atur cara yang terkini; d) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan e) Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.	Pengguna, Pentadbir Sistem ICT, ICTSO

8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PELAKSANAAN AUDIT

ID	KETERANGAN	PERANAN
8.34.1	Kawalan Audit Sistem Maklumat Keperluan dan aktiviti audit yang melibatkan penentuan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses perkhidmatan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Keperluan audit untuk capaian kepada sistem dan data perlu dipersetujui oleh ICTSO; b) Skop bagi audit teknikal perlu dipersetujui oleh pengurusan atasan serta perlu dikawal; c) Audit perlu dihadkan kepada capaian <i>Read Only</i>. Capaian lebih daripada <i>Read Only</i> hanya dibenarkan ke atas salinan yang telah	ICTSO, Pentadbir Sistem ICT

	diasingkan dan perlu dipadamkan setelah selesai audit; d) Persetujuan daripada pihak pengurusan atasan adalah perlu sekiranya terdapat keperluan khas semasa audit; e) Audit yang boleh menyebabkan gangguan terhadap perkhidmatan perlu disemak semula mekanisme audit agar tidak menyebabkan gangguan terhadap perkhidmatan; dan f) Semua aktiviti audit termasuk capaian terhadap sistem, infrastruktur dan dokumen perlu dipantau dan dilogkan sebagai bahan bukti.	
--	---	--

**LAMPIRAN A: SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER
JABATAN IMIGRESEN MALAYSIA**



**SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER (PKS)
JABATAN IMIGRESEN MALAYSIA (JIM)**

Nama Penuh :
No Kad Pengenalan :
Jawatan / Gred :
Bahagian / Agensi :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

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

Tandatangan :
Tarikh :

Pengesahan Ketua Pegawai Digital (CDO) JIM

(DR. ROSBI BINTI ABDUL RAHMAN)
Timbalan Ketua Pengarah (Pengurusan)
Jabatan Imigresen Malaysia

LAMPIRAN B: SENARAI UNDANG-UNDANG YANG TERPAKAI

1. Arahan Keselamatan (Semakan dan Pindaan 2017);
2. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk 'Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan'
3. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS)
4. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk 'Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi- agensi Kerajaan'
5. Surat Pekeliling Am Bilangan 3 Tahun 2024 – Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024
6. Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022
7. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – 'Tatacara Penyediaan, Penilaian dan Penerimaan Tender'
8. Surat Pekeliling Perbendaharaan Bil.3/1995- 'Peraturan Perolehan Perkhidmatan Perundingan'
9. Akta Tandatangan Digital 1997
10. Akta Rahsia Rasmi 1972
11. Akta Jenayah Komputer 1997
12. Akta Hak Cipta (Pindaan) Tahun 1997
13. Akta Komunikasi dan Multimedia 1998
14. Perintah-perintah Am
15. Arahan Perbendaharaan
16. Arahan Teknologi Maklumat 200
17. Surat Akujanji
18. MyPortfolio
19. Pelan Kesenambungan Perkhidmatan
20. Surat Arahan MAMPU.702-1/1/7 Jld. 3(48) bertarikh 23 Mac 2009 bertajuk 'Pengaktifan Fail LogServer bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan'
21. Surat Arahan MAMPU.BDPIC(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk 'Penggunaan Media Jaringan Sosial di Sektor Awam'
22. Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk 'Tatacara Pengurusan Aset Alih Kerajaan (TPA)'
23. Pekeliling Perkhidmatan Bil 5 2007 bertajuk Panduan Pengurusan Pejabat bertarikh 30 April 2007
24. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA, April 2016
25. Garis Panduan GPKI
26. Akta Perlindungan Data Peribadi (Pindaan) 2024
27. Akta Keselamatan Siber (2024)

28. Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam.