DASAR KESELAMATAN SIBER (DKS)

JABATAN PERANCANGAN BANDAR DAN DESA (PLANMALAYSIA)

JABATAN PERANCANGAN BANDAR DAN DESA
(PLANMalaysia)

Dasar Keselamatan Siber

(DKS)

PLANMalaysia-ISMS-P1-001

Disediakan Oleh:	Disemak Oleh:	Diluluskan Oleh:
Nama: Ts. Mohd. Aziri bin Che Wil Jawatan: Ketua Seksyen Teknologi Maklumat	Nama: En. Shahrul Azam bin Shaari Jawatan: Pengarah Bahagian Khidmat Pengurusan	Nama: YBhg. Datuk TPr Dr. Alias bin Rameli Jawatan: Ketua Pengarah Perancangan Bandar dan Desa

A. REKOD PINDAAN DOKUMEN

TARIKH	NO. KELUARAN/ PINDAAN	BAB/ MUKA SURAT	KETERANGAN PINDAAN
14 Februari 2023	1.0	Keseluruhan	Versi Awalan
25 Jun 2026	2.0	Keseluruhan	Salinan Pertama Pindaan Dasar Keselamatan Siber (DKS) merujuk Standard ISO/IEC 27001:2022

KANDUNGAN

I. RINGKASAN EKSEKUTIF 5
II. SINGKATAN DAN GLOSARI 6
III. SENARAI RAJAH 17
IV. SENARAI JADUAL 17
V. SENARAI PROSEDUR 18
1.0 PENGENALAN 20
2.0 TUJUAN 20
3.0 OBJEKTIF 20
4.0 TADBIR URUS 20
5.0 PRINSIP-PRINSIP KESELAMATAN 25
6.0 SKOP DKS PLANMALAYSIA 27
7.0 PENILAIAN RISIKO KESELAMATAN SIBER 35
8.0 PELAN PENGURUSAN KESELAMATAN MAKLUMAT 35
9.0 PERNYATAAN DASAR KESELAMATAN SIBER PLANMALAYSIA 37
10.0 BIDANG KAWALAN 38
BIDANG 01: KAWALAN ORGANISASI 40
BIDANG 02: KAWALAN MANUSIA 91
BIDANG 03: KAWALAN FIZIKAL 101
BIDANG 04: KAWALAN TEKNOLOGI 119
11.0 LAMPIRAN 163
12.0 PENGHARGAAN 177

I. RINGKASAN EKSEKUTIF

Secara umumnya, keselamatan siber merujuk kepada bagaimana pengguna Internet menggunakan medium Internet secara positif dan selamat serta melindungi diri mereka daripada ancaman siber.

Amalan keselamatan siber adalah untuk mempertahankan aset siber seperti rangkaian, sistem maklumat dan program atau sistem aplikasi daripada ancaman siber seperti kecurian, kompromi dan/atau serangan. Amalan ini memerlukan pemahaman tentang ancaman maklumat yang berpotensi seperti virus dan kod hasad yang lain. Strategi keselamatan siber termasuklah pengurusan identiti, pengurusan risiko dan pengurusan insiden.

Terdapat 4 bidang kawalan utama Dasar Keselamatan Siber PLANMalaysia ini dan objektif setiap bidang kawalan adalah seperti yang berikut:

(a) Bidang 01: Kawalan Organisasi
Bidang ini meliputi polisi dan prosedur yang telah dibangunkan untuk menangani isu-isu di dalam organisasi, seperti pembahagian tugas dan tanggungjawab, pengurusan maklumat dan kepatuhan terhadap peraturan dan undang-undang.

(b) Bidang 02: Kawalan Manusia
Bidang ini meliputi kawalan-kawalan untuk mengurus risiko berkaitan sumber manusia.

(c) Bidang 03: Kawalan Fizikal
Tujuan bidang ini adalah untuk memastikan perlindungan terhadap aset maklumat organisasi daripada ancaman fizikal.

(d) Bidang 04: Kawalan Teknologi
Bidang ini mengandungi kawalan yang memerlukan organisasi untuk membangunkan dan mengekalkan keselamatan sistem teknologi.

II. SINGKATAN DAN GLOSARI

Berikut ialah jadual singkatan dan glosari bagi perkataan yang digunakan dalam dokumen ini.

Jadual 1: Singkatan dan Glosari

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
1.	Antivirus	Perisian yang mengimbas virus pada media storan seperti *flash disk* (USB), CDROM untuk sebarang kemungkinan adanya virus.
2.	API (*Application Programming Interface*)	Satu set arahan pengaturcaraan dan *standard* untuk akses menerusi aplikasi web menggunakan perisian aplikasi web.
3.	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
4.	*Backup* (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat. Sumber yang boleh digunakan untuk menggantikan sumber utama yang gagal atau terhapus.
5.	*Bandwidth*	Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi dalam jangka masa yang ditetapkan. Contoh: *video streaming* dan *teleconference*.
6.	BKP	Bahagian Khidmat Pengurusan PLANMalaysia
7.	*Broadband*	Teknologi yang menyediakan capaian Internet melalui rangkaian luas.
8.	SSM	Seksyen Sumber Manusia PLANMalaysia
9.	STM	Seksyen Teknologi Maklumat PLANMalaysia
10.	BYOD (*Bring Your Own Device*)	Peralatan mudah alih persendirian seperti telefon pintar, tablet, komputer riba dan media storan yang digunakan untuk tujuan rasmi.
11.	CSIRT (*Cyber Security Incident Response Team*)	Pasukan Tindak Balas Insiden Keselamatan Siber, iaitu pasukan yang ditubuhkan untuk membantu PLANMalaysia menguruskan pengendalian insiden keselamatan ICT di PLANMalaysia.
12.	CDO (*Chief Digital Officer*)	Ketua Pegawai Maklumat, iaitu pegawai yang dilantik untuk menjadi peneraju dalam merancang, melaksana dan memantau program Kerajaan berasaskan ICT bagi memudahkan pelanggan berurusan dengan agensi Kerajaan. Beliau juga merupakan agen transformasi menerusi inovasi,

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
		kreativiti dan inisiatif pembaharuan yang berterusan.
13.	CGSO (*Chief Government Security Office*)	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia, iaitu sebuah unit di bawah Jabatan Perdana Menteri, Malaysia.
14.	*Clear Desk* dan *Clear Screen*	Tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.
15.	*Content Filtering*	Satu teknik yang menyekat atau membenarkan berdasarkan analisis kepada kandungan dan bukannya berdasarkan sumber atau kriteria. Ia digunakan secara meluas untuk capaian internet dan email.
16.	Data-dalam-simpanan (*Data-at-rest*)	Data yang tidak aktif yang disimpan secara fizikal dalam bentuk digital. Contohnya pangkalan data, gudang data, hamparan, arkib dan sebagainya.
17.	Data-dalam-pergerakan (*Data-in-motion*)	Data transit maklumat digital yang sedang dalam proses pergerakan di dalam atau antara sistem komputer.
18.	Data-dalam-penggunaan (*Data-in-use*)	Data yang sedang diperbaharui, diproses, dihapus, diakses atau dibaca oleh sistem. Jenis data ini tidak disimpan secara pasif, tetapi bergerak aktif melalui infrastruktur IT.
19.	Data Raya	Data yang bersaiz besar (*high-volume*), berubah dengan pantas (*high-velocity*) dan kepelbagaian yang tinggi (*high-variety*).
20.	DDSA	Data *Dictionary* Sektor Awam, iaitu keterangan data yang *standard* untuk diguna pakai oleh agensi-agensi sektor awam.
21.	*Defence-in-depth*	Satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
22.	DKS	Dasar Keselamatan Siber, iaitu dokumen yang mengandungi dasar dan peraturan dalam menggunakan aset ICT dan ruang siber.
23.	DRP (*Disaster Recovery Plan*)	Pelan Pemulihan Bencana, iaitu dokumentasi pendekatan berstruktur yang menerangkan bagaimana sesebuah organisasi dengan cepatnya memulakan semula kerja setelah berlakunya bencana. DRP merupakan bahagian penting dalam

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
		Pelan Pengurusan Kesinambungan Perkhidmatan yang melibatkan aspek-aspek tertentu organisasi yang bergantung kepada infrastruktur ICT.
24.	DTSA (Data Terbuka Sektor Awam)	Data Terbuka Sektor Awam, iaitu inisiatif kerajaan yang menggalakkan perkongsian data, meningkatkan sistem penyampaian perkhidmatan kerajaan dengan lebih mudah, cepat dan telus serta menggalakkan pertumbuhan ekonomi negara. Data terbuka merujuk kepada data kerajaan yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan.
25.	E-Dagang	Proses menjalankan urusan perniagaan membeli atau menjual barangan atau perkhidmatan melalui rangkaian komputer atau internet.
26.	E-mel (Mel Elektronik)	Maklumat atau mesej yang dihantar secara elektronik dari satu terminal komputer ke terminal komputer yang lain.
27.	EMS (*Environment Monitoring System*)	Sistem Pemantauan Persekitaran, iaitu sistem yang memantau kualiti persekitaran menggunakan peralatan untuk menilai keadaan dan kecenderungan/trend persekitaran.
28.	Enkripsi (*Encryption*)	Penukaran data sensitif kepada bentuk kod sulit untuk membolehkan data dikirim dengan selamat tanpa difahami pihak lain.
29.	FAT (*Final Acceptance Test*)	Ujian Penerimaan Akhir, iaitu keadaan apabila penyiapan kerja disahkan, dan selalunya setelah ujian-ujian yang perlu telah siap dilaksanakan. Jika terdapat sebarang kecacatan dan kekurangan dikenal pasti, pembetulan perlu dilakukan.
30.	GAMMA (Gallery of Malaysian Government Mobile Application)	Galeri Aplikasi Mudah Alih Kerajaan Malaysia yang menempatkan aplikasi mudah alih agensi Kerajaan bagi kemudahan Pengguna.
31.	GENSET (Generator Set)	Genset atau Janakuasa berfungsi membekal tenaga mekanikal kepada tenaga elektrik.
32.	ICT (Information and Communication Technology)	Penggabungan teknologi maklumat dan teknologi komunikasi dalam perolehan, penyimpanan, pemprosesan dan pengagihan maklumat secara elektronik.
33.	ICT Hijau Kerajaan	Amalan dari segi pengeluaran, penggunaan dan

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
		pelupusan komputer, pelayan (server) serta aksesori seperti monitor, tetikus, pencetak dan peralatan rangkaian secara berkesan dan efektif dengan memberi kesan yang minima atau tiada kesan terhadap alam sekitar.
34.	ICTSO (ICT Security Officer)	Pegawai Keselamatan ICT, iaitu pegawai yang dilantik untuk bertanggungjawab terhadap keselamatan siber.
35.	IDS (*Intrusion Detection System*)	Sistem yang menyiasat semua aktiviti rangkaian dan mengenal pasti pola yang disyaki untuk menunjukkan bahawa rangkaian atau sistem diceroboh. Terdapat dua bentuk IDS yang lazim, iaitu pengesanan salah guna dan pengesanan anomali. Dalam pengesanan salah guna, IDS menganalisis maklumat yang dikumpul dan membandingkannya dengan pangkalan data tandatangan serangan yang besar. Secara khusus IDS mencari serangan tertentu yang telah didokumenkan. Seperti sistem pengesan virus, keberkesanan perisian pengesan salah guna ini hanyalah bergantung kepada sebaik mana pangkalan data tandatangan serangan yang ada untuk membandingkan maklumat yang dikumpul.
36.	Insiden Keselamatan Siber	Musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin satu perbuatan yang melanggar DKS sama ada yang ditetapkan secara tersurat atau tersirat.
37.	Internet	Sistem perangkaian antarabangsa yang membolehkan pengguna di seluruh dunia berhubung antara satu sama lain dan mencapai maklumat di seluruh dunia.
38.	IP (*Internet Protocol*)	Protokol yang menyalurkan datagram ke saluran yang tertentu dengan harapan ia sampai ke destinasinya.
39.	IPS (*Intrusion Prevention System*)	Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan seperti *malicious code*. Contoh: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
		serangan.
40.	ISMS (*Information Security Management System*)	Sistem Pengurusan Keselamatan Maklumat. ISO/IEC 27001 (ISMS) menyatakan keperluan untuk mewujud, mengoperasi, memantau, mengkaji semula, menyenggara dan memperbaiki Sistem Pengurusan Keselamatan Maklumat organisasi. Pematuhan kepada *standard*/piawaian ISMS ini menunjukkan bahawa sistem pengurusan organisasi perlu memastikan kerahsiaan, integriti dan ketersediaan maklumat.
41.	ISP (*Internet Service Provider*)	Organisasi yang membekalkan pengguna dengan capaian Internet dan khidmat- khidmat yang berkaitan.
42.	Jejak Audit (*Audit Trail*)	Log yang merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.
43.	JPICT	Jawatankuasa Pemandu ICT, iaitu jawatankuasa yang memproses, menilai dan mengesyorkan perakuan projek ICT.
44.	JTISA	Jawatankuasa Teknikal ICT Sektor Awam, iaitu jawatankuasa yang menimbang dan meluluskan permohonan kelulusan teknikal daripada agensi sektor awam berdasarkan pelan strategik organisasi dan pelan strategik ICT agensi masing-masing bagi perolehan ICT mengikut had nilai yang telah ditetapkan.
45.	Kawasan Larangan	Kawasan yang dihadkan kemasukannya kepada pegawai-pegawai yang tertentu sahaja.
46.	Kawasan Terperingkat	Kawasan yang menempatkan aset ICT berisiko tinggi dan meliputi premis atau sebahagian daripada premis di mana rahsia rasmi disimpan, diuruskan atau di mana kerja terperingkat dijalankan. Akses ke kawasan terperingkat adalah dihadkan dengan kebenaran.
47.	KP	Ketua Pengarah Perancangan Bandar dan Desa.
48.	Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
49.	KPK	Ketua Pegawai Keselamatan, iaitu pegawai yang mengetuai dan bertanggungjawab ke atas semua

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
		aspek keselamatan dokumen dan maklumat rasmi, bangunan dan harta benda Kerajaan daripada sebarang ancaman, kecurian, kebakaran dan sebagainya dengan mengambil kira langkah-langkah melindungi selaras dengan peraturan-peraturan yang ditetapkan oleh Kerajaan.
50.	KPKT	Kementerian Pembangunan Kerajaan Tempatan, iaitu sebuah kementerian di bawah Kerajaan Persekutuan Malaysia yang menerajui kemakmuran komuniti bandar dan persekitaran mampan. Juga merujuk kepada Bahagian/Unit/Jabatan/ Tribunal/Institut/Agensi di bawah KPKT.
51.	Kriptografi	Penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak tertentu sahaja.
52.	Kawasan Larangan	Kawasan yang dihadkan kemasukan bagi warga PLANMALAYSIA yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis PLANMALAYSIA seperti Pusat Data dan Bilik CCTV.
53.	LAN (*Local Area Network*)	Rangkaian komputer yang berkongsi data dan sumber dalam sesuatu kawasan yang terhad seperti sebuah bangunan dan sebuah pejabat.
54.	Lesen Perisian	Maklumat yang berkaitan pendaftaran, pengesahan lesen bagi membolehkan perisian digunakan secara sah seperti *registration code, serials* dan *CD-keys*.
55.	*Log Out*	Tindakan menarik diri secara rasmi daripada log sistem komputer sebelum berhenti secara muktamad daripada menggunakan sistem.
56.	*Malicious Code*	Sebahagian atau keseluruhan kod atur cara terkompil, skrip, atau jujukan arahan sistem pengendalian atau perisian yang boleh menyebabkan sistem bertindak dengan cara yang tidak diingini oleh Pemilik Sistem dan pengguna. Ia mampu menyebabkan kemudaratan kepada data, pengguna, sumber atau aset sistem komputer yang disasarkan.
57.	Jabatan Digital Negara (JDN)	Menyelaras dan melaksana tatakelola program nasional dan projek pendigitalan kerajaan.
58.	Media	Alat atau perantara komunikasi.

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
59.	Media Sosial	Saluran komunikasi dalam talian yang berasaskan Internet yang membolehkan penggunanya berhubung, bertukar-tukar maklumat, berkongsi idea, bekerjasama dan membina komuniti.
60.	Media Storan	Peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti *flash disk* (USB), CDROM dan media storan lain.
61.	*Mobile Code*	Kod program yang boleh disebarkan dari komputer ke komputer dan dilaksanakan secara automatik. Contoh: JavaScript, VBScript, applet Java, ActiveX, Flash, Shockwave dan *macro embedded* bagi dokumen Microsoft Office.
62.	Muat turun	Tindakan memindahkan fail atau data daripada sumber tertentu ke komputer pengguna melalui talian rangkaian.
63.	NACSA (National Cyber Security Agency)	Agensi Keselamatan Siber Negara. Ditubuhkan pada Februari 2017 sebagai agensi negara yang menerajui hal ehwal keselamatan siber, dengan objektif memastikan keselamatan dan memperkukuhkan ketahanan Malaysia dalam menghadapi ancaman serangan siber, dengan mengkoordinasi dan mengkonsolidasi pakar-pakar dan sumber negara dalam bidang keselamatan siber.
64.	*Outsource*	Menggunakan perkhidmatan luar atau pihak ketiga untuk melaksanakan fungsi tertentu bagi suatu tempoh berdasarkan dokumen perjanjian dengan bayaran yang telah dipersetujui.
65.	Pegawai Data	Pegawai yang dilantik untuk menyelaras dan menyemak set data PLANMalaysia bagi keperluan penerbitan statistik PLANMalaysia serta keperluan Data Terbuka untuk dimuat naik ke portal Data Terbuka Sektor Awam.
66.	Pegawai Pengawal	Pegawai yang dilantik oleh Menteri Kewangan atau Menteri Besar atau Ketua Menteri di bawah seksyen 15A Akta Tatacara Kewangan 1957 (Akta 61) bagi setiap tujuan perbelanjaan yang diperuntukkan bagi mana-mana tahun kewangan dalam anggaran, bagi mengawal, tertakluk kepada sebarang arahan yang ditujukan oleh pihak Penguatkuasa Kewangan, perbelanjaan yang dikuatkuasakan di bawah tujuan itu dan termasuk

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
		semua tanggungjawab Pegawai Perakaunan.
67.	Pelan Pemulihan Perkhidmatan (BCP)	Pelan ini meliputi segala sumber, proses, peranan dan tanggungjawab semua pihak terlibat yang diperlukan sebelum, semasa dan selepas sesuatu gangguan terhadap sistem penyampaian perkhidmatan.
68.	Pelan Pengurusan Krisis Siber Negara dan Prosedur Tindak Balas, Komunikasi dan Penyelarasan (NCCMP)	Pelan yang dibangunkan berdasarkan kepada rangka kerja pengurusan risiko yang menggariskan strategi bagi mengurangkan kesan serangan siber dan tindak balas yang perlu dilaksanakan oleh agensi Infrastruktur Maklumat Kritikal Negara (CNII) yang terdiri daripada pelbagai agensi awam dan swasta.
69.	Pembekal	Individu, entiti perniagaan atau organisasi yang menyediakan produk atau perkhidmatan kepada Pengguna.
70.	Pemilik Sistem	Pemilik perniagaan (*business owner*) bagi sistem yang dibangunkan di PLANMalaysia yang paling banyak memiliki data dalam sesuatu sistem.
71.	Pengguna	Pegawai yang berkhidmat secara kontrak atau pegawai khidmat singkat yang menggunakan aset ICT dan siber secara langsung atau tidak langsung.
72.	Pentadbir Sistem ICT	Pentadbir yang melaksanakan dan menyelenggara sistem aplikasi, laman web, media sosial dan aplikasi mudah alih.
73.	Pentadbir Perisian	Pentadbir yang melaksanakan proses pemasangan perisian yang hanya menggunakan perisian yang tulen dan berdaftar.
74.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT	Pentadbir yang melaksanakan dan menyelenggara Pusat Data, rangkaian ICT dan komunikasi ICT.
75.	Pentadbir Laman Web	Pentadbir yang mengurus, menyelenggara, dan mengemas kini kandungan laman web bagi memastikan maklumat yang disiarkan adalah tepat, terkini, dan selamat.
76.	Peralatan ICT	Merujuk kepada komponen dalaman perkakasan ICT.
77.	Peralatan Mudah Alih	Peralatan mudah alih termasuk komputer riba dan peranti mudah alih seperti tablet, Personal Digital

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
		Assistant (PDA), telefon bimbit, telefon pintar, kamera digital, cakera padat serta pemacu Universal Serial Bus (USB) dan sebagainya.
78.	Perisian	Set atur cara komputer yang menjalankan sesuatu tugas pada sistem komputer. Terdapat tiga (3) jenis perisian iaitu sistem pengendali (contoh: Linux dan Windows), sistem utiliti (contoh: Disk Cleanup dan Disk Defragmenter) dan perisian aplikasi (contoh: Microsoft Office dan Google Chrome).
79.	Perkakasan ICT	Merujuk kepada peralatan dan perisian ICT.
80.	Penyelaras ICT	Pegawai yang dilantik oleh Pengarah Bahagian untuk memastikan urusan ICT berjalan dengan lancar.
81.	PICT	Pengurus ICT.
82.	PK	Pegawai Keselamatan.
83.	Pihak Ketiga	Pakar runding, pertukaran pegawai, juruteknik residen, pihak agensi, pelajar praktikal dan individu yang mempunyai urusan dengan perkhidmatan ICT dan siber serta dilantik untuk melaksanakan tugas di PLANMalaysia dalam jangka masa yang tertentu.
84.	PII (*Personal Identifiable Information*)	Maklumat yang boleh digunakan secara tersendiri atau digunakan dengan maklumat lain untuk mengenal pasti individu tertentu.
85.	PKI (*Public Key Infrastructure*)	Infrastruktur Kunci Awam, iaitu sistem enkripsi lengkap khusus untuk mencipta dan mengurus kekunci awam semasa proses penyulitan data dan pertukaran kekunci dalam kalangan pengguna. Ia merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
86.	PLANMalaysia	Jabatan Perancangan Bandar dan Desa.
87.	PKP	Pengurusan Kesinambungan Perkhidmatan (Business Continuity Management), bertujuan untuk memastikan fungsi-fungsi kritikal, perkhidmatan, sistem dan proses-proses utama agensi dapat segera dipulihkan dalam masa yang ditetapkan sekiranya berlaku gangguan atau bencana.
88.	Portal DTSA	Portal Data Terbuka Sektor Awam, iaitu

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
		data.gov.my yang dibangunkan pada tahun 2014 untuk memudahkan data terbuka kerajaan diakses secara berpusat daripada sumber yang rasmi.
89.	Produk Kriptografi Terpercaya	Produk kriptografi yang dinilai dan diiktiraf oleh Kerajaan bertujuan untuk mengawal dan menjaga keselamatan maklumat, integriti, pengesahan dan tidak boleh disangkal.
90.	PSP (Pelan Strategik Pendigitalan)	Hala tuju strategik pelaksanaan pendigitalan yang akan menjadi panduan bagi memacu agenda Kerajaan Digital yang mampan ke arah membentuk masyarakat digital.
91.	*Restore*	Aktiviti pemulihan atau penyalinan semula data daripada media penduaan.
92.	*Router*	Peranti yang digunakan untuk menghantar data antara dua (2) rangkaian yang mempunyai kedudukan rangkaian yang berlainan. contoh: capaian Internet.
93.	*Screen Saver*	Imej yang akan diaktifkan pada komputer setelah ia tidak digunakan dalam jangka masa tertentu.
94.	*Server*	Unit dalam rangkaian yang membekalkan data dan maklumat kepada komputer lain yang mempunyai hubungan rangkaian dengannya.
95.	Siber	Ruang maya yang diwujudkan oleh rangkaian komputer sejagat. Ruang tempat berlangsungnya kegiatan pemanfaatan ICT dan internet ini disebut ruang siber. Ruang siber (cyberspace) atau siber adalah ruang di mana komunikasi saling terhubung menggunakan jaringan (misalnya internet) untuk melakukan berbagai kegiatan sehari- hari.
96.	Sistem ICT	Merangkumi Sistem Aplikasi, Sistem Pusat Data, Rangkaian dan Komunikasi ICT.
97.	SLA (*Service Level Agreement*)	Perjanjian Tahap Perkhidmatan, iaitu komponen kontrak perkhidmatan antara pembekal perkhidmatan dan pelanggan. SLA menyediakan aspek khusus dan terukur yang berkaitan dengan penawaran perkhidmatan.
98.	SoA (Statement of Applicability)	Dokumen yang memperincikan kawalan- kawalan yang terdapat di Annex A dalam *standard* ISO/IEC 27001:2022 *Information Security Management*

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
		System (ISMS) bagi menangani risiko keselamatan maklumat perniagaan atau maklumat sensitif perniagaan.
99.	SPPA	Sistem Pemantauan Pengurusan Aset, iaitu aplikasi yang dibangunkan oleh Kementerian Kewangan untuk tujuan kawalan dan pemantauan aset bagi semua Kementerian dan Jabatan Persekutuan.
100.	*Switch*	Alat yang boleh menapis (*filter*) dan memajukan (*forward*) isyarat paket data antara segmen rangkaian LAN.
101.	UAT (*User Acceptance Test*)	Ujian yang dilakukan oleh pengguna/pelanggan untuk mengesahkan/menerima sistem aplikasi.
102.	UC (*Unified Communication*)	Saluran-saluran komunikasi elektronik selain e-mel yang disepadukan dalam satu rangkaian dan antara muka yang sama.
103.	UPS (*Uninterruptible Power Supply*)	Satu alat yang akan membekalkan kuasa secara automatik kepada peralatan komputer khususnya dan peralatan elektrik umumnya apabila bekalan elektrik utama terputus.
104.	VPN (*Virtual Private Network*)	Teknologi rangkaian atau kaedah yang diguna pakai untuk membuat sambungan rangkaian yang selamat dan menyediakan privasi pada rangkaian peribadi atau awam.
105.	WAN (*Wide Area Network*)	Rangkaian komunikasi yang merangkumi kawasan geografi yang luas di seluruh bandar, negara atau rantau.

III. SENARAI RAJAH

Berikut ialah senarai rajah yang digunakan dalam dokumen ini.

RAJAH	TAJUK
1	Struktur Jawatankuasa ISMS PLANMalaysia
2	Struktur Jawatankuasa Kajian Semula Pengurusan (JKSP) PLANMalaysia

IV. SENARAI JADUAL

Berikut ialah senarai jadual yang digunakan dalam dokumen ini.

JADUAL	TAJUK
1	Singkatan dan Glosari
2	4 Bidang Kawalan Keselamatan Siber PLANMalaysia

V. SENARAI PROSEDUR

Berikut ialah senarai prosedur yang digunakan dalam dokumen ini.

PROSEDUR	TAJUK
1	Prosedur Penyelenggaraan DKS PLANMalaysia
2	Prosedur Kawalan Perubahan
3	Prosedur Pembangunan Sistem Aplikasi (KRISA)
4	Prosedur Pengurusan Insiden Keselamatan Siber

PENGENALAN

1.0 PENGENALAN

Dasar Keselamatan Siber (DKS) Jabatan Perancangan Bandar Dan Desa (PLANMalaysia) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan peralatan ICT dan ruang siber. Peraturan- peraturan ini perlu difahami dan dipatuhi oleh semua Pengguna, Pembekal dan Pihak Ketiga dalam melindungi maklumat di PLANMalaysia. Dasar ini juga menerangkan kepada semua Pengguna, Pembekal dan Pihak Ketiga mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT dan siber PLANMalaysia.

2.0 TUJUAN

DKS PLANMalaysia diwujudkan untuk memastikan pengurusan tadbir urus keselamatan siber bagi semua inisiatif digital PLANMalaysia dipatuhi bagi meredakan kebimbangan mengenai masalah keselamatan maklumat.

3.0 OBJEKTIF

Objektif utama DKS PLANMalaysia ialah seperti berikut:

(i) Memastikan kelancaran operasi pendigitalan PLANMalaysia dan meminimumkan kerosakan atau kemusnahan disebabkan insiden keselamatan siber;

(ii) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem ICT daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan telekomunikasi;

(iii) Mencegah salah guna atau kecurian aset ICT dan siber Kerajaan;

(iv) Meminimumkan kos penyelenggaraan aset ICT akibat ancaman, godaman dan penyalahgunaan;

(v) Memperkemaskan pengurusan keselamatan siber PLANMalaysia; dan

(vi) Menghindari tindakan penggodaman ruang siber yang dituju kepada sistem ICT atau laman web rasmi PLANMalaysia.

4.0 TADBIR URUS

Secara umumnya, tadbir urus yang baik merupakan satu bentuk mekanisme penyediaan perkhidmatan yang baik untuk masyarakat.

DKS PLANMalaysia merangkumi:

(a) Semua Bahagian PLANMalaysia.

Tadbir urus dilaksanakan melalui jawatankuasa-jawatankuasa yang ditubuhkan dan peraturan-peraturan yang sedang berkuat kuasa bagi memastikan keberkesanan dan kejayaan pelaksanaan DKS PLANMalaysia. Antara jawatankuasa tersebut adalah seperti berikut:

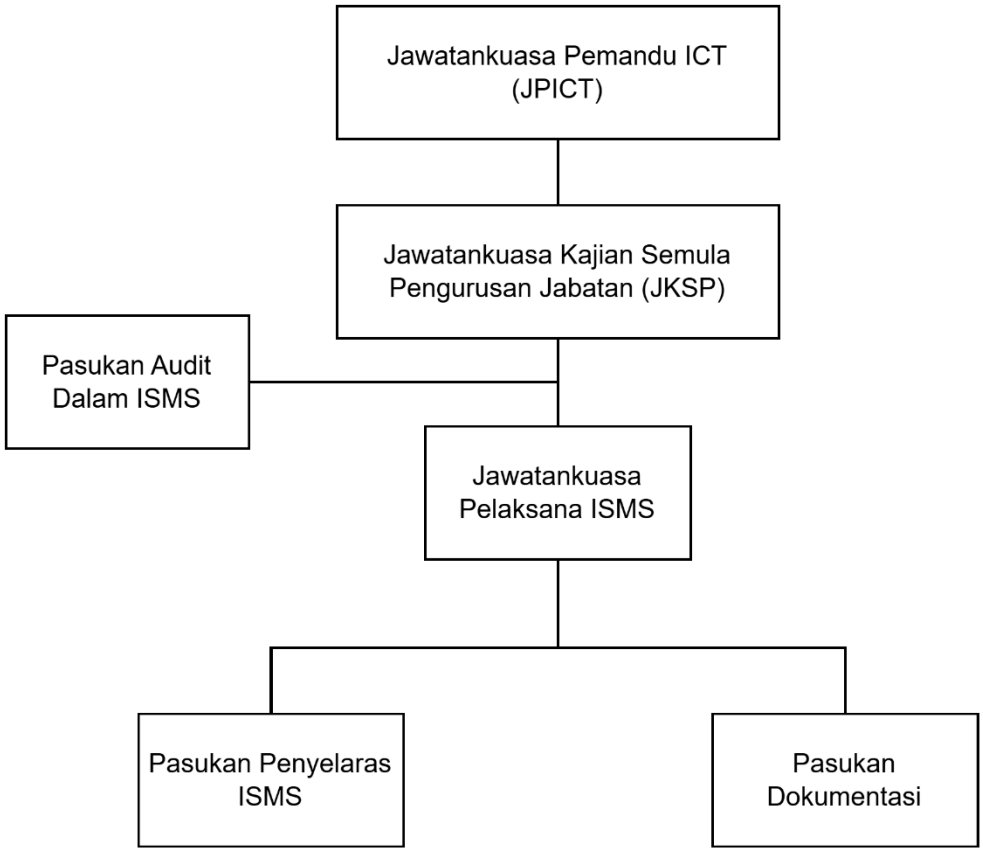
(i) Jawatankuasa ISMS PLANMalaysia;

(ii) Jawatankuasa Pemandu ICT (JPICT) PLANMalaysia; dan

(iii) Jawatankuasa Kajian Semula Pengurusan (JKSP) PLANMalaysia.

4.1 JAWATANKUASA ISO/IEC 27001:2022 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) PLANMalaysia

DKS PLANMalaysia dibangunkan selaras dengan keperluan ISO/IEC 27001:2022 ISMS yang merupakan amalan terbaik ISO/ IEC 27000 dan standard antarabangsa dalam menetapkan keperluan secara berterusan sistem pengurusan keselamatan maklumat mengikut konteks organisasi. Struktur Jawatankuasa ISMS PLANMalaysia adalah seperti Rajah 2: Struktur Jawatankuasa ISMS PLANMalaysia.



Rajah 1: Struktur Jawatankuasa ISMS PLANMalaysia

Keahlian Jawatankuasa ISMS PLANMalaysia adalah seperti yang berikut:

BIL.	PERANAN	TANGGUNGJAWAB
1.	Jawatankuasa Pemandu ICT (JPICT)	a) Menetapkan arah tuju dan strategi untuk pembangunan dan pelaksanaan ICT PLANMalaysia; b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/strategi ICT PLANMalaysia; c) Memantau pelaksanaan pensijilan ISMS PLANMalaysia; d) Memantau status kemajuan ISMS; e) Meluluskan Dasar Keselamatan Siber (DKS) PLANMalaysia; f) Memperakui Skop ISMS; dan g) Memperakui Tadbir Urus ISMS.
2.	Jawatankuasa Kajian Semula Pengurusan Jabatan (JKSP)	a) Memantau dan menyemak pelaksanaan pensijilan ISMS; b) Menetapkan struktur organisasi ISMS; c) Menetap kriteria penerimaan risiko, tahap risiko dan pelan penguraian risiko; d) Melaksanakan Mesyuarat Kajian Semula Pengurusan (MKSP) PLANMalaysia sekurang-kurangnya satu kali (1) setahun; e) Mengesahkan status tindakan daripada kajian semula pengurusan terdahulu; f) Mengesahkan perubahan pada isu luaran dan dalaman yang berkaitan dengan ISMS; g) Memantau prestasi keselamatan maklumat termasuk: h) Ketakakuran dan Tindakan pembetulan i) Hasil pemantauan dan pengukuran j) Hasil audit; k) Pencapaian objektif keselamatan maklumat; l) Memantau maklum balas daripada pihak berkepentingan; m) Merancang peluang untuk penambahbaikan berterusan; n) Meluluskan Skop ISMS; dan o) Meluluskan Tadbir Urus ISMS.

BIL.	PERANAN	TANGGUNGJAWAB
3.	Jawatankuasa Pelaksana ISMS	a) Melaksana ISMS dengan: i. menghadiri kursus kesedaran standard ISO/IEC 27001:2022; ii. menyediakan dasar ISMS, Statement of Applicability (SoA), laporan risiko, pelan penguraian risiko dan prosedur-prosedur; iii. melaksanakan prosedur dan kawalan dalam ISO/IEC 27001:2022; iv. melaksanakan tindakan pembetulan dan pelan penguraian risiko. b) Mengemukakan isu dan masalah ISMS, jika ada; c) Menguruskan dokumen dan rekod pelaksanaan ISMS; d) Melantik pasukan audit dalam dan ketua audit dalam ISMS; a) Menyedia kaedah pengukuran keberkesanan kawalan ISMS; b) Mengukur keberkesanan kawalan ISMS; c) Memantau pelaksanaan tindakan pembetulan dan penambahbaikan; d) Memantau dan menyemak semula ISMS; dan e) Melaksana Mesyuarat Jawatankuasa Pelaksana ISMS PLANMalaysia sekurang-kurangnya satu kali (1) setahun.
4.	Pasukan Penyelaras ISMS	a) Menyelaras dokumen ISMS; dan b) Menjalankan kerja-kerja pentadbiran ISMS seperti penyediaan minit mesyuarat dan logistik.
5.	Pasukan Audit Dalam ISMS	a) Menyediakan jadual audit tahunan, jadual pelaksanaan audit dan senarai semak audit; b) Melaksana Audit Dalam ISMS PLANMalaysia berdasarkan kawalan yang diperlukan dalam ISO/IEC 27001:2022; c) Menyediakan Laporan Audit Dalam ISMS; d) Membentang penemuan Audit Dalam ISMS; e) Menjalankan audit susulan bagi mengesahkan tindakan pembetulan yang dilaksanakan (jika perlu); dan f) Mengemukakan Laporan Audit Susulan.

Bil.	Nama Pegawai	Jawatan/Bahagian	Peranan
1.	YBhg. Datuk TPr Dr. Alias bin Rameli	Ketua Pengarah PLANMalaysia	Pengerusi
2.	TPr Shahrul Niza bin Samsudin	Pengarah Bahagian Maklumat Gunatanah Negara	Ahli
3.	En. Shahrul Azam bin Shaari	Pengarah Bahagian Khidmat Pengurusan	Ahli
4.	TPr Wan Andery bin Wan Mahmood	Ketua Unit Maklumat Gunatanah (BMGN)	Ahli
5.	En. Anuar bin Abidin	Ketua Seksyen Pentadbiran	Ahli
6.	Pn. Nadiah binti Said	Ketua Seksyen Sumber Manusia	Ahli
7.	YM Raja Nor Azlina binti Raja Ahmad	Ketua Unit Integriti	Ahli
8.	En. Mohd Fadzil bin Abdul Rahman	Ketua Seksyen Kewangan	Ahli
Urusetia ISMS			
9.	Ts. Mohd Aziri bin Che Wil	Seksyen Teknologi Maklumat	Ahli
10.	Cik Shaidatul Ezzan Binti Mohamad Yusop		Ahli
11	Cik Fahwani binti Mohd Ali		Ahli
12.	En.Mohamad Eqmal Fareed Bin Md Yusof		Ahli
Wakil i-PLAN			
13.	En. Muhamad Ikhwan bin Saadon	Bahagian Maklumat Gunatanah Negara	Ahli
14.	En. Mohd Shazir bin Ashari		Ahli

Rajah 2: Struktur Jawatankuasa Kajian Semula Pengurusan (JKSP) PLANMalaysia

5.0 PRINSIP-PRINSIP KESELAMATAN

Prinsip-prinsip yang menjadi asas kepada DKS PLANMalaysia dan perlu dipatuhi mengikut kesesuaian maklumat yang dikendalikan adalah seperti berikut:

a) Akses atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset ICT dan ruang siber hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan dan dibenarkan akses maklumat tersebut.

Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan Kerajaan yang sedang berkuatkuasa.

b) Hak Akses Minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/ atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna atau bidang tugas;

c) Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICTdan ruang siber. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk membolehkan pertanggungjawaban ini dilaksanakan, sistem komputer hendaklah mampu menyokong kemudahan mengesan dan mengesahkan penggunaan sistem komputer.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

(i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

(ii) Memeriksa data dan maklumat serta menentukan ianya tepat dan lengkap dari semasa ke semasa;

(iii) Menentukan data dan maklumat sedia untuk digunakan;

(iv) Menjaga kerahsiaan kata laluan;

(v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

(vi) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

(vii) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.

d) Pengasingan

Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT dan ruang siber daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan sistem dan operasi;

e) Pengauditan

Pengauditan ialah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Oleh yang demikian, aset ICT seperti komputer, pelayan, router, firewall, rangkaian dan lain-lain hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau audit trail;

f) Pematuhan

DKS PLANMalaysia hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan siber;

g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan Pelan Pemulihan Bencana (DRP) dan/atau Pengurusan Kesinambungan Perkhidmatan; dan

h) Saling Bergantungan

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

6.0 SKOP DKS PLANMalaysia

Skop DKS PLANMalaysia merangkumi perkara berikut:

a) Aset ICT dan Siber;
b) Manusia;
c) Proses; dan
d) Teknologi

6.1 ASET ICT DAN SIBER

Ruang siber (cyberspace) atau siber adalah ruang di mana komunikasi saling terhubung menggunakan jaringan (misalnya internet) untuk melakukan berbagai kegiatan sehari-hari.

DKS PLANMalaysia menetapkan keperluan-keperluan asas berikut:

a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
b) Data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan integriti dan kesahihan maklumat serta untuk melindungi kepentingan Kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan ruang siber ini terpelihara keselamatannya sepanjang masa, DKS PLANMalaysia ini merangkumi perlindungan semua bentuk maklumat Kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan sebagai sandaran. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan serta prosedur dalam pengendalian semua perkara-perkara berikut:

a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan PLANMalaysia. Contoh: komputer, pelayan, peralatan komunikasi dan sebagainya;

b) Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian yang disimpan dalam sistem komputer. Contoh: perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat PLANMalaysia;

c) Perkhidmatan

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

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem kawalan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain- lain.

d) Data dan Maklumat

Koleksi fakta dalam bentuk kertas atau mesej elektronik yang mengandungi maklumat untuk digunakan bagi mencapai visi, misi dan objektif PLANMalaysia. Contoh: sistem dokumentasi, prosedur operasi, rekod PLANMalaysia, profil pelanggan, pangkalan data dan fail data, maklumat arkib dan lain-lain; dan

e) Premis Komputer dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) - (d) di atas.

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran data dan maklumat atau kelemahan perlindungan dianggap sebagai perlanggaran langkah-

langkah keselamatan siber.

6.2 MANUSIA

Pengguna, Pembekal dan Pihak Ketiga hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

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

a) Kompetensi Pengguna

i. Kompetensi pengguna termasuk:

- Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan siber dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan siber; dan
- Kemahiran menggunakan alat-alat/tool menjaga keselamatan siber dengan latihan yang mencukupi untuk pelaksanaan tugas rasmi harian.

ii. Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian mendalam.

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

b) Kompetensi Pelaksana

i. Pengguna yang menguruskan aset ICT dan ruang siber hendaklah memenuhi keperluan kecekapan minimum mengikut tugas mereka.

ii. Pegawai Keselamatan ICT/ICTSO hendaklah memenuhi syarat-syarat berikut:

- Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber;
- Memenuhi keperluan pembelajaran berterusan;
- Menimba pengalaman yang mencukupi dalam bidang keselamatan siber; dan
- Menjalani dan memperolehi kelulusan tapisan keselamatan daripada

agensi yang diberi kuasa.

iii. Pegawai Keselamatan ICT/ICTSO yang dilantik hendaklah memenuhi keperluan kompetensi di atas. ICTSO bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan siber di PLANMalaysia.

c) Peranan

i. Peranan Pengguna hendaklah diberi berdasarkan keperluan dan kompetensi Pengguna.

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

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

iv. Pegawai Aset yang menguruskan aset ICT hendaklah memastikan semua aset ICT PLANMalaysia dikembalikan sekiranya berlaku perubahan peranan.

v. Pengguna yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset PLANMalaysia yang berkaitan seperti tersenarai dalam senarai aset pada Nota Serah Tugas.

vi. Pengguna yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset PLANMalaysia dengan diselia oleh Pegawai Aset yang dipertanggungjawabkan oleh PLANMalaysia.

6.3 PROSES

Pengguna hendaklah memastikan keselamatan siber dengan melaksanakan perkara-perkara berikut:

a) Konfigurasi Asas

i. Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem.

ii. Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan Prosedur Kawalan Perubahan.

b) Kawalan Perubahan Konfigurasi

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

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

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

c) Sandaran

i. Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan sekiranya berlaku sebarang bencana.

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

d) Kitaran Pengurusan Aset

i. Pindah

- Pemindahan hak milik aset berlaku dalam keadaan berikut:
  - Pengguna meninggalkan agensi disebabkan oleh persaraan, perletakan jawatan atau penugasan semula;
  - Aset yang dikongsi untuk kegunaan sementara;
  - Pemberian aset kepada agensi lain; dan
  - Aset dikembalikan setelah tamat tempoh sewaan.

- Data dalam peranti tersebut hendaklah diuruskan mengikut Prosedur Pelupusan.

ii. Pelupusan

- Pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu

mengandungi maklumat terperingkat atau sebaliknya.

- Berdasarkan keputusan CGSO, pelupusan perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara [Akta 629] dan Peraturan- peraturan Arkib Negara yang sedang berkuatkuasa.
- Pelupusan boleh dilaksanakan dalam bentuk/ kaedah pemusnahan fizikal dan/ atau sanitasi data.
- Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa.

iii. Kitaran Hayat

- Kitaran hayat data hendaklah diuruskan mengikut Akta Arkib Negara [Akta 629] dan Peraturan-peraturan Arkib Negara yang sedang berkuatkuasa.
- Rekod kewangan hendaklah disimpan selama 7 tahun dan rekod umum selama 5 tahun.

6.4 TEKNOLOGI

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

a) Peringkat Pemprosesan Data

i. Data-dalam-simpanan

- PLANMalaysia hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-simpanan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-simpanan.
- Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

ii. Data-dalam-pergerakan

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

iii. Data-dalam-penggunaan

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

iv. Perlindungan Ketirisan/Kebocoran Data

- Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.
- Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

b) Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan Penilaian Pisiko dan Pelan Pengurusan Risiko, PLANMalaysia hendaklah menggunakan kaedah teknologi dan kawalan keselamatan (*counter measure dan control measure*) yang dapat melindungi data di semua peringkat saluran pemprosesan bagi semua elemen dalam persekitaran pengkomputeran.

Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam persekitaran pengkomputeran mengikut Arahan Keselamatan yang dikeluarkan oleh CGSO atau mendapat pengesahan dari CGSO.

Setiap projek ICT yang dibangunkan di PLANMalaysia hendaklah mempunyai pengurusan keselamatan maklumat tersendiri yang mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

i. Peranti Pengkomputeran Peribadi

- Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja, *desktop*, telefon pintar, tablet, dan peranti storan.
- Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada PLANMalaysia. Walau bagaimanapun, peranti pengkomputeran peribadi milik persendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk

ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada Pelan Penguraian Risiko.

ii. Peranti Rangkaian

- Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti *switch, router, firewall*, peranti VPN dan kabel.
- Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diambil kira dalam pengurusan keselamatan maklumat.

iii. Perisian Aplikasi

- Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.
- Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diambil kira dalam pengurusan keselamatan maklumat.

iv. Pelayan

- Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.
- Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam- penggunaan, data-dalam-pergerakan, data- dalam-simpanan dan menghalang ketirisan data hendaklah diambil kira dalam pengurusan keselamatan maklumat.

v. Persekitaran Fizikal

- Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.
- Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip defence-in-depth.
- Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diambil kira dalam pengurusan keselamatan maklumat.

7.0 PENILAIAN RISIKO KESELAMATAN SIBER

PLANMalaysia hendaklah mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT dan ruang siber supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT dan ruang siber. PLANMalaysia hendaklah melaksanakan penilaian risiko keselamatan siber secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan siber. Seterusnya mengambil tindakan susulan dan/ atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan siber berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan siber hendaklah dilaksanakan ke atas sistem maklumat PLANMalaysia termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik penyelenggaraan, kemudahan utiliti dan sistem-sistem sokongan lain. PLANMalaysia bertanggungjawab melaksanakan dan menguruskan risiko keselamatan selaras dengan keperluan Surat PekelilingArahan/Garis Panduan Penilaian Risiko Keselamatan Maklumat yang sedang berkuatkuasa.

PLANMalaysia hendaklah mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a) mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

b) menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan atasan;

c) mengelak dan/atau mencegah risiko daripada terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan

d) memindahkan risiko kepada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

8.0 PELAN PENGURUSAN KESELAMATAN MAKLUMAT

Setiap projek di PLANMalaysia hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain. Pelan ini hendaklah mengenal pasti perlindungan data- dalam-penggunaan, data-dalam pergerakan, data dalam-simpanan dan menghalang ketirisan data dan maklumat.

Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), DKS KPKT dan surat pekeliling/ arahan terkini untuk

menangani isu-isu operasi sesebuah projek.

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

a) Peranti Pengkomputeran Peribadi

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

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

b) Peranti Rangkaian

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

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

c) Aplikasi

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

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

d) Pelayan

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

ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-

dalam-penggunaan, data-dalam- pergerakan, data-dalam-simpanan dan menghalang ketirisan data dan maklumat hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

e) Persekitaran Fizikal

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

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

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

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

9.0 PERNYATAAN DASAR KESELAMATAN SIBER PLANMALAYSIA

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

Keselamatan siber adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem komputer berjalan secara berterusan tanpa gangguan. Keselamatan siber berkait rapat dengan perlindungan aset ICT,manusia dan persekitaran bekerja. Lima (5) komponen asas keselamatan siber adalah seperti berikut:

a) Melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan dari capaian tanpa kuasa yang sah;

b) Menjamin setiap maklumat adalah tepat dan sempurna;

c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna;

d) Memastikan akses hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat daripada sumber yang sah; dan

e) Menghindari ruang siber dari menimbulkan berbagai ancaman dan potensi ancaman serta gangguan mulai dari skala kecil hingga skala yang besar.

DKS PLANMalaysia merangkumi perlindungan semua bentuk maklumat sama ada maklumat elektronik atau bukan elektronik yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bertujuan untuk menjamin keselamatan dan ketersediaan maklumat kepada semua Pengguna, Pembekal dan Pihak Ketiga yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

a) Kerahsiaan

Data dan maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

b) Integriti

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

c) Tidak Boleh Disangkal

Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

d) Kesahihan

Data dan maklumat hendaklah dijamin kesahihannya; dan

e) Ketersediaan

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

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

10.0 BIDANG KAWALAN

Sebagai mendokong pematuhan DKS PLANMalaysia bagi mengelakkan sebarang bentuk pelanggaran ke atasnya, bidang-bidang keselamatan siber yang berkaitan dinyatakan dengan jelas sebagai panduan/ pembudayaan/ ikutan/ pemahaman. Terdapat 4 bidang keselamatan yang merujuk kepada Annex A piawaian ISO/IEC 27001:2022 Information Security Management Systems. 4 bidang tersebut adalah seperti Jadual 2:14 Bidang Kawalan Keselamatan Siber PLANMalaysia.

Jadual 2:14 Bidang Kawalan Keselamatan Siber PLANMalaysia

BIDANG	TAJUK	BILANGAN KAWALAN
01	Kawalan Organisasi	36
02	Kawalan Manusia	8
03	Kawalan Fizikal	14
04	Kawalan Teknologi	34

Seterusnya setiap bidang kawalan keselamatan siber ini diterangkan secara lebih terperinci.

BIDANG 01: KAWALAN ORGANISASI

0101 Dasar Keselamatan Maklumat

Objektif:

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

010101 Pelaksanaan DKS PLANMalaysia	Tanggungjawab
Pelaksanaan dasar ini akan dijalankan dengan arahan Ketua Pengarah (KP) PLANMalaysia.	KP
010102 Penyebaran/Hebahan DKS PLANMalaysia	**Tanggungjawab**
DKS ini perlu dihebahkan kepada semua Pengguna, Pembekal dan Pihak Ketiga dari semasa ke semasa yang menggunakan aset ICT dan ruang siber di PLANMalaysia.	STM
010103 Pematuhan dan Pengecualian DKS PLANMalaysia	**Tanggungjawab**
DKS PLANMalaysia perlu dipatuhi dan terpakai kepada semua Pengguna, Pembekal dan Pihak Ketiga. Tiada pengecualian bagi pematuhan DKS PLANMalaysia.	Pengguna, Pembekal dan Pihak Ketiga
010104 Penyelenggaraan DKS PLANMalaysia	**Tanggungjawab**
DKS PLANMalaysia adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi,aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. DKS PLANMalaysia hendaklah dikaji semula dengan kekerapan sekurang-kurangnya sekali dalam dua (2) tahun atau mengikut keperluan. Berikut adalah Prosedur Penyelenggaraan DKS PLANMalaysia: (a) Mengenal pasti dan menentukan pindaan yang diperlukan;	Ahli Jawatankuasa Kajian Semula Pengurusan (JKSP) ISMS PLANMalaysia

(b) Mengemukakan cadangan pindaan yang telah diselaras kepada JKSP ISMS PLANMalaysia; (c) Mengemukakan cadangan pindaan secara bertulis untuk mendapat kelulusan Mesyuarat JPICT PLANMalaysia; (d) Meminda dokumen DKS kepada versi baharu setelah pindaan diluluskan; dan (e) Memaklumkan pemakaian/penguatkuasaan DKS versi terkini kepada Pengguna, Pembekal dan Pihak Ketiga.	

0102 Peranan Dan Tanggungjawab Dalam Keselamatan Maklumat	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKS PLANMalaysia.	
010201 Ketua Pengarah (KP) PLANMalaysia	**Tanggungjawab**
Peranan dan tanggungjawab KP adalah seperti berikut: (a) Menentukan halatuju dan strategi pelaksanaan keselamatan siber PLANMalaysia; (b) Memastikan semua keperluan organisasi (contoh: sumber kewangan, sumber manusia dan sumber perlindungan keselamatan) adalah mencukupi; (c) Memastikan penilaian risiko keselamatan siber dilaksanakan seperti yang ditetapkan di dalam DKS PLANMalaysia; (d) Memastikan program keselamatan siber dilaksanakan; (e) Memastikan perancangan, penyelarasan dan penyeragaman pelaksanaan program/projek-projek keselamatan siber PLANMalaysia supaya selaras dengan **Pelan Strategik Pendigitalan (PSP) PLANMalaysia** yang sedang berkuatkuasa; dan (f) Melantik CDO PLANMalaysia dan ICTSO PLANMalaysia.	KP
010202 Ketua Pegawai Digital (CDO) PLANMalaysia	**Tanggungjawab**
Timbalan Ketua Pengarah (Pembangunan) PLANMalaysia ialah CDO PLANMalaysia yang dilantik oleh KP. Peranan dan tanggungjawab CDO PLANMalaysia adalah seperti berikut: (a) Meneraju inisiatif pendigitalan di Kementerian/Agensi melalui penggunaan data, analisis dan teknologi digital; (b) Mewujudkan budaya berpacukan data dalam sektor awam yang mengamalkan pendekatan *principle-based* melalui penggunaan data dan teknologi digital; (c) Mentransformasi penyampaian perkhidmatan digital di Kementerian/Agensi berfokuskan pengalaman pelanggan (*customer*	CDO PLANMalaysia

experience) yang berteraskan konsep *Whole-of-Government* melalui inovasi melibatkan perkongsian data, data terbuka dan teknologi baru muncul; (d) Menilai, menyelaras, memperaku keperluan perkhidmatan digital, *Technical Service Design* dan bajet pembangunan serta mengurus agensi sebagai pelaksana inisiatif dan projek pendigitalan; (e) Meneraju perubahan melalui Penjajaran Pelan Strategik Pendigitalan (PSP) Kementerian/Negeri/Agensi dengan: i. Memastikan PSP Agensi selari dengan PSP Sektor Awam dan Pengurusan Risiko dan Pelan Pengurusan Perubahan; ii. Memastikan *blueprint Enterprise Architecture* (EA) agensi tersedia; dan iii. Memantapkan struktur tadbir urus pendigitalan agensi & menyelaras penggunaan dasar, standard dan amalan terbaik global. (f) Melaporkan pelaksanaan dan kemajuan transformasi pendigitatan kepada YBhg. Ketua Setiausaha Negara sebagai Pengerusi Kluster Kerajaan di bawah Majlis Ekonomi Digital dan 41R Negara melalui sekretariat kluster kerajaan.	
010203 Ketua Pegawai Keselamatan (PK) PLANMalaysia	**Tanggungjawab**
KPK PLANMalaysia ialah Timbalan Ketua Pengarah (Perancangan). Peranan dan tanggungjawab KPK PLANMalaysia adalah seperti berikut: (a) Membantu melaksana urusan pergerakan kunci-kunci bangunan peringkat kementerian; (b) Membantu melaksana hal ehwal keselamatan di dalam peringkat kementerian; (c) Melaksanakan pemeriksaan operasi keselamatan dan kesihatan bersama jabatan lain di peringkat kementerian; (d) Melaksanakan dan bekerjasama dengan pihak berkuasa bagi keselamatan dan ketenteraman awam di kementerian ; dan (e) Menyediakan laporan ringkas jika ada melibatkan keselamatan fizikal, personel dan dokumen untuk diambil tindakan oleh pihak berkenaan.	KPK PLANMalaysia

010204 Jawatankuasa Pemandu ICT (JPICT) PLANMalaysia	Tanggungjawab
Keahlian JPICT PLANMalaysia adalah terdiri daripada: Pengerusi: Ketua Pengarah (KP) PLANMalaysia atau Timbalan Ketua Pengarah PLANMalaysia Ahli-ahli: i. Pengarah Bahagian Penyelidikan dan Pembangunan ii. Pengarah Bahagian Rancangan Fizikal Negara iii. Pengarah Bahagian Perundangan dan Kawal Selia Perancangan iv. Pengarah Bahagian Maklumat Gunatanah Negara v. Pengarah Bahagian Korporat vi. Pengarah Bahagian Perancangan Wilayah vii. Pengarah Pejabat Projek Zon Tengah viii. Pengarah Pejabat Projek Zon Timur ix. Pengarah Pejabat Projek Zon Utara x. Pengarah Pejabat Projek Zon Selatan xi. Pengarah Bahagian Khidmat Pengurusan xii. Ketua Unit Penyelarasan Projek xiii. Ketua Unit Integriti Urus Setia: Seksyen Teknologi Maklumat (STM) PLANMalaysia. Peranan dan tanggungjawab JPICT PLANMalaysia adalah seperti berikut: (a) Menetapkan arah tuju dan strategi untuk pembangunan dan pelaksanaan ICT PLANMalaysia; (b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/strategi ICT PLANMalaysia; (c) Memantau pelaksanaan pensijilan ISMS PLANMalaysia; (d) Memantau status kemajuan ISMS; (e) Meluluskan Dasar Keselamatan Siber (DKS) PLANMalaysia; (f) Meluluskan Skop ISMS; dan (g) Meluluskan Tadbir Urus ISMS.	JPICT PLANMalaysia
010205 Organisasi Pensijilan Sistem Pengurusan Keselamatan	**Tanggungjawab**

Maklumat (ISMS) PLANMalaysia	
Struktur organisasi ISMS PLANMalaysia melibatkan Jawatankuasa Pemandu ICT (JPICT), Jawatankuasa Kajian Semula Pengurusan ISMS, dan Jawatankuasa Pelaksana ISMS yang turut sama dibantu oleh Pasukan Penyelaras ISMS. Di samping itu, tadbir urus ISMS turut melibatkan kumpulan audit ISMS yang terdiri daripada Audit Dalam dan Audit Pensijilan ISMS. Struktur organisasi ISMS adalah seperti yang telah didokumenkan di dalam Manual ISMS PLANMalaysia (PLANMalaysia-ISMS-P1-002).	Jawatankuasa ISMS PLANMalaysia
010206 Koordinator Pengurusan Kesinambungan Perkhidmatan (PKP) PLANMalaysia	**Tanggungjawab**
Koordinator PKP PLANMalaysia ialah pegawai yang dilantik oleh KP. Peranan dan tanggungjawab Koordinator PKP PLANMalaysia adalah seperti berikut: (a) Bertindak sebagai pegawai perhubungan (single point of contact) bagi aktiviti pemulihan bencana dan mengetuai pelaksanaan aktiviti pemulihan bencana; (b) Memastikan ujian simulasi pemulihan bencana dijalankan mengikut jadual atau mengikut perancangan yang telah dipersetujui; (c) Mengurus penyediaan laporan ujian (post-mortem) dan melaksanakan penambahbaikan dokumen PKP; dan (d) Menyediakan dan melaksanakan penambahbaikan dokumen PKP.	Koordinator PKP PLANMalaysia
010207 Pegawai Keselamatan ICT (ICTSO PLANMalaysia)	**Tanggungjawab**
ICTSO bagi PLANMalaysia ialah Pegawai Teknologi Maklumat yang dilantik oleh KP. ICTSO merupakan ahli Pasukan CSIRT PLANMalaysia. Peranan dan tanggungjawab ICTSO PLANMalaysia adalah seperti berikut: (a) Mengkaji dan melaksanakan kawalan keselamatan siber selaras dengan keperluan PLANMalaysia; (b) Menentukan kawalan akses pengguna terhadap aset ICT;	ICTSO PLANMalaysia

(c) Melaporkan sebarang insiden atau penemuan mengenai keselamatan siber kepada Pengarah CSIRT; (d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan siber; (e) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; dan (f) Menangani insiden keselamatan siber PLANMalaysia.	
010208 Pasukan Cyber Security Incident Response Team (CSIRT) PLANMalaysia	**Tanggungjawab**
Keahlian CSIRT PLANMalaysia adalah terdiri daripada: <u>Pengarah CSIRT</u>: Timbalan Ketua Pengarah (Pembangunan) *Chief Digital Officer* (CDO) <u>Pengurus CERT:</u> Ketua Seksyen Teknologi Maklumat Bahagian Khidmat Pengurusan <u>Ahli CERT:</u> i. Pegawai Perancang Bandar dan Desa, Unit Malaysia Urban Observatory (MUO); ii. Pegawai Perancang Bandar dan Desa, Bahagian Rancangan Fizikal Negara; iii. Pegawai Perancang Bandar dan Desa, Bahagian Penyelidikan dan Pembangunan; iv. Pegawai Teknologi Maklumat, Bahagian Khidmat Pengurusan; v. Penolong Pegawai Teknologi Maklumat, Bahagian Maklumat Gunatanah Negara; dan vi. Penolong Pegawai Teknologi Maklumat, Bahagan Khidmat Pengurusan.	CSIRT PLANMalaysia

Peranan dan tanggungjawab CERT PLANMalaysia adalah seperti berikut: (a) Memantau, mengesan insiden, menerima, mengesahkan aduan insiden keselamatan siber dan mengenal pasti jenis insiden serta menilai impak insiden; (b) Merekod dan menjalankan siasatan awal; (c) Melaksanakan pengurusan dan pengendalian insiden serta mengambil tindakan awal; (d) Menjalankan penialaian serta mendambil tindakan pengukuhan supaya insiden baharu dapat dielakkan; (e) Melapor insiden kepada KPKT dan NC4; (f) Menasihati agensi mengambil tindakan pemulihan dan pengukuhan; (g) Hebahan makluman dan amaran berkaitan insiden kepada kakitangan agensi; dan (h) Memastikan fail log disimpan sekurang-kurangnya enam bulan.	
010209 Pentadbir Sistem ICT	**Tanggungjawab**
Pentadbir Sistem ICT ialah pegawai PLANMalaysia yang dipertanggungjawabkan berdasarkan skop tugasan masing-masing seperti menyelenggara sistem aplikasi, sistem aplikasi mudah alih dan laman web. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (a) Mengambil tindakan segera mengikut proses yang ditetapkan apabila dimaklumkan perubahan pengguna ICT melibatkan urusan perkhidmatan atau berlaku perubahan dalam bidang kuasa; (b) Menentukan ketepatan dan kesempurnaan (integriti) sesuatu tahap capaian berdasarkan arahan Pemilik Sistem sebagaimana yang telah ditetapkan di dalam DKS PLANMalaysia; (c) Memantau aktiviti capaian harian sistem/aplikasi pengguna; (d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pengubahsuaian	Pemilik Sistem dan Pentadbir Sistem ICT PLANMalaysia

data tanpa kebenaran serta membatalkan atau memberhentikannya dengan serta-merta dan melaporkannya kepada PICT; (e) Menganalisis, menyimpan, melindungi dan membuat *backup* rekod jejak audit; dan (f) Menyediakan laporan mengenai aktiviti capaian secara berkala kepada Pemilik Sistem.	
010210 Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT	**Tanggungjawab**
Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT ialah pegawai PLANMalaysia yang dipertanggungjawabkan untuk merancang, mengurus, memantau dan menyelenggara Pusat Data, Rangkaian dan Komunikasi ICT. Peranan dan tanggungjawab Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT adalah seperti berikut: (a) Memastikan kerahsiaan akaun pentadbir; (b) Merangka, melaksana dan menguatkuasakan polisi keselamatan siber merangkumi: i. Perlindungan serta perkongsian data dan maklumat; ii. Ancaman keselamatan siber; dan iii. Capaian rangkaian dan komunikasi ICT. (c) Memastikan semua aset di Pusat Data berfungsi dan beroperasi dengan sempurna; (d) Menyelia dan membuat proses *backup* dan *restore*; dan (e) Menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian dan komunikasi ICT dan memantau operasi serta prestasi rangkaian dan komunikasi ICT.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia
010211 Pegawai Aset	**Tanggungjawab**
Pegawai Aset ialah pegawai PLANMalaysia yang dilantik oleh KP selaku Pengerusi Jawatankuasa Pengurusan Aset Kerajaan (JKPAK) peringkat Jabatan yang bertanggungjawab menguruskan aset kerajaan berdasarkan pekeliling yang berkuatkuasa.	KP/Pengerusi Jawatankuasa Pengurusan Aset Kerajaan

Peranan dan tanggungjawab Pegawai Aset adalah seperti berikut: (a) Memastikan pengurusan aset Kerajaan dijalankan selaras dengan peraturan yang ditetapkan dan pekeliling yang berkuatkuasa; (b) Memastikan penerimaan aset Kerajaan dilaksanakan oleh pegawai yang dilantik secara bertulis oleh KP selaku Pengerusi Jawatankuasa Pengurusan Aset Kerajaan (JKPAK); (c) Memastikan semua aset Kerajaan yang diterima, didaftarkan dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset; (d) Memastikan semua aset Kerajaan yang dipinjam, direkodkan ke dalam Rekod Pergerakan/Peminjaman Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan bertulis daripada Ketua Jabatan di PLANMalaysia; (e) Memastikan Daftar Aset dikemaskini apabila berlaku penambahan/penggantian/penaiktarafan aset termasuk selepas pemeriksaan aset, pelupusan, pindahan dan hapus kira; (f) Memastikan semua aset Kerajaan diberi tanda pengenalan dengan cara melabel/mengecat/mencetak timbul (emboss) tanda Hak Kerajaan Malaysia dan nama PLANMalaysia di tempat yang mudah dilihat dan sesuai pada aset berkenaan; (g) Memastikan semua aset Kerajaan dilabelkan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan; (h) Memastikan senarai daftar induk aset Kerajaan disediakan; (i) Memastikan senarai aset Kerajaan mengikut lokasi disediakan berdasarkan format Senarai Aset Alih Kerajaan dalam dua (2) salinan. Satu (1) senarai berkenaan perlu disimpan oleh Pegawai Aset dan satu (1) salinan perlu dipaparkan oleh pegawai yang bertanggungjawab di lokasi; (j) Memastikan setiap kerosakan aset Kerajaan dilaporkan; (k) Bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset Kerajaan; (l) Merancang, memantau dan memastikan pemeriksaan aset Kerajaan dilaksanakan ke atas keseluruhan aset alih Kerajaan sekurang-kurangnya sekali setahun; dan (m) Memastikan setiap kes kehilangan aset Kerajaan dilaporkan dan diuruskan dengan teratur.	(JKPAK), dan Pegawai Aset PLANMalaysia

010212 Unit Komunikasi Korporat dan Hubungan Awam	Tanggungjawab
Unit Komunikasi Korporat dan Hubungan Awam ialah pegawai PLANMalaysia yang menguruskan hal ehwal media sosial. Peranan dan tanggungjawab Unit Komunikasi Korporat dan Hubungan Awam adalah seperti berikut: (a) Memaklumkan tujuan pewujudan media sosial dan mendapat perakuan mematuhi syarat-syarat sebagai ahli kumpulan media sosial tersebut; (b) Sentiasa peka terhadap peraturan atau syarat-syarat yang ditetapkan oleh penyedia platform; (c) Melaksanakan pemantauan terhadap pengguna untuk memastikan pengguna sentiasa mematuhi syarat-syarat serta garis panduan keselamatan media sosial yang telah ditetapkan; dan (d) Melaporkan sebarang pelanggaran polisi penggunaan yang sedang berkuatkuasa.	Unit Komunikasi Korporat dan Hubungan Awam PLANMalaysia
010213 Pengguna	**Tanggungjawab**
Pengguna mempunyai peranan dan tanggungjawab seperti berikut: (a) Membaca, memahami, dan mematuhi DKS PLANMalaysia; (b) Mengetahui dan memahami implikasi keselamatan siber akibat daripada tindakannya; (c) Menjalani tapisan keselamatan seperti yang diarahkan (sekiranya berkaitan) berdasarkan Arahan Keselamatan Kerajaan yang sedang berkuatkuasa; (d) Melaksanakan dan mematuhi prinsip-prinsip DKS PLANMalaysia serta menjaga kerahsiaan maklumat PLANMalaysia; (e) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; (f) Menghadiri program-program kesedaran mengenai keselamatan siber; dan (g) Menandatangani Surat Akuan Pematuhan DKS PLANMalaysia seperti **LAMPIRAN 1** melalui Sistem Pematuhan DKS PLANMalaysia.	Pengguna

0103 Pengasingan Tugas dan Tanggungjawab	
Objektif: Mengurangkan risiko penipuan, kesilapan dan pemintasan dalam kawalan keselamatan maklumat.	
010301 Keperluan Keselamatan Dalam Pengasingan Tugas	**Tanggungjawab**
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab termasuk mewujud, memadam, mengemas kini, mengubah dan mengesahkan perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan, akses atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT daripada ralat, kebocoran maklumat terperingkat atau dimanipulasi; (b) Aset ICT yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan daripada aset ICT yang digunakan sebagai persekitaran sebenar (*production*). Pengasingan juga merangkumi tindakan memisahkan antara kumpulan pembangun sistem dan pelaksana operasi; dan (c) Pengasingan tugas bagi tugasan yang bersifat kritikal tidak boleh dilaksanakan oleh seorang individu sahaja atas kuasa tunggalnya dan hendaklah dikendalikan dalam tadbir urus yang bersesuaian.	PICT,Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia

0104 Tanggungjawab Pengurusan	
Objektif: Memastikan pengurusan memahami peranan mereka dalam keselamatan maklumat dan mengambil tindakan yang bertujuan untuk memastikan semua kakitangan menyedari dan memenuhi tanggungjawab dalam keselamatan maklumat PLANMalaysia.	
010401 Tanggungjawab Pengurusan Terhadap Pengguna	**Tanggungjawab**
Pengurusan hendaklah memastikan pengguna yang mempunyai urusan dengan perkhidmatan ICT PLANMalaysia supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.	KP, CDO dan KPK

0105 Hubungan Dengan Pihak Berkuasa	
Objektif: Memastikan aliran maklumat berkaitan keselamatan berlaku dengan sewajarnya di antara PLANMalaysia dan pihak berkuasa.	
010501 Hubungan Dengan Pihak Berkuasa	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Mewujudkan dan mengemaskini senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan; (b) Pihak berkuasa perundangan ialah NC4, Polis Diraja Malaysia (PDRM) dan Suruhanjaya Komunikasi Dan Multimedia Malaysia (SKMM). Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan (c) Mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab PLANMalaysia.	Jawatankuasa Keselamatan PLANMalaysia

0106 Hubungan Dengan Pihak Berkepentingan Yang Khusus	
Objektif: Memastikan aliran maklumat berkaitan keselamatan berlaku dengan sewajarnya.	
010601 Hubungan Dengan Pihak Berkepentingan Yang Khusus	**Tanggungjawab**
Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan seperti *National Cyber Security Agency* (NACSA) dan pertubuhan profesional hendaklah dikekalkan. Keperluan hubungan dengan pihak berkepentingan yang khusus adalah seperti berikut: (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.	ICTSO

0107 Risikan Ancaman (*Threat Intelligence*)	
Objektif: Memberi kesedaran tentang persekitaran ancaman organisasi supaya tindakan mitigasi yang sewajarnya dapat diambil.	
010701 Keperluan Risikan Ancaman	**Tanggungjawab**
Maklumat mengenai ancaman sedia ada atau baharu hendaklah dikumpulkan daripada sumber luaran dan dalaman, dan dianalisis untuk: (a) Memudahkan tindakan sewajarnya diambil untuk mencegah ancaman daripada menyebabkan kemudaratan kepada	Pentadbir Rangkaian

organisasi; dan (b) Mengurangkan kesan ancaman tersebut. Aktiviti perisikan ancaman hendaklah termasuk: (a) Mengenal pasti, memeriksa dan memilih sumber maklumat dalaman dan luaran yang diperlukan dan sesuai untuk melaksanakan tindakan yang diperlukan berdasarkan pengeluaran perisikan ancaman; (b) Memproses dan menganalisis maklumat untuk memahami bagaimana ia berkaitan dan bermakna kepada organisasi; dan (c) Berkomunikasi dan berkongsi kepada individu yang berkaitan dalam format yang boleh difahami. Perisikan ancaman hendaklah dianalisis dan kemudian digunakan: (a) Dengan melaksanakan proses untuk memasukkan maklumat yang dikumpulkan dari sumber perisikan ancaman ke dalam proses pengurusan risiko keselamatan maklumat organisasi; (b) Sebagai input tambahan kepada kawalan pencegahan dan pengesanan teknikal seperti *firewall*, *intrusion detection system*, atau penyelesaian anti perisian hasad; dan (c) Sebagai input kepada proses dan teknik Penilaian Tahap Keselamatan.	

0108 Keselamatan Maklumat Dalam Pengurusan Projek

Objektif:

Mengenal pasti risiko keselamatan maklumat bagi mengawal dan menjamin keselamatan maklumat dalam pengurusan projek.

010801 Pengurusan Projek ICT dan Keselamatan Maklumat	Tanggungjawab
Pengurusan Projek ICT merupakan satu pengurusan proses dan prosedur dalam satu tempoh masa, sumber dan tahap kualiti yang ditetapkan bagi menghasilkan satu atau lebih produk ICT. Keselamatan maklumat perlu diambil kira dalam pengurusan projek bagi melindungi maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan objektif keselamatan maklumat dimasukkan di dalam objektif projek; (b) Melaksanakan penilaian risiko keselamatan maklumat hendaklah di peringkat awal pelaksanaan projek bagi menentukan kaedah kawalan yang bersesuaian; (c) Memastikan keselamatan maklumat bagi setiap fasa metodologi pembangunan projek dilaksanakan; dan (d) Memastikan implikasi keselamatan maklumat bagi semua projek ditangani secara teratur dan berkesan.	CDO, PICT, Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia, Pembekal dan Pihak Ketiga

0109 Pengurusan Aset ICT

Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset PLANMalaysia.

010901 Aset ICT	Tanggungjawab
Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh Pengguna masing-masing. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT perolehan secara pembelian dikenal pasti dan maklumat aset direkodkan serta dikemaskini dari semasa ke semasa ke dalam sistem pengurusan aset berdasarkan pekeliling yang sedang berkuatkuasa; (b) Memastikan semua aset perolehan secara sewaan dikenal pasti dan maklumat aset direkodkan serta dikemaskini dari semasa ke semasa; (c) Memastikan semua aset ICT diuruskan oleh Penyelaras ICT/Pegawai Aset dan dikendalikan oleh Pengguna yang dibenarkan sahaja; (d) Memastikan semua Pengguna mengesahkan penempatan aset ICT yang ditempatkan; (e) Peraturan bagi pengendalian aset ICT hendaklah dipatuhi dan dilaksanakan; (f) Setiap Pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan (g) Memastikan semua aset ICT diagihkan kepada Pengguna mengikut piawaian dan garis panduan yang ditetapkan.	Pegawai Aset, Penyelaras ICT PLANMalaysia dan Pengguna

0110 Penggunaan Maklumat Dan Aset ICT

Objektif:

Memastikan maklumat dan aset ICT dilindungi, diguna dan dikendali sewajarnya.

011001 Pengendalian Aset	Tanggungjawab
Aktiviti pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) Menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberi perhatian terutama semasa aktiviti pengendalian maklumat terperingkat; (g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum; dan (h) Mewujudkan sandaran/ salinan pendua maklumat penting bagi mengurangkan risiko kehilangan dan kemusnahan serta memelihara kerahsiaan maklumat terperingkat.	Pengguna

0111 Pemulangan Aset ICT

Objektif:

Melindungi aset PLANMalaysia sebagai sebahagian dari proses pertukaran atau penamatan perkhidmatan kakitangan, kontrak dan perjanjian.

011101 Pemulangan Aset ICT	Tanggungjawab
Memastikan semua Pengguna, Pembekal dan Pihak Ketiga yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT sebelum **bertukar atau tamat perkhidmatan** agar meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna perlu menyatakan dengan lengkap dan jelas peranan dan tanggungjawab dalam menjamin keselamatan aset ICT secara bertulis selepas perkhidmatan; (b) Pengguna perlu memastikan semua aset ICT dikembalikan kepada PLANMalaysia mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (c) Pengguna, Pembekal dan Pihak Ketiga perlu memastikan kebenaran capaian ke atas maklumat dan kemudahan proses maklumat dibatalkan atau ditarik balik dengan serta-merta mengikut peraturan yang ditetapkan oleh PLANMalaysia; (d) Pengguna, Pembekal dan Pihak Ketiga perlu melaksanakan perakuan bagi melupuskan semua maklumat terperingkat dalam simpanan secara selamat; dan (e) Menandatangani Borang Pengesahan Pegawai Bertukar Keluar Atau Tamat Perkhidmatan Di PLANMalaysia seperti **LAMPIRAN 2**.	Pengguna, Pembekal dan Pihak Ketiga

0112 Pengelasan Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
011201 Pengelasan Maklumat	**Tanggungjawab**
Maklumat hendaklah dikelaskan sewajarnya oleh pegawai yang diberi kuasa mengikut Arahan Keselamatan Kerajaan yang sedang berkuatkuasa. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan dalam Arahan Keselamatan Kerajaan yang sedang berkuatkuasa seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad.	Pegawai Pengelas

0113 Pertukaran Maklumat	
Objektif: Memastikan keselamatan perpindahan/ pertukaran data, maklumat dan perisian antara PLANMalaysia dan pihak luar terjamin.	
011301 Polisi dan Prosedur Pemindahan/ Pertukaran Data dan Maklumat	**Tanggungjawab**
PLANMalaysia perlu mengambil kira keselamatan maklumat apabila berlaku pemindahan data dan maklumat organisasi antara PLANMalaysia dengan pihak luar. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mewujudkan polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; (b) Menyediakan perjanjian atau kebenaran bertulis untuk pertukaran maklumat dan perisian di antara PLANMalaysia dengan pihak agensi luar; (c) Melindungi media yang mengandungi maklumat daripada capaian yang tidak dibenarkan, didedahkan, disalah guna atau dirosakkan semasa pemindahan keluar dari PLANMalaysia; dan (d) Memastikan maklumat yang terdapat dalam mel elektronik hendaklah dilindungi sebaik-baiknya.	PICT, ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia dan Pengguna
011302 Pengurusan Pertukaran Maklumat	**Tanggungjawab**
PLANMalaysia perlu mengambil kira keselamatan maklumat apabila berlaku pemindahan data dan maklumat organisasi antara PLANMalaysia dengan pihak luar. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mewujudkan polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; (b) Menyediakan perjanjian atau kebenaran bertulis untuk pertukaran maklumat dan perisian di antara PLANMalaysia	PICT, ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia dan Pengguna

dengan pihak agensi luar; (c) Melindungi media yang mengandungi maklumat daripada capaian yang tidak dibenarkan, didedahkan, disalah guna atau dirosakkan semasa pemindahan keluar dari PLANMalaysia; dan (d) Memastikan maklumat yang terdapat dalam mel elektronik hendaklah dilindungi sebaik-baiknya.	
011303 Perjanjian Mengenai Pemindahan/ Pertukaran Data dan Maklumat	**Tanggungjawab**
PLANMalaysia perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan/pertukaran data dan maklumat organisasi antara PLANMalaysia dengan pihak luar. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal penghantaran dan penerimaan maklumat; (b) Memastikan prosedur keupayaan mengesan dan tanpa sangkalan semasa pemindahan/pertukaran data dan maklumat; (c) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan/pertukaran data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan (d) Mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.	CDO, Pemilik Sistem dan PICT PLANMalaysia
011304 Pengurusan Mel Elektronik	**Tanggungjawab**
Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa yang sedang berkuatkuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan pesanan elektronik disediakan untuk memudahkan komunikasi antara Pengguna, Pembekal dan Pihak Ketiga hanya untuk kegunaan perniagaan dengan sekatan-sekatan tertentu; (b) Penghantaran e-mel dan kepilan tidak berkaitan tugas rasmi	Pengguna

harian adalah dilarang; (c) Mesej yang dihantar hendaklah ringkas dan ditujukan kepada yang berkenaan sahaja; (d) Mesej yang dihantar tidak menggunakan akaun orang lain melainkan dengan arahan yang telah ditetapkan; dan (e) Pengguna dilarang mengulang hantar/*forward* maklumat terhad tanpa kebenaran penghantar/ pemunya maklumat. E-mel merupakan surat, pesanan atau mesej dalam bentuk fail komputer yang dikirim dan diterima melalui sistem rangkaian komputer. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan akaun e-mel yang diperuntukkan oleh PLANMalaysia sahaja sebagai e-mel rasmi; (b) Memastikan pengemaskinian peti e-mel (mailbox) dilaksanakan supaya kapasiti e-mel tidak melebihi kuota yang telah ditetapkan; (c) Menggunakan akaun e-mel rasmi untuk tujuan tugas rasmi sahaja; (d) Mengambil tindakan dan memberi maklum balas segera terhadap e-mel; dan (e) Memastikan e-mel rasmi yang dihantar atau diterima disimpan mengikut prosedur pengurusan sistem fail elektronik yang telah ditetapkan.	
011305 Keselamatan Media Sosial	**Tanggungjawab**
Keselamatan media sosial merupakan proses menyingkirkan ancaman keselamatan melalui pemantauan keselamatan siber. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara; (b) Tidak melibatkan penyebaran maklumat dan dokumen	Pentadbir Media Sosial PLANMalaysia

terperingkat; (c) Tidak memaparkan kenyataan yang boleh menjejaskan imej Kerajaan; (d) Tidak menyentuh isu sensitif seperti agama, politik dan perkauman; (e) Tidak memaparkan kenyataan yang berunsur fitnah atau hasutan; (f) Tidak menyebarkan berita yang tidak sahih; (g) Tidak melibatkan diri dengan aktiviti yang boleh menjurus kepada *CyberStalking* atau *CyberHarassment*; (h) Tidak menggunakan media sosial untuk tujuan peribadi semasa waktu pejabat sama ada menerusi peralatan komputer/peranti mudah alih yang dibekalkan oleh Kerajaan; (i) Mematuhi dasar dan peraturan semasa berkaitan media sosial yang sedang berkuatkuasa; dan (j) Memastikan keselamatan media sosial dengan melaporkan masalah yang berlaku seperti spam dan pencerobohan kepada penyedia perkhidmatan media sosial.	

0114 Kawalan Capaian	
Objektif: Memastikan hanya capaian yang disahkan dan mengelakkan capaian yang tidak sah kepada maklumat dan aset ICT.	
011401 Dasar Kawalan Capaian	**Tanggungjawab**
Kawalan Capaian/Akses merupakan pendekatan untuk mengehadkan capaian sistem kepada Pengguna yang berdaftar. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Melaksanakan kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan Pengguna; (b) Melaksanakan kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Melaksanakan keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan (d) Melaksanakan kawalan ke atas kemudahan pemprosesan maklumat.	ICTSO,Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian danKomunikasi ICT, Pentadbir Peralatan ICT PLANMalaysiadan Pengguna

0115 Pengurusan Identiti

Objektif:

Membenarkan individu dan sistem yang menggunakan identiti unik membuat capaian kepada maklumat PLANMalaysia dan aset ICT serta melaksanakan tugasan berdasarkan hak capaian.

011501 Pendaftaran Dan Penamatan Pengguna	Tanggungjawab
Setiap Pengguna adalah bertanggungjawab ke atas aset ICT yang digunakan. Akaun Pengguna diwujudkan bagi mengenalpasti Pengguna dan aktiviti yang dilakukan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Akaun yang diperuntukkan sahaja boleh digunakan; (b) Akaun Pengguna mestilah unik; (c) Pengguna bertanggungjawab sepenuhnya ke atas segala kegunaan melalui akaun dan kata laluannya; (d) Akaun Pengguna akan dibeku atau ditamatkan atas sebab-sebab berikut: i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi 90 hari; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan. (e) Sebarang perubahan tahap akses bagi Pengguna hendaklah mendapat kelulusan daripada Pemilik Sistem; dan (f) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang.	Pemilik Sistem, Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia dan Pengguna

0116 Pengesahan Maklumat	
Objektif: Memastikan pengesahan entiti yang betul dan mengelakkan kegagalan ketika proses pengesahan.	
011601 Pengurusan Maklumat Pengesahan Rahsia Pengguna	**Tanggungjawab**
(a) Maklumat pengesahan rahsia bagi pengguna hendaklah dikawal dan diselia melalui proses pengurusan yang formal; dan (b) Maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.	ICTSO dan Pentadbir Sistem
011602 Penggunaan Maklumat Pengesahan Rahsia Pengguna	**Tanggungjawab**
(a) Mengikut amalan keselamatan baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti; dan (b) Melaksanakan langkah-langkah perlindungan seperti 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; dan iv. Menjaga kerahsiaan kata laluan.	ICTSO, Ketua Sekysen/ Bahagian, Pentadbir Sistem dan Pengguna
011603 Pengurusan Kata Laluan	**Tanggungjawab**
Pengurusan kata laluan mestilah mematuhi amalan terbaik serta memastikan keselamatan kata laluan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;	Pentadbir Sistem ICT, Pentadbir Pusat Data Rangkaian dan Komunikasi ICT PLANMalaysia dan Pengguna

(b) Kata laluan hendaklah ditukar apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Kata laluan hendaklah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus; (d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun; (e) Kata laluan windows dan screen saver hendaklah diaktifkan apabila meninggalkan komputer melebihi 10 minit; (f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; (g) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (h) Kata laluan hendaklah ditukar dalam tempoh yang ditetapkan; dan (i) Sistem aplikasi yang dibangunkan digalakkan mempunyai kemudahan menukar kata laluan oleh Pengguna.	

0117 Hak Capaian

Objektif:

Memastikan capaian kepada maklumat dan aset ICT ditakrifkan dan disahkan mengikut keperluan perkhidmatan PLANMalaysia.

011701 Capaian/Akses Pengguna	Tanggungjawab
Capaian/Akses Pengguna melibatkan aktiviti muat naik, muat turun dan penggunaan untuk tujuan yang dibenarkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Sebarang bahan yang dimuat turun daripada Internet hendaklah digunakan untuk tujuan yang dibenarkan; dan (b) Pengguna adalah DILARANG melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen serta sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian Internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah, jenayah atau pernyataan berbentuk hasutan tanpa kebenaran berbuat demikian.	Pengguna

0118 Keselamatan Maklumat Berhubung Dengan Pembekal	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).	
011801 Dasar Keselamatan Maklumat Ke Atas Pembekal	**Tanggungjawab**
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset PLANMalaysia. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori; (b) Proses kitaran hayat (*lifecycle*) yang seragam untuk menguruskan Pembekal; (c) Mengawal dan memantau akses oleh Pembekal; (d) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; (e) Jenis-jenis obligasi kepada Pembekal; (f) Melaksanakan hebahan kesedaran terhadap Dasar Keselamatan Siber PLANMalaysia kepada Pembekal; (g) Menandatangani Surat Akuan Pematuhan DKS seperti **LAMPIRAN 1**; dan (h) Pembekal perlu mematuhi Arahan Keselamatan Kerajaan yang sedang berkuatkuasa.	Pemilik Sistem, PICT dan Pembekal

0119 Menangani Keselamatan Maklumat Dalam Perjanjian Dengan Pembekal	
Objektif: Mengekalkan tahap persetujuan bagi keselamatan maklumat dalam hubungan pembekal.	
011901 Menangani Keselamatan Maklumat Dalam Perjanjian Dengan Pembekal	**Tanggungjawab**
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 PLANMalaysia. Pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak PLANMalaysia selaras dengan peraturan dan kawalan keselamatan yang sedang berkuat kuasa. Sekiranya Pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang Pembekal daripada melaksanakan perkhidmatan tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Produk atau perkhidmatan yang ditawarkan oleh Pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; (b) Penilaian teknikal oleh Jawatankuasa Penilaian Teknikal boleh dilaksanakan melalui laporan yang dikemukakan oleh Pembekal; (c) Laporan penilaian Pihak Ketiga yang dikemukakan oleh Pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut: i. Badan penilai Pihak Ketiga adalah bebas dan berintegriti; ii. Badan penilai Pihak Ketiga adalah kompeten; iii. Kriteria penilaian;	Pembekal

iv. Parameter pengujian; dan v. Andaian yang dibuat berkaitan dengan skop penilaian. (d) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan PLANMalaysia; dan (e) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh PLANMalaysia.	

0120 Pengurusan Keselamatan Maklumat Dalam Rantaian Bekalan Teknologi Maklumat Dan Komunikasi	
Objektif: Mengekalkan tahap persetujuan bagi keselamatan maklumat dalam hubungan pembekal.	
012101 Rantaian Bekalan Teknologi Maklumat dan Komunikasi	**Tanggungjawab**
Perjanjian dengan pembekal utama hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; (b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan (c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	Pemilik Sistem, PICT dan Pembekal

0121 Pengurusan Pemantauan, Kajian Semula Dan Perubahan Perkhidmatan Pembekal	
Objektif: Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan penyampaian perkhidmatan adalah sama seperti perjanjian pembekal.	
012101 Memantau dan Mengkaji Semula Perkhidmatan Pembekal	**Tanggungjawab**
PLANMalaysia hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu dipatuhi adalah seperti 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 insiden keselamatan siber kepada pembekal oleh pemilik sistem seperti yang dikehendaki dalam perjanjian bagi penyelesaian insiden.	Pemilik Sistem, PICT dan Pembekal
012102 Pengurusan Perubahan Perkhidmatan Pembekal	**Tanggungjawab**
Perubahan kepada peruntukan perkhidmatan oleh Pembekal yang disebabkan oleh perubahan pada DKS PLANMalaysia, prosedur dan kawalan, hendaklah diuruskan dengan mengambil kira kepentingan data dan maklumat, sistem penyampaian dan proses perkhidmatan yang terlibat dan risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan dalam perjanjian dengan Pembekal; (b) Perubahan yang dilakukan oleh PLANMalaysia bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan (c) Perubahan dalam perkhidmatan Pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran Pembekal dan subkontraktor.	Pemilik Sistem, PICT dan Pembekal

0122 Perkhidmatan Awan (Cloud Services)	
Objektif: Memastikan keselamatan dan kawalan maklumat bagi perolehan, penggunaan, pengurusan dan penamatan/pelucutan daripada perkhidmatan awan yang bergantung kepada sumber pengkomputeran seperti pelayan, storan, pangkalan data, rangkaian dan perisian yang boleh dicapai menerusi internet.	
012201 Kawalan Keselamatan Pengkomputeran Awan	**Tanggungjawab**
Penggunaan aplikasi dan kemudahan infrastruktur pengkomputeran awan (*cloud computing*) dibenarkan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa.	Pentadbir Pusat Data
012202 Penstoran Awan (*Cloud Storage*)	**Tanggungjawab**
Maklumat yang terlibat dalam transaksi dalam pengkomputeran awan perlu dilindungi daripada aktiviti penipuan dan pendedahan serta pengubahsuaian yang tidak dibenarkan. Penstoran awan ini tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa.	Pentadbir Pusat Data

0123 Perancangan Dan Persediaan Pengurusan Insiden Keselamatan Maklumat	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan siber.	
012301 Tanggungjawab Dan Prosedur	**Tanggungjawab**
Sebarang insiden keselamatan siber hendaklah dikawal dengan menggunakan **Prosedur Pengurusan Insiden Keselamatan Siber** yang telah ditetapkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan (sekiranya perlu); dan (d) Melapor kepada NACSA apabila berlaku sebarang insiden keselamatan siber (sekiranya perlu).	ICTSO dan CSIRT PLANMalaysia

0124 Penilaian Dan Keputusan Dalam Kejadian Keselamatan Maklumat	
Objektif: Memastikan kategori dan keutamaan yang efektif dalam kejadian keselamatan maklumat.	
012401 Penilaian Dan Keputusan Dalam Kejadian Keselamatan Maklumat	**Tanggungjawab**
(a) Kejadian keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai kejadian keselamatan maklumat; dan (b) Penilaian dan keputusan dalam kejadian keselamatan maklumat merujuk kepada **Prosedur Pengurusan Insiden Keselamatan Siber.**	ICTSO dan CSIRT PLANMalaysia

0125 Tindak Balas Terhadap Insiden Keselamatan Maklumat	
Objektif: Memastikan tindak balas yang efisien dan efektif kepada insiden keselamatan maklumat.	
012501 Tindak Balas Terhadap Insiden Keselamatan Maklumat	**Tanggungjawab**
Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan **Prosedur Pengurusan Insiden Keselamatan Siber.**	ICTSO dan CSIRT PLANMalaysia

0126 Pembelajaran Insiden Keselamatan Maklumat	
Objektif: Mengurangkan kebarangkalian atau kesan daripada insiden akan datang.	
012601 Pembelajaran Insiden Keselamatan Maklumat	**Tanggungjawab**
(a) Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya; dan (b) 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

0127 Pengumpulan Bahan Bukti	
Objektif: Memastikan pengurusan bukti yang konsisten dan efektif berkaitan dengan insiden keselamatan maklumat bagi tujuan tindakan disiplin dan undang-undang.	
012701 Pengumpulan Bahan Bukti	**Tanggungjawab**
PLANMalaysia hendaklah menentukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.	CSIRT PLANMalaysia

0128 Kesinambungan Keselamatan Maklumat	
Objektif: Melindungi keselamatan maklumat dan aset ICT ketika berlakunya gangguan.	
012801 Perancangan Kesinambungan Keselamatan Maklumat	**Tanggungjawab**
Pelan Pengurusan Kesinambungan Perkhidmatan (PKP) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi memastikan kesinambungan perkhidmatan PLANMalaysia. Pelan PKP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai pegawai PLANMalaysia dan Pembekal berserta nombor yang boleh dihubungi (contoh: faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel yang tidak dapat hadir untuk menangani insiden; (c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan (e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses perniagaan, impak gangguan yang mungkin berlaku dan kesannya terhadap keselamatan siber serta tindakan bagi meminimumkan impak gangguan tersebut; (b) Melaksanakan prosedur tindak balas kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin	Koordinator PKP PLANMalaysia, Pembekal dan Pengguna

atau dalam jangka masa yang telah ditetapkan; (c) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (d) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (e) Membuat *backup* mengikut keperluan DRP; (f) Salinan pelan PKP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama; (g) Pelan PKP hendaklah diuji sekurang-kurangnya setahun sekali atau apabila terdapat perubahan dalam persekitaran atau fungsi utama untuk memastikan ia sentiasa kekal berkesan; (h) Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan PKP bersesuaian dan memenuhi tujuan dibangunkan; dan (i) Ujian pelan PKP hendaklah dijadualkan untuk memastikan semua yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.	

0129 Persediaan ICT Untuk Kesinambungan Perkhidmatan	
Objektif: Memastikan maklumat dan aset ICT PLANMalaysia tersedia apabila berlaku gangguan.	
012901 Mengkaji Semula Dan Menilai Kesinambungan Keselamatan Maklumat	**Tanggungjawab**
PKP termasuk Pelan Pemulihan Bencana (DRP) hendaklah diuji sekurang-kurangnya sekali setahun untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian ini hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan pegawai yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. PLANMalaysia hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan bagi memastikan kawalan tersebut sah dan berkesan semasa situasi kecemasan.	Pasukan DRT

0130 Keperluan Undang-Undang, Peraturan Dan Kontrak	
Objektif: Memastikan pematuhan kepada keperluan undang-undang, peraturan dan kontrak yang berkaitan dengan keselamatan maklumat.	
013001 Pematuhan Dasar	**Tanggungjawab**
Pematuhan DKS PLANMalaysia adalah diwajibkan kepada semua Pengguna, Pembekal dan Pihak Ketiga. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap Pengguna hendaklah membaca, memahami dan mematuhi DKS PLANMalaysia serta undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa; (b) Semua aset ICT PLANMalaysia termasuk data dan maklumat yang disimpan di dalamnya adalah hak milik Kerajaan; (c) ICTSO PLANMalaysia berhak untuk memantau aktiviti Pengguna untuk mengesan penggunaan selain daripada tujuan yang telah ditetapkan; dan (d) Sebarang penggunaan aset ICT PLANMalaysia selain daripada maksud dan tujuan yang telah ditetapkan adalah merupakan satu penyalahgunaan sumber PLANMalaysia.	Pengguna, Pembekal dan Pihak Ketiga
013002 Keperluan Perundangan	**Tanggungjawab**
Senarai perundangan dan peraturan yang perlu dipatuhi oleh pengguna aset ICT PLANMalaysia adalah seperti **LAMPIRAN 4.** Pengguna, Pembekal dan Pihak Ketiga juga perlu mematuhi perundangan dan peraturan semasa yang sedang berkuat kuasa.	Pengguna, Pembekal dan Pihak Ketiga

0131 Hak Harta Intelek	
Objektif: Memastikan pematuhan kepada keperluan undang-undang, peraturan dan kontrak yang berkaitan dengan Hak Harta intelek dan pengunaan Hak Milik produk.	
013101 Kawalan Hak Harta Intelek	**Tanggungjawab**
Prosedur-prosedur yang sesuai akan dilaksanakan untuk memastikan keselarasan dengan perundangan, peraturan dan juga keperluan kontrak yang berkaitan dengan *Intellectual Property Right* (IPR) dan juga pelesenan perisian. PLANMalaysia akan mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat.	Bahagian Korporat

0132 Perlindungan Rekod

Objektif:

Melindungi maklumat PLANMalaysia daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian, pencerobohan, kemalangan atau kecurian.

013201 Kawalan Perlindungan Rekod	Tanggungjawab
Dokumen mengandungi Maklumat Rasmi atau Maklumat Terperingkat hedaklah didaftar, dikelas (dikelaskan sebagai Rahsia Besar, Rahsia, Sulit atau Terhad), dikelas semula dan dilupus dengan mematuhi peraturan yang sedang berkuat kuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen (termasuk pergerakan ke luar dari premis PLANMalaysia) hendaklah dikawal dan direkodkan serta perlu mengikut prosedur keselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan Kerajaan yang sedang berkuatkuasa; (d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa; dan (e) Penyimpanan maklumat rasmi di storan dalam talian diluar kawalan PLANMalaysia adalah tidak dibenarkan.	Pegawai Pengelas dan Seksyen Pentadbiran

0133 Privasi Dan Perlindungan Maklumat Pengecaman Individu (PII)	
Objektif: Memastikan pematuhan kepada keperluan undang-undang, peraturan dan kontrak berkaitan aspek keselamatan maklumat dalam perlindungan maklumat pengecaman individu (PII).	
013301 Privasi dan Perlindungan Maklumat Peribadi	**Tanggungjawab**
PLANMalaysia hendaklah mengenal pasti privasi dan perlindungan maklumat peribadi pengguna dijamin seperti yang tertakluk dalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkenaan.	Pengguna

0134 Kajian Semula Keselamatan Maklumat	
Objektif: Memastikan kesesuaian, kecekapan dan keberkesanan yang berterusan dalam pendekatan PLANMalaysia untuk menguruskan keselamatan maklumat.	
013401 Keperluan Kajian Semula Keselamatan Maklumat	**Tanggungjawab**
Penilaian keselamatan yang dilaksanakan oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	ICTSO

0135 Pematuhan Kepada Polisi, Peraturan Dan Piawaian Keselamatan Maklumat	
Objektif: Memastikan keselamatan maklumat yang dilaksanakan dan beroperasi sesuai dengan polisi keselamatan, polisi tajuk khusus, peraturan dan piawaian yang dikaji semula secara berkala.	
013501 Pematuhan Polisi Dan Piawaian Keselamatan Maklumat	**Tanggungjawab**
PLANMalaysia 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.	Pengguna

0136 Mendokumenkan Prosedur Operasi	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
013601 Keperluan Mendokumenkan Prosedur Operasi	**Tanggungjawab**
Prosedur adalah dasar yang mengatur pengoperasian sistem maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan 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; dan (c) Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	ICTSO, PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia

BIDANG 02: KAWALAN MANUSIA

0201 Saringan

Objektif:

Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan PLANMalaysia, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

020101 Saringan	Tanggungjawab
Memastikan semua Pengguna, Pembekal dan Pihak Ketiga yang berkepentingan memahami tanggungjawab masing- masing ke atas keselamatan aset ICT **sebelum perkhidmatan** agar meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab dalam menjamin keselamatan aset ICT secara bertulis sebelum perkhidmatan; (b) Menjalani tapisan keselamatan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; (c) Pengguna perlu mengisi secara dalam talian Akuan Pematuhan DKS PLANMalaysia; (d) Pengguna perlu menandatangani Perakuan Akta Rahsia Rasmi 1972; (e) Pembekal dan Pihak Ketiga perlu menandatangani Surat Akuan Pematuhan DKS PLANMalaysia seperti **LAMPIRAN 1**; (f) Pembekal dan Pihak Ketiga perlu menandatangani Perakuan Akta Rahsia Rasmi 1972; dan (g) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Pengguna, Pembekal dan Pihak Ketiga

0202 Terma Dan Syarat Perkhidmatan

Objektif:

Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

020201 Terma Dan Syarat Perkhidmatan	Tanggungjawab
Warga PLANMalaysia hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut: (a) Menjalankan tapisan keselamatan untuk warga PLANMalaysia yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; (b) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan: i. Warga PLANMalaysia perlu mengisi surat Akuan Pematuhan DKS PLANMalaysia; dan ii. Warga PLANMalaysia perlu menandatangani surat Perakuan Akta Rahsia Rasmi 1972.	Pengarah Bahagian Khidmat Pengurusan
020202 Dalam Perkhidmatan	**Tanggungjawab**
Memastikan semua Pengguna, Pembekal dan Pihak Ketiga yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT **dalam perkhidmatan** agar meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna perlu menyatakan dengan lengkap dan jelas peranan dan tanggungjawab dalam menjamin keselamatan	Pengguna, Pembekal dan Pihak Ketiga

aset ICT secara bertulis semasa perkhidmatan; (b) Pengguna, Pembekal dan Pihak Ketiga perlu memastikan keselamatan aset ICT diurus berdasarkan prosedur dan peraturan yang ditetapkan oleh PLANMalaysia; (c) Pengguna perlu memastikan program kesedaran yang berkaitan mengenai pengurusan keselamatan aset ICT dihadiri secara berterusan dan berusaha meningkatkan kemahiran keselamatan siber; (d) Pengguna, Pembekal dan Pihak Ketiga perlu memastikan sentiasa mempunyai kesedaran berkenaan kepentingan menjaga rahsia Kerajaan dalam urusan kerja harian; (e) Pengguna perlu mengambil maklum mengenai tindakan disiplin dan/atau undang-undang yang akan dikenakan sekiranya berlaku perlanggaran dengan prosedur dan peraturan ditetapkan oleh PLANMalaysia; dan (f) Pengguna perlu memantapkan pengetahuan berkaitan dengan penggunaan aset ICT melalui medium kursus, latihan teknikal dan medium yang bersesuaian bagi memastikan setiap kemudahan ICT digunakan dengan tujuan dan cara yang betul demi menjamin kepentingan keselamatan siber.	

0203 Kesedaran, Pendidikan Dan Latihan Keselamatan Maklumat	
Objektif: Memastikan kakitangan dan pihak yang berkepentingan sedar dan memenuhi tanggungjawab keselamatan maklumat.	
020301 Kesedaran, Pendidikan Dan Latihan Keselamatan Maklumat	**Tanggungjawab**
Pengguna perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan kesedaran, pendidikan dan latihan yang berkaitan DKS PLANMalaysia, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; dan (b) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	Pengarah Bahagian

0204 Proses Tatatertib	
Objektif: Memastikan kakitangan dan pihak yang berkepentingan faham ke atas kesan perlanggaran polisi keselamatan, menghalang serta berurusan dengan kakitangan dan pihak yang berkepentingan yang terlibat dengan perlanggaran.	
020401 Proses Tatatertib	**Tanggungjawab**
Proses tatatertib yang formal dan disampaikan kepada warga PLANMalaysia hendaklah tersedia bagi membolehkan tindakan diambil terhadap warga PLANMalaysia yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga PLANMalaysia sekiranya berlaku perlanggaran terhadap perundangan dan peraturan yang ditetapkan oleh PLANMalaysia; dan (d) Warga PLANMalaysia yang melanggar dasar ini akan dikenakan tindakan tatatertib di bawah akta yang sedang berkuatkuasa.	Unit Integriti

0205 Tanggungjawab Selepas Pertukaran Atau Penamatan Perkhidmatan	
Objektif: Melindungi pihak berkepentingan PLANMalaysia sebagai sebahagian proses pertukaran atau penamatan kakitangan atau kontrak.	
020501 Penamatan atau Pertukaran Tanggungjawab Perkhidmatan	**Tanggungjawab**
Memastikan semua Pengguna, Pembekal dan Pihak Ketiga yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT sebelum **bertukar atau tamat perkhidmatan** agar meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna perlu menyatakan dengan lengkap dan jelas peranan dan tanggungjawab dalam menjamin keselamatan aset ICT secara bertulis selepas perkhidmatan; (b) Pengguna perlu memastikan semua aset ICT dikembalikan kepada PLANMalaysia mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (c) Pengguna, Pembekal dan Pihak Ketiga perlu memastikan kebenaran capaian ke atas maklumat dan kemudahan proses maklumat dibatalkan atau ditarik balik dengan serta-merta mengikut peraturan yang ditetapkan oleh PLANMalaysia; (d) Pengguna, Pembekal dan Pihak Ketiga perlu melaksanakan perakuan bagi melupuskan semua maklumat terperingkat dalam simpanan secara selamat; dan (e) Menandatangani Borang Pengesahan Pegawai Bertukar Keluar Atau Tamat Perkhidmatan Di PLANMalaysia seperti **LAMPIRAN 2**.	Pengarah Bahagian, Pengguna, Pembekal dan Pihak Ketiga

0206 Perjanjian Kerahsiaan Maklumat	
Objektif: Mengekalkan kerahsiaan maklumat yang boleh dicapai oleh kakitangan dan pihak luaran/ketiga.	
020601 Perjanjian Kerahsiaan atau Ketakdedahan	**Tanggungjawab**
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan PLANMalaysia dan hendaklah disemak dan didokumentasikan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan Kerajaan yang sedang berkuatkuasa. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan; dan (b) Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.	PICT, ICTSO, Pentadbir Sistem ICT PLANMalaysia, Pembekal dan Pengguna

0207 Telekerja

Objektif:

Memastikan keselamatan maklumat bagi kakitangan yang bekerja jarak jauh.

020701 Telekerja	Tanggungjawab
Kawalan Kemudahan Kerja Jarak Jauh adalah bagi memastikan tiada berlakunya kehilangan peralatan, pendedahan maklumat dan capaian tidak sah dan salah guna kemudahan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil untuk melindungi dari risiko penyalahgunaan peralatan mudah alih dan kemudahan komunikasi; (b) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; dan (c) Untuk capaian dari luar rangkaian PLANMalaysia ke rangkaian MyGov*Net dengan menggunakan *Virtual Private Network* (VPN) perlu melalui permohonan kepada STM.	Pengguna
020702 Keperluan dan Kawalan Penggunaan BYOD	**Tanggungjawab**
Penggunaan BYOD yang disambungkan kepada rangkaian PLANMalaysia sama ada menyimpan atau mengakses data rasmi Kerajaan adalah tertakluk kepada keperluan dan kawalan penggunaan BYOD. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna perlu mengetahui risiko dan kesan penggunaan BYOD terhadap keselamatan maklumat; (b) Pengguna perlu mengetahui peraturan-peraturan yang telah ditetapkan apabila menggunakan BYOD; (c) Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD;	Pengguna

(d) Pendaftaran ke atas peralatan mudah alih; (e) Keperluan ke atas perlindungan secara fizikal; (f) Kawalan ke atas pemasangan perisian peralatan mudah alih; (g) Kawalan ke atas versi dan *patches* perisian; (h) Sekatan ke atas akses perkhidmatan maklumat secara dalam talian; (i) Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptograf; dan (j) Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.	

0208 Pelaporan Kejadian Keselamatan Maklumat	
Objektif: Menyokong pelaporan bagi kejadian keselamatan maklumat yang boleh dikenalpasti oleh kakitangan tepat pada masanya, konsisten dan berkesan.	
020801 Pelaporan Kejadian Keselamatan Maklumat	**Tanggungjawab**
Insiden keselamatan siber hendaklah dilaporkan kepada ICTSO dan CSIRT KPKT dengan kadar segera. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Melaporkan insiden keselamatan siber apabila: i. Maklumat disyaki/didapati hilang atau terdedah kepada pihak-pihak yang tidak diberi kuasa; ii. Sistem komputer disyaki atau digunakan tanpa kebenaran; iii. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; iv. Berlaku kejadian yang luar biasa kepada sistem komputer seperti kehilangan fail, sistem komputer kerap kali gagal dan komunikasi tersalah hantar; dan v. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden keselamatan maklumat yang tidak dijangka. (b) Ringkasan bagi semua proses kerja yang terlibat dalam Pelaporan Insiden Keselamatan Siber di PLANMalaysia seperti **LAMPIRAN 3**.	Pemilik Sistem, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia dan Pengguna

BIDANG 03: KAWALAN FIZIKAL

0301 Perimeter Keselamatan Fizikal

Objektif:

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

030101 Perimeter Keselamatan Fizikal	Tanggungjawab
Kawalan Kawasan bertujuan menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan dan lain-lain) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (c) Melindungi kawasan terhad melalui kawalan-kawalan tertentu seperti memasang alat penggera, kamera litar tertutup atau EMS sekiranya berkaitan; (d) Mengehadkan jalan keluar masuk; (e) Mengadakan kaunter kawalan; (f) Menyediakan ruang menunggu atau ruang kerja untuk Pihak Ketiga (jika perlu); (g) Mewujudkan perkhidmatan kawalan keselamatan; (h) Melindungi kawasan terperingkat melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;	Seksyen Pentadbiran

(i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam ruang dan bilik pejabat serta kemudahan yang disediakan; (j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; (k) Menyediakan garis panduan untuk warga yang bekerja di dalam kawasan terperingkat; dan (l) Memastikan kawasan-kawasan penghantaran dan pemunggahan serta tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya.	

0302 Laluan Masuk Fizikal	
Objektif: Memastikan penggunaan laluan masuk fizikal kepada maklumat dan aset ICT PLANMalaysia yang disahkan sahaja.	
030201 Kawalan Kemasukan Fizikal	**Tanggungjawab**
Kawalan masuk fizikal bertujuan mengawal akses oleh pihak-pihak Pengguna, Pembekal dan Pihak Ketiga bagi keselamatan maklumat organisasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pas keselamatan hendaklah dipakai sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan semula kepada PLANMalaysia apabila Pengguna berhenti, bersara atau berpindah keluar; (c) Pihak Ketiga hendaklah menyerahkan semula pas pelawat kepada PLANMalaysia apabila urusan selesai atau tamat kontrak; (d) Pas pelawat hendaklah diambil di kaunter masuk. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (e) Kehilangan pas keselamatan/pelawat mestilah dilaporkan dengan segera kepada pihak berkuasa yang berkaitan mengikut prosedur yang telah ditetapkan.	PK PLANMalaysia Pengguna, Pembekal dan Pihak Ketiga
030203 Kawasan Larangan	**Tanggungjawab**
Kawasan Larangan dilaksanakan untuk melindungi aset ICT. Kawasan larangan ICT di PLANMalaysia adalah Pusat Data/Bilik Server/Bilik Fail. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Akses kepada kawasan terperingkat hanyalah kepada pegawai-pegawai yang dibenarkan sahaja. (b) Buku log keluar/masuk Pusat Data sentiasa dipantau dan	Seksyen Pentadbiran, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia, Pembekal dan Pihak Ketiga

diselenggara; (c) Pihak Ketiga dilarang sama sekali untuk memasuki kawasan terperingkat kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal; (d) Pihak Ketiga hendaklah diiringi dan dipantau sepanjang masa oleh pegawai yang diberi kebenaran untuk mengakses Pusat Data sehingga tugas di kawasan berkenaan selesai. Pihak Ketiga juga perlu mematuhi semua peraturan Pusat Data yang ditetapkan; dan (e) Peralatan rakaman/penyimpanan seperti kamera, video, perakam suara dan storan mudah alih adalah tidak dibenarkan dibawa masuk ke dalam Kawasan Terperingkat kecuali dengan kebenaran Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT.	

0303 Keselamatan Pejabat, Bilik dan Kemudahan	
Objektif: Mencegah dari akses fizikal yang tidak sah, kerosakan dan gangguan terhadap maklumat dan aset ICT PLANMalaysia di pejabat, bilik dan kemudahan.	
030301 Keselamatan Pejabat, Bilik dan Kemudahan	**Tanggungjawab**
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawasan tempat kerja, bilik mesyuarat, bilik perbincangan, bilik fail, bilik kawalan Closed-Circuit Televsion (CCTV) dan pusat data perlu dihadkan daripada diakses tanpa kebenaran; (b) Kawasan tempat kerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh pihak luar; dan (c) Fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk ke dalam kawasan larangan KECUALI pegawai yang telah dipertanggungjawabkan.	Pengguna, Pembekal dan Pihak Ketiga

0304 Pemantauan Keselamatan Fizikal	
Objektif: Mengesan dan menghalang akses fizikal yang tidak sah.	
030401 Kawalan Pemantauan Keselamatan Fizikal	**Tanggungjawab**
Premis fizikal perlu dipantau menggunakan sistem pengawasan (contoh: pengawal, penggera pencerobohan, sistem pemantauan video seperti CCTV, sistem aplikasi pengurusan maklumat keselamatan fizikal atau mana-mana yang bersesuaian). Akses ke lokasi kritikal perlu dipantau secara berterusan bagi mengesan akses yang tidak sah atau tingkah laku yang mencurigakan.	Seksyen Pentadbiran

0305 Perlindungan Daripada Ancaman Fizikal Dan Persekitaran	
Objektif: Mencegah atau mengurangkan kesan dari kejadian yang berpunca dari ancaman fizikal dan persekitaran.	
030501 Perlindungan Daripada Ancaman Fizikal Dan Persekitaran	**Tanggungjawab**
Kawalan persekitaran bertujuan menghindar kerosakan dan capaian terhadap peralatan ICT dan peralatan rangkaian bagi keselamatan maklumat agensi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan susun atur semua aset ICT di Pusat Data adalah teratur dan kemas; (b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan peralatan perlindungan keselamatan yang bersesuaian dan dibenarkan seperti alat pengesan kebakaran, alat pencegah kebakaran dan pintu kecemasan; (c) Semua bahan mudah terbakar, cecair, bahan atau peralatan lain yang boleh merosakkan peralatan ICT hendaklah diletakkan di tempat yang bersesuaian dan berjauhan daripada aset ICT; (d) Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran aset ICT; (e) Memastikan akses kepada saluran riser sentiasa dikunci; (f) Memastikan peralatan rangkaian seperti *switch*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; (g) Memastikan pegawai yang bertanggungjawab menyimpan semua kunci yang berkenaan dapat dihubungi apabila keadaan memerlukan berbuat demikian; (h) Insiden kecemasan persekitaran mesti dilaporkan; dan (i) Merancang dan menyertai latihan kecemasan bencana yang diadakan di PLANMalaysia.	Seksyen Pentadbiran, ICTSO, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMAlaysia dan Pengguna

0306 Bekerja Di Kawasan Selamat	
Objektif: Mencegah maklumat dan aset ICT di dalam kawasan yang selamat dari kerosakan dan gangguan oleh kakitangan yang tidak sah yang bekerja di kawasan tersebut.	
030601 Bekerja Di Kawasan Selamat	**Tanggungjawab**
Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam; dan Kawalan keselamatan ke atas kawasan tersebut adalah seperti berikut: (a) Pangkalan data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; (b) Peralatan keselamatan (CCTV) perlu diperiksa secara berjadual; (c) Butiran pelawat yang keluar masuk ke kawasan terperingkat perlu direkodkan; (d) Pelawat yang dibawa masuk mesti diiringi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; (e) Lokasi pusat data hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air danlaluan awam; dan (f) Memastikan keselamatan bangunan mengikut piawaian yang telah ditetapkan.	Seksyen Pentadbiran dan Seksyen Teknologi Maklumat

0307 *Clear Desk* dan *Clear Screen*	
Objektif: Mengurangkan risiko capaian tidak sah, kehilangan dan kerosakan kepada maklumat di meja, skrin dan mana-mana lokasi yang boleh dimasuki sewaktu dan selepas waktu bekerja.	
030701 Polisi Meja Kosong (Clear Desk) dan Skrin Kosong (Clear Screen)	**Tanggungjawab**
Clear Desk dan *Clear Screen* merupakan amalan yang digalakkan bagi menjaga keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau *log out* apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera daripada pencetak dan mesin fotostat.	Pengguna

0308 Penempatan Dan Perlindungan Peralatan

Objektif:

Melindungi peralatan ICT PLANMalaysia daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

030801 Penempatan Dan Perlindungan Peralatan ICT	Tanggungjawab
Pengguna yang diberikan peralatan ICT hendaklah menjaga dan bertanggungjawab sepenuhnya ke atas peralatan ICT tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (b) Melaporkan sebarang kerosakan peralatan ICT melalui saluran yang ditetapkan; (c) Bertanggungjawab sepenuhnya ke atas peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran dan perubahan konfigurasi yang telah ditetapkan; (d) Dilarang sama sekali menambah, mengganti atau mengeluarkan sebarang perkakasan ICT yang telah ditetapkan; (e) Dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran; (f) Bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (g) Memastikan perisian antivirus yang dibekalkan di komputer peribadi/komputer riba sentiasa aktif (*active*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan. Pengguna dilarang untuk menyahpasang (*uninstall*) antivirus yang telah dipasang (*installed*); (h) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (i) Semua peralatan sokongan ICT (aksesori) hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan	Pegawai Aset, PICT, Seksyen Teknologi Maklumat dan Pengguna

atau pengubahsuaian tanpa kebenaran; (j) Peralatan-peralatan kritikal perlu disokong oleh UPS; (k) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; (l) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; (m) Peralatan ICT yang hendak dibawa keluar dari premis PLANMalaysia hendaklah mematuhi peraturan yang telah ditetapkan; (n) Peralatan ICT yang hilang hendaklah dilaporkan kepada PICT dan Pegawai Aset PLANMalaysia dengan segera; (o) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; (p) Pengguna tidak dibenarkan mengalih kedudukan peralatan ICT dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset dan Penyelaras ICT PLANMalaysia. Perpindahan peralatan ICT hendaklah mematuhi peraturan yang telah ditetapkan; (q) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; (r) Bertanggungjawab terhadap peralatan ICT di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (s) Memastikan semua peralatan ICT yang tidak digunakan dalam keadaan tutup (*off*) apabila meninggalkan pejabat; (t) Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat; dan (u) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada PICT.	

0309 Keselamatan Aset Di Luar Premis	
Objektif: Mencegah maklumat dan aset ICT di dalam kawasan yang selamat dari kerosakan dan gangguan oleh kakitangan yang tidak sah yang bekerja di kawasan tersebut.	
030901 Keselamatan Peralatan dan Aset di Luar Premis	**Tanggungjawab**
Peralatan ICT yang dibawa keluar dari premis PLANMalaysia adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan ICT termasuk perisian dan maklumat perlu dilindungi dan dikawal sepanjang masa; (b) Penyimpanan atau penempatan peralatan ICT mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (c) Kehilangan peralatan ICT perlu dilaporkan mengikut prosedur pengurusan aset yang ditetapkan.	Pengguna, Pembekal dan Pihak Ketiga

0310 Media Storan	
Objektif: Memastikan pendedahan, pengubahsuaian, penghapusan dan pemusnahan yang sah pada media storan.	
031001 Pengurusan Media Boleh Alih	**Tanggungjawab**
Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh PLANMalaysia. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Mengehadkan dan menentukan capaian media kepada Pengguna yang dibenarkan sahaja; (c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Menyimpan semua media di tempat yang selamat; (f) Media yang mengandungi maklumat terperingkat hendaklah dilupuskan mengikut prosedur yang telah ditetapkan; dan (g) Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pentadbir Peralatan ICT terlebih dahulu.	Pengarah Bahagian
031002 Pemindahan Media Fizikal	**Tanggungjawab**
Senarai syarikat kourier/pemindah yang diluluskan perlu diselenggara dan prosedur pengenalan syarikat kourier/ pemindah perlu diwujudkan. Log identiti bagi maklumat, masa pemindahan dan resit perlu diselenggara yang merupakan sebahagian dari prosedur tersebut.	Pentadbir Pusat Data

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pelupusan media fizikal perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan; dan (b) Media fizikal yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	

0311 Utiliti Sokongan

Objektif:

Mencegah maklumat dan aset ICT dari hilang, rosak dan dikompromi atau gangguan kepada operasi PLANMalaysia akibat dari kegagalan dan gangguan utiliti sokongan.

031101 Kawalan Utiliti Sokongan	Tanggungjawab
Peralatan ICT perlu dilindungi daripada kegagalan bekalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan; (b) Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan (c) Semua peralatan sokongan bekalan kuasa hendaklah diperiksa, diuji dan diselenggara dari semasa ke semasa (sekurang-kurangnya setahun sekali).	Seksyen Pentadbiran

0312 Keselamatan Kabel	
Objektif: Mencegah maklumat dan aset ICT dari hilang, rosak dan dikompromi atau gangguan kepada operasi PLANMalaysia berkaitan dengan punca kuasa dan kabel komunikasi.	
031201 Keselamatan Kabel	**Tanggungjawab**
Kabel peralatan ICT hendaklah dilindungi kerana ia boleh menyebabkan maklumat terdedah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia dan Pembekal

0313 Penyelenggaraan Peralatan	
Objektif: Mencegah maklumat dan aset ICT dari hilang, rosak dan dikompromi atau gangguan kepada operasi PLANMalaysia berpunca dari kekurangan penyelenggaran.	
031301 Penyelenggaraan Peralatan	**Tanggungjawab**
Semua peralatan ICT dan sokongan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan ICT dan sokongan yang diselenggara hendaklah mengikut spesifikasi yang telah ditetapkan; (b) Memastikan peralatan hanya boleh diselenggara oleh Seksyen Pentadbiran, Seksyen Teknologi Maklumat atau Pembekal yang dibenarkan sahaja; (c) Penyelenggaraan melibatkan perkakasan ICT dan sokongan dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua peralatan ICT dan sokongan sebelum dan selepas proses penyelenggaraan; dan (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Seksyen Pentadbiran, Seksyen Teknologi Maklumat dan Pembekal

0314 Pelupusan Yang Selamat Atau Penggunaan Semula Peralatan ICT dan Sokongan

Objektif:

Mencegah ketirisan maklumat dari peralatan yang mengandungi media storan yang perlu dilupuskan atau diguna semula.

031401 Pelupusan Yang Selamat Atau Penggunaan Semula Peralatan ICT dan Sokongan	Tanggungjawab
Pelupusan melibatkan peralatan ICT dan sokongan yang telah rosak, usang dan tidak boleh dibaiki. Peralatan ICT dan sokongan yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan ICT dan sokongan yang hendak dilupuskan perlulah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (b) Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT dan sokongan; (c) Pelupusan peralatan ICT dan sokongan hendaklah dilakukan secara berpusat dan mengikut prosedur pelupusan semasa yang berkuat kuasa; dan (d) Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan. Contoh: CPU, RAM, *hardisk, motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan; dan iii. Memindah keluar dari lokasi mana-mana peralatan ICT yang hendak dilupuskan.	Pegawai Aset PLANMalaysia dan Pengguna

BIDANG 04: KAWALAN TEKNOLOGI

0401 Peralatan Pengguna

Objektif:

Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.

040101 Peralatan Mudah Alih	Tanggungjawab
Peralatan mudah alih yang boleh mengumpul, merakam, menyiar dan menyampaikan maklumat dalam apa jua bentuk rekod elektronik perlu diberi kawalan perlindungan bagi memastikan keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua Pengguna bertanggungjawab sepenuhnya terhadap pengurusan dan kawalan keselamatan setiap peralatan mudah alih yang dibekalkan; (b) Rekod penggunaan peralatan mudah alih hendaklah diwujudkan, dikemaskini dan diperiksa; (c) Memastikan peralatan mudah alih dihindari daripada sebarang ancaman, keselamatan maklumat seperti pendedahan, kecurian, pengubahsuaian dan pemalsuan; (d) Peralatan mudah alih tidak disimpan di dalam kenderaan tanpa pengawasan, di tempat-tempat awam dan premis/ kawasan yang tidak selamat; dan (e) Peralatan mudah alih yang didapati hilang hendaklah diuruskan berdasarkan kepada pekeliling/proses semasa yang berkuatkuasa.	Pegawai Aset PLANMalaysia, Penyelaras ICT dan Pengguna

0402 Hak Capaian Istimewa

Objektif:

Memastikan pengguna, komponen perisian dan perkhidmatan yang sah sahaja diberi hak capaian istimewa.

040201 Pengurusan Hak Akses Istimewa	Tanggungjawab
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 Pendaftaran dan Penamatan Pengguna.	Pemilik Sistem, Pentadbir Sistem ICT, Pentadbir Pusat Data Rangkaian dan Komunikasi ICT PLANMalaysia dan Pengguna

0403 Sekatan Akses Maklumat

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

040301 Sekatan Akses Maklumat	Tanggungjawab
Sistem Pengoperasian membolehkan Kawalan Capaian Sistem Pengoperasian bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian kepada sumber sistem komputer. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan mekanisme log masuk yang terjamin; (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Mengehadkan dan mengawal penggunaan perisian; (d) Mengehadkan tempoh penggunaan dan/atau sambungan ke sesebuah aplikasi berisiko tinggi; (e) Mengesahkan Pengguna yang dibenarkan selaras dengan peraturan PLANMalaysia; dan (f) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian.	Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia dan Pengguna
040302 Capaian/ Akses Sistem Aplikasi dan Maklumat	**Tanggungjawab**
Capaian sistem aplikasi dan maklumat adalah terhad kepada Pengguna dan tujuan yang dibenarkan sahaja. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan sistem aplikasi yang dibenarkan adalah mengikut ketetapan kawalan capaian, tahap capaian dan keselamatan yang telah ditentukan;	Pentadbir Sistem ICT PLANMalaysia dan Pengguna

(b) Memastikan jejak audit dan sistem log dilaksanakan bagi setiap aktiviti capaian sistem aplikasi dan maklumat; (c) Mengehadkan capaian sistem aplikasi dan maklumat kepada lima (5) kali percubaan. Sekiranya gagal, pengguna dan pentadbir sistem perlu menetapkan semula kata laluan; (d) Mengawal capaian ke atas sistem aplikasi dan maklumat menggunakan prosedur log masuk yang selamat, kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; (e) Capaian sistem aplikasi dan maklumat melalui capaian internet adalah dibenarkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; dan (f) Capaian kepada sistem aplikasi di PLANMAlaysia hendaklah mempunyai ciri-ciri keselamatan (contoh penggunaan *Secure Socket Layer* (SSL): https).	

0404 Capaian Kepada Kod Sumber	
Objektif: Memastikan supaya kod sumber dikawal dan dikendalikan dengan baik dan selamat.	
040401 Kawalan Capaian Kepada Kod Sumber Program	**Tanggungjawab**
Fail sistem aplikasi perlu dikawal dan dikendalikan dengan baik dan selamat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT dan mengikut prosedur yang telah ditetapkan; (b) Kod sumber sistem aplikasi yang telah dikemaskini hanya boleh digunakan selepas diuji; (c) Mengawal capaian ke atas kod sumber sistem aplikasi bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan (d) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem, Pentadbir Sistem ICT, Pembekal dan Pihak Ketiga

0405 Pengesahan Rahsia (*Secure Authentication*)	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
040501 Pengesahan Rahsia (*Secure Authentication*)	**Tanggungjawab**
Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti berikut: (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan PLANMalaysia; (b) Mewujudkan kata laluan yang berkualiti; (c) Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin; dan (d) Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna.	Pemilik Sistem

0406 Pengurusan Kapasiti

Objektif:

Memastikan kapasiti yang diperlukan oleh kemudahan pemprosesan maklumat, sumber manusia, pejabat dan kemudahan lain.

040601 Pengurusan Perancangan Kapasiti	Tanggungjawab
Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem aplikasi yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Kapasiti sesuatu komponen atau sistem aplikasi hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan, kegunaan dan operasi sistem aplikasi pada masa akan datang; dan (b) 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.	Pemilik Sistem, ICTSO, PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia

0407 Perisian Berbahaya

Objektif:

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

040701 Perlindungan Dari Perisian Berbahaya	Tanggungjawab
Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan *malware* hendaklah dilaksanakan dan digabungkan dengan kesedaran Pengguna terhadap serangan tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti *antivirus* dan IPS serta memastikan prosedur penggunaan yang betul dan selamat diikuti; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang- undang bertulis yang berkuat kuasa; (c) Mengimbas peralatan ICT dengan antivirus sebelum digunakan; (d) Mengemas kini antivirus dengan paten antivirus yang terkini; (e) Menyemak maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Melaksanakan program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (g) Memasukkan klausa penyelenggaraan pembaikan di dalam kontrak pembekal perisian. Klausa ini bertujuan untuk memastikan perisian terlindung daripada program berbahaya; dan (h) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan *virus*.	Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia dan Pengguna

0408 Kawalan Teknikal Kerentanan (*Vulnerability*)

Objektif:

Memastikan kawalan teknikal kerentanan (vulnerability) adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.

040801 Pengurusan Kerentanan Teknikal	Tanggungjawab
Kawalan daripada ancaman teknikal ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan maklumat ancaman diperolehi daripada sumber yang sahih; (b) Menilai tahap kerentanan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	ICTSO, Pemilik Sistem, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia

0409 Pengurusan Konfigurasi	
Objektif: Memastikan peralatan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul dengan aturan keselamatan yang diperlukan dan konfigurasi tidak diubah oleh perubahan yang tidak sah dan tidak betul.	
040901 Kawalan Pengurusan Konfigurasi	**Tanggungjawab**
Memastikan peralatan, perisian, perkhidmatan dan rangkaian berfungsi dengan baik dengan aturan keselamatan yang diperlukan dan konfigurasi tidak diubah tanpa kelulusan.	ICTSO, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia

0410 Penghapusan Maklumat	
Objektif: Mencegah pendedahan maklumat sensitif yang tidak sewajarnya dan mematuhi undang-undang, peraturan dan keperluan kontrak dalam penghapusan maklumat.	
041001 Kawalan Penghapusan Maklumat	**Tanggungjawab**
Maklumat yang disimpan di dalam sistem informasi, peralatan dan mana-mana storan media perlu dihapuskan apabila tidak diperlukan.	Pemilik Sistem dan Seksyen Teknologi Maklumat

0411 *Data Masking*	
Objektif: Untuk mengehadkan pendedahan data sensitif termasuk maklumat data peribadi (PII), dan mematuhi keperluan undang-undang, peraturan dan kontrak.	
041101 *Data Masking*	**Tanggungjawab**
PLANMalaysia hendaklah memastikan sebarang paparan data sensitif termasuk maklumat data peribadi (contohnya PII) disembunyikan. Teknik-teknik yang boleh digunakan untuk *Data Masking* termasuk, tetapi tidak terhad kepada: (a) *Pseudonymization*; (b) *Anonymization*; (c) Enkripsi (memerlukan pengguna yang diberi kuasa untuk mempunyai kunci); (d) Membatalkan (*nulling*) atau memadamkan aksara (menghalang pengguna yang tidak dibenarkan daripada melihat mesej penuh); (e) Nombor dan tarikh yang berbeza-beza; (f) Penggantian (mengubah satu nilai bagi yang lain untuk menyembunyikan data sensitif); atau (g) Menggantikan nilai dengan fungsi *hash*.	Pemilik Sistem

0412 Pencegahan Kebocoran Data (DLP)

Objektif:

Untuk mengesan dan mencegah pendedahan dan pengekstrakan maklumat yang tidak dibenarkan oleh individu atau sistem.

041201 Kawalan Pencegahan Kebocoran Data	Tanggungjawab
Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.	Pemilik Sistem

0413 Sandaran (*Backup*) Maklumat

Objektif:

Membolehkan salinan maklumat, perisian dan sistem diselenggara dan diuji secara berkala berdasarkan polisi tajuk khusus berkaitan *backup*.

041301 Sandaran (*Backup*) Maklumat	Tanggungjawab
Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di *off site*. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Melaksanakan *backup* keselamatan ke atas semua perisian aplikasi dan sistem aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Melaksanakan *backup* ke atas semua data dan maklumat mengikut keperluan. Kekerapan *backup* bergantung pada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi; (c) *Backup* hendaklah dilakukan di dalam media yang bersesuaian; (d) Menguji secara berkala prosedur dan media *backup* dan *restore* bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila perlu digunakan; (e) Membangun dan melaksana pengurusan generasi *backup* berdasarkan pelan pengurusan risiko bagi setiap aset ICT; (f) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat; dan (g) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan.	Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia

0414 Lewahan (*Redundancy*)	
Objektif: Memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.	
041401 Ketersediaan Kemudahan Pemprosesan Maklumat	**Tanggungjawab**
Kemudahan pemprosesan maklumat PLANMalaysia perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (*fail over test*) keberkesanannya dari semasa ke semasa.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia

0415 Pengelogan (*Logging*)

Objektif:

Merekod kejadian, menjana pembuktian, memastikan integriti maklumat log, mencegah capaian tidak sah, mengenal pasti kejadian keselamatan maklumat yang membawa kepada insiden keselamatan maklumat dan menyokong penyiasatan.

041501 Pengelogan Kejadian	Tanggungjawab
Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem komputer ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian 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. Jenis fail log bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti yang berikut: (a) Fail log sistem pengoperasian; (b) Fail log servis (contoh: web, e-mel); (c) Fail log aplikasi (*audit trail*); dan (d) Fail log rangkaian (contoh: *switch, firewall*, IPS). Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti	ICTSO, PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia

kecurian maklumat dan pencerobohan, aktiviti ini hendaklah dilaporkan kepada ICTSO dan PICT; dan (d) Melaksanakan pemantauan secara berterusan.	

0416 Aktiviti Pemantauan

Objektif:

Mengesan tingkah laku anomali dan potensi kepada insiden keselamatan maklumat.

041601 Pemantauan Berterusan	Tanggungjawab
Pemantauan kepada rangkaian, sistem dan aplikasi perlu dilaksanakan secara berterusan mengikut tempoh yang bersesuaian. Perkara-perkara yang memerlukan pemantauan termasuklah tetapi tidak terhad kepada: (a) Trafik keluar masuk rangkaian, sistem dan aplikasi; (b) Capaian kepada sistem, server dan perkakasan rangkaian yang kritikal dan lain-lain; (c) Tahap pentadbir sistem dan fail konfigurasi rangkaian; (d) Log dari peralatan/perisian keselamatan (contoh: *Antivirus*, IDS, IPS, *firewall* dan lain-lain); (e) Log kejadian berkaitan aktiviti sistem dan rangkaian; (f) Penggunaan kod yang disahkan tidak disalah guna; dan (g) Penggunaan sumber (contoh: CPU, *hard disk*, *memory* dan *bandwidth*).	Pentadbir Sistem dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia

0417 Penyegerakan Jam (*Clock Synchronization*)	
Objektif: Membolehkan korelasi dan analisis kejadian berkaitan keselamatan dan lain-lain data yang direkodkan dan untuk menyokong siasatan kepada insiden keselamatan maklumat.	
041701 Penyegerakan Jam	**Tanggungjawab**
Jam bagi semua sistem 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 PLANMalaysia atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh *National Metrology Institute of Malaysia* (NMIM).	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia dan Seksyen Pentadbiran

0418 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa	
Objektif: Memastikan penggunaan program utiliti tidak mendatangkan mudarat kepada keselamatan maklumat bagi kawalan sistem dan aplikasi.	
041801 Kawalan Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa	**Tanggungjawab**
Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding* sistem.	Pentadbir Sistem dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia

0419 Pemasangan Perisian Pada Sistem Operasi	
Objektif: Memastikan integriti pada sistem operasi dan mengelakkan eksploitasi kepada kerentanan (*vulnerabilities*) teknikal.	
041901 Pemasangan dan Sekatan Perisian Pada Sistem yang Beroperasi	**Tanggungjawab**
Proses pemasangan perisian hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa.	Pentadbir Perisian

0420 Keselamatan Rangkaian

Objektif:

Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.

042001 Kawalan Rangkaian	Tanggungjawab
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman bagi PLANMalaysia. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan rangkaian hendaklah melalui proses *User Acceptance Test* (UAT) semasa pemasangan dan konfigurasi; (e) *Firewall* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT; (f) Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan JDN; (g) Semua trafik keluar dan masuk rangkaian di Pusat Data dan pejabat-pejabat cawangan hendaklah melalui *firewall* di bawah kawalan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT; (h) Digalakkan memasang perisian bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat seperti berikut: i. IPS; dan	PICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT dan Pentadbir Sistem ICT PLANMalaysia

ii. *Web Content Filtering*. (i) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer Pengguna; (j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT adalah tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di PLANMalaysia sahaja dan penggunaan rangkaian luar adalah dengan kelulusan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT; (l) Kemudahan bagi wireless LAN hendaklah dipantau dan dikawal penggunaannya; (m) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan; (n) Menempatkan atau memasang antara muka (interface) yang bersesuaian di antara rangkaian PLANMalaysia, rangkaian agensi lain dan rangkaian awam; (o) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; (p) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian yang dibenarkan sahaja; (q) Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh; (r) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan PLANMalaysia; dan (s) Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap kawalan capaian PLANMalaysia.	

0421 Keselamatan Pada Perkhidmatan Rangkaian	
Objektif: Memastikan keselamatan dalam penggunaan perkhidmatan rangkaian.	
042101 Keselamatan Perkhidmatan Rangkaian	**Tanggungjawab**
Pengurusan bagi semua perkhidmatan rangkaian (*inhouse* atau *outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti. Mekanisme keselamatan dan tahap perkhidmatan hendaklah dimasukkan di dalam perjanjian perkhidmatan rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Komponen keselamatan rangkaian merangkumi perkakasan, perisian dan perkhidmatan perkomputeran awan digunakan bagi memastikan rangkaian selamat dari ancaman, serangan siber, cubaan pengodaman dan kecuaian Pengguna; (b) Sistem Keselamatan Rangkaian menggunakan kombinasi pelbagai komponen keselamatan rangkaian bagi membentuk sistem pertahanan berlapis/ *layered defense system*; dan (c) Setiap lapisan sistem pertahanan membekal keupayaan pemantauan, pengenalan dan pemulihan bagi memastikan rangkaian selamat.	PICT, ICTSO, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT, Pentadbir Sistem ICT PLANMalaysia, Pembekal dan Pihak Ketiga

0422 Pengasingan Dalam Rangkaian

Objektif:

Memisahkan rangkaian dalam sempadan keselamatan dan mengawal trafik di kalangan rangkaian tersebut berdasarkan keperluan perkhidmatan PLANMalaysia.

042201 Pengasingan Dalam Rangkaian	Tanggungjawab
Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian PLANMalaysia. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengenal 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) Mengemaskinikan hak capaian pengguna dari semasa ke semasa mengikut keperluan; dan (e) Operasi rangkaian hendaklah diasingkan untuk meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT dan Pentadbir Sistem ICT PLANMalaysia

0423 Penapisan Web (*Web Filtering*)	
Objektif: Untuk melindungi sistem daripada terjejas oleh perisian hasad dan untuk menghalang akses kepada sumber web yang tidak dibenarkan.	
042301 Kawalan Penapisan Web	**Tanggungjawab**
Memasang *Web Content Filtering* pada *Internet Gateway* atau kawalan capaian Internet yang bersesuaian untuk menyekat aktiviti/capaian laman web yang dilarang.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia

0424 Penggunaan Kriptografi

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

042401 Polisi Penggunaan Kawalan Kriptografi	Tanggungjawab
Kriptografi merangkumi kaedah-kaedah seperti berikut: a) <u>Enkripsi</u> Enkripsi/ penyulitan digunakan untuk melindungi kerahsiaan, integriti dan kesahihan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap maklumat terperingkat hendaklah disulitkan; (b) Untuk mengendalikan Maklumat Rasmi penggunaan Produk Kriptografi Terpercaya adalah digalakkan; dan (c) Kesemua pelaksanaan sistem hendaklah menggunakan ID atau kata laluan dan dibuat enkripsi. b) <u>Tandatangan Digital</u> Penggunaan tandatangan digital adalah mengikut keperluan pelaksanaan dan melibatkan Sijil Digital. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan tandatangan digital adalah dimestikan kepada pengguna yang menguruskan transaksi maklumat rahsia rasmi secara elektronik; dan (b) Sijil Digital yang digunakan hendaklah diperoleh daripada Pihak Berkuasa Pemerakuan Berlesen sahaja.	Pemilik Sistem, Pentadbir Sistem ICT PLANMalaysia dan Pengguna

042402 Pengurusan Kunci Awam	Tanggungjawab
PKI merupakan teknologi berasaskan sijil digital yang dapat membantu organisasi menggunakan tandatangan digital, enkripsi dan pengesahan identiti antara manusia, sistem dan peranti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut; (b) Kunci persendirian mesti disimpan dengan selamat dan hanya digunakan oleh entiti yang memilikinya sahaja bagi tujuan nyahsulit atau mewujudkan tandatangan digital. Kunci awam tersedia bagi ahli kumpulan yang menggunakan enkripsi bagi menentusah tandatangan digital yang diterima; dan (c) Pengurusan sijil digital pelayan *Secure Socket Layer* (SSL) hendaklah dilakukan bagi mengelakkan sebarang capaian, kecurian atau digunakan oleh pihak lain.	Pemilik Sistem dan Pengguna

0425 Keselamatan Kitar Hayat Pembangunan (SDLC)

Objektif:

Memastikan keselamatan maklumat direka bentuk dan dilaksanakan pada kitar hayat pembangunan perisian dan sistem aplikasi.

042501 Prosedur Pembangunan Sistem Aplikasi	Tanggungjawab
Sistem aplikasi membantu Pengguna melaksanakan tugas rasmi harian. Contoh sistem aplikasi adalah sistem aplikasi pengurusan data. Sistem aplikasi juga merujuk kepada sistem aplikasi web dan sistem aplikasi mudah alih. Sistem aplikasi yang selamat perlu dibangunkan meliputi seluruh kitar hayat pembangunan sistem aplikasi berdasarkan Prosedur Pembangunan Sistem Aplikasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Permohonan Pembangunan Sistem Aplikasi secara rasmi hendaklah dikemukakan kepada Urus Setia JPICT PLANMalaysia untuk kelulusan; (b) Permohonan hendaklah lengkap meliputi spesifikasi teknikal, anggaran kos yang terlibat, guna tenaga dan juga skop perluasan sistem aplikasi tersebut; (c) Pembangunan sistem aplikasi hendaklah mengambil kira sistem aplikasi sedia ada di PLANMalaysia bagi mengelakkan pertindihan pembangunan sistem aplikasi yang sama; (d) Pembangunan sistem aplikasi mestilah menggunakan kod-kod piawaian di bawah DDSA dan sumber rujukan daripada Kementerian/Jabatan lain yang berkaitan; (e) Pemilik Sistem aplikasi bertanggungjawab mempromosi dan memastikan kelancaran pelaksanaan sistem; (f) Pemilik Sistem aplikasi hendaklah membaca dan memahami dokumentasi serta mematuhi prosedur yang berkaitan; (g) Pemilik Sistem aplikasi perlu melaporkan kepada JPICT PLANMalaysia secara berkala bagi kemajuan pelaksanaan sistem aplikasi; (h) Pembangunan sistem aplikasi hendaklah menggunakan teknik	Pemilik Sistem dan Pentadbir Sistem ICT PLANMalaysia

pengaturcaraan dan pangkalan data yang selamat; (i) Sistem aplikasi PLANMalaysia boleh didemonstrasi atau diagihkan kepada Kementerian/Jabatan lain dengan kebenaran PICT; (j) Kod sumber sistem aplikasi hendaklah disimpan dengan teratur dan sebarang pindaan hendaklah direkodkan bagi tujuan kawalan versi; (k) Proses perolehan pembangunan sistem aplikasi secara outsource perlu dilakukan melalui prosedur perolehan yang sedang berkuatkuasa bagi mendapatkan perkhidmatan pembekal yang terbaik dan berwibawa; (l) Pembangunan sistem aplikasi secara outsource perlu diselia dan dipantau oleh Pemilik Sistem bagi memastikan kejayaan pelaksanaan projek; (m) Kod sumber (*source code*) bagi sistem aplikasi dan perisian adalah menjadi hak milik Kerajaan; (n) Kod sumber (*source code*) bagi sistem aplikasi yang dibangunkan perlu dilengkapi dengan penerangan terperinci; (o) *Transfer of Technology* (ToT) perlu dilaksanakan apabila pembangunan sistem aplikasi selesai atau berlaku pertukaran Pentadbir Sistem ICT; dan (p) Pembangunan sistem aplikasi yang melibatkan integrasi antara sistem hendaklah menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang tidak memberi risiko ancaman keselamatan.	
042502 Prosedur Pembangunan Laman Web/Portal	**Tanggungjawab**
Laman Web adalah salah satu saluran penyebaran maklumat yang semakin penting antara kerajaan dan orang awam. Pembangunan dan perubahan pada laman web hendaklah dikawal dengan menggunakan **Prosedur Pengurusan Laman Web** yang telah ditetapkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua maklumat yang hendak dimuatkan ke dalam laman web mestilah mendapat kelulusan Jawatankuasa Pengurusan Laman	Pentadbir Sistem ICT PLANMalaysia dan Pentadbir Laman Web

Web; (b) Maklumat yang terkandung dalam laman web adalah di bawah tanggungjawab PLANMalaysia; (c) Maklumat di laman web hendaklah dikemaskini dari semasa ke semasa; (d) Laman web agensi luar yang memerlukan pautan ke Laman Web PLANMalaysia atau sebaliknya mestilah mendapat kebenaran Ketua Jabatan; dan (e) Pembangunan laman web hendaklah mempunyai ciri-ciri keselamatan bagi mengelak diceroboh dan digodam.	
042503 Prosedur Pembangunan Sistem Aplikasi Mudah Alih	**Tanggungjawab**
Sistem aplikasi mudah alih yang selamat perlu dibangunkan meliputi seluruh kitar hayat pembangunan sistem aplikasi PLANMalaysia berdasarkan **Prosedur Pembangunan Sistem Aplikasi (KRISA).** Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pembangunan sistem aplikasi mudah alih hendaklah melaksanakan pengujian sebelum dimuatnaik; (b) Penyediaan langganan sistem aplikasi mudah alih kepada orang awam hendaklah melalui perkhidmatan GAMMA; dan (c) Pembangunan sistem aplikasi mudah alih yang melibatkan integrasi antara sistem hendaklah menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang tidak memberi risiko ancaman keselamatan.	Pentadbir Sistem ICT PLANMalaysia

0426 Keperluan Keselamatan Aplikasi

Objektif:

Memastikan sebarang aplikasi yang dibangunkan atau diperolehi adalah selamat.

042601 Keperluan Keselamatan Aplikasi	Tanggungjawab
Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem aplikasi baharu atau penambahbaikan pada sistem aplikasi sedia ada. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pembangunan, penambahbaikan dan penyelenggaraan sistem aplikasi hendaklah mengambil kira kawalan keselamatan bagi memastikan tiada sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (b) Mewujudkan dan melindungi persekitaran bagi pembangunan sistem aplikasi yang merangkumi keseluruhan kitar hayat pembangunan sistem aplikasi; (c) Ujian keselamatan hendaklah dijalankan ke atas sistem aplikasi bagi memastikan integriti data dan sistem pemprosesan berjalan dengan betul dan sempurna; (d) Sistem aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; (e) Semua sistem aplikasi yang dibangunkan hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan; (f) memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan; (g) Semua sistem aplikasi yang dibangunkan hendaklah menjalani sekurang-kurangnya UAT dan FAT; (h) Dokumentasi sistem aplikasi hendaklah disediakan bagi semua sistem aplikasi yang dibangunkan; dan (i) Semua sistem aplikasi yang hendak dibangunkan perlu mengikut keperluan pengguna dan selaras dengan garis panduan dan pekeliling semasa yang sedang berkuatkuasa.	Pemilik Sistem, Pembekal, Pihak Ketiga dan Pentadbir Sistem ICT PLANMalaysia

0427 Prinsip Keselamatan Arkitektur Dan Kejuruteraan Sistem	
Objektif: Memastikan aktiviti pembangunan sistem maklumat adalah selamat.	
042701 Prinsip Keselamatan Arkitektur Dan Kejuruteraan Sistem	**Tanggungjawab**
Prinsip untuk keselamatan arkitektur dan kejuruteraan sistem hendaklah berpandukan kepada **Garis Panduan Pembangunan Aplikasi (KRISA)** yang terkini untuk apa-apa usaha pelaksanaan sistem maklumat.	Pemilik Sistem dan Pembekal

0428 Kod Selamat (*Secure Coding*)	
Objektif: Memastikan perisian ditulis dengan selamat dengan mengurangkan potensi kerentanan (*vulnerability*) keselamatan maklumat di dalam perisian.	
042801 Kawalan Kod Selamat	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Digalakkan menggunakan OWASP *Secure Codung Practice Checklist* untuk memastikan kod sumber selamat. Elakkan *hard-coded credentials* dan menggunakan *Input Validation* dan *Output Encoding*.	Pemilik Sistem dan Pembekal

0429 Pengujian Keselamatan Dalam Pembangunan Dan Penerimaan	
Objektif: Memastikan perisian ditulis dengan selamat dengan mengurangkan potensi kerentanan (*vulnerability*) keselamatan maklumat di dalam perisian.	
042901 Pengujian Keselamatan Sistem	**Tanggungjawab**
Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; (b) Membuat semakan pengesahan 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) Melakukan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem; dan (e) Menjalankan ujian penembusan untuk mengenal pasti kod dan reka bentuk yang tidak selamat.	Pemilik Sistem, PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia
042902 Pengujian Penerimaan Sistem	**Tanggungjawab**
Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Semua sistem aplikasi baharu (termasuklah sistem aplikasi yang dikemaskini atau diubah suai) hendaklah memenuhi kriteria yang ditetapkan dan juga mengikut garis panduan yang sedang berkuatkuasa sebelum diterima atau	Pemilik Sistem, PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia

dipersetujui; dan (b) Sistem aplikasi baharu hendaklah menjalani proses imbasan keselamatan dan melaksanakan tindakan pengukuhan sebelum digunakan.	

0430 Pembangunan Oleh Sumber Luar (*Outsourced*)	
Objektif: Memastikan langkah-langkah keselamatan maklumat yang diperlukan oleh PLANMalaysia dilaksanakan oleh pembangun sistem dari sumber luar (*outsourced*).	
043001 Pembangunan oleh Khidmat Luaran	**Tanggungjawab**
PLANMalaysia hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Kod sumber (*source code*) adalah menjadi **HAK MILIK KERAJAAN** atau mengikut terma perolehan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pelesenan dan kod sumber ialah **HAK MILIK KERAJAAN** dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource*; (b) Pembekal hendaklah membenar PLANMalaysia mencapai hak kod sumber dan melaksanakan pengolahan risiko atau mengikut terma perolehan; (c) Setiap sistem, aplikasi dan perisian hendaklah mematuhi garis panduan keselamatan dan lulus *User Acceptance Test* (UAT) dan *Final Acceptance Test* (FAT); (d) Penilaian keselamatan perlu dilakukan untuk memastikan keselamatan sistem; dan (e) Keperluan reka bentuk yang selamat, pengekodan dan pengujian pembangunan sistem perlu mengikut amalan terbaik.	Pemilik Sistem dan Pembekal

0431 Pengasingan Persekitaran Pembangun, Pengujian dan Produksi	
Objektif: Melindungi persekitaran produksi dan data dari dikompromi dari aktiviti pembangunan dan pengujian.	
043101 Pengasingan Persekitaran Pembangun, Pengujian dan Produksi	**Tanggungjawab**
Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perkakasan dan perisian yang diperlukan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari peralatan yang digunakan sebagai pengeluaran (*production*); (b) Pengasingan juga merangkumi tindakan memisahkan kumpulan produksi dan *development*; dan (c) Kawalan keselamatan pada data yang mengandungi maklumat rahsia rasmi sekiranya digunakan di dalam persekitaran pembangunan.	Pemilik Sistem
043102 Persekitaran Pembangunan Yang Selamat	**Tanggungjawab**
Organisasi hendaklah mewujudkan dan melindungi persekitaran pembangunan supaya selamat untuk pembangunan sistem dan integrasi yang meliputi seluruh kitar hayat pembangunan *System Development Life Cycle* (SDLC). PLANMalaysia perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: (a) Sensitiviti data yang akan diproses, disimpan dan dihantar/diterima dari/ke sistem; (b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; (c) Keperluan dalam pengasingan di antara pelbagai	Pemilik Sistem

persekitaran pembangunan sistem; (d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; (e) Kawalan ke atas capaian kepada persekitaran pembangunan sistem; dan (f) Pegawai bertugas dalam persekitaran pembangunan sistem yang boleh dipercayai.	

0432 Pengurusan Perubahan

Objektif:

Memelihara keselamatan maklumat ketika melaksanakan perubahan.

043201 Pengurusan Perubahan	Tanggungjawab
Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada Pemilik Sistem dan/ atau PICT dan/atau Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana perkakasan ICT hendaklah dikendalikan oleh Pentadbir Peralatan ICT dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian aset ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	ICTSO, Pemilik Sistem, PICT, Pentadbir Sistem ICT, Pentadbir Peralatan ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia
043202 Prosedur Kawalan Perubahan Sistem	**Tanggungjawab**
Perubahan pada sistem aplikasi dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan Prosedur Kawalan Perubahan Sistem yang telah ditetapkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem aplikasi dan/atau pakej perisian hendaklah dikawal, diuji,	PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT

direkodkan dan disahkan sebelum diguna pakai; (b) Sistem aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian dan/atau pangkalan data untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan PLANMalaysia. (c) PICT dan Pentadbir Sistem ICT perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh Pembekal; (d) Akses kepada kod sumber sistem aplikasi perlu dihadkan kepada Pengguna yang dibenarkan sahaja; dan (e) Sebarang kemungkinan kebocoran maklumat hendaklah dihalang.	

0433 Maklumat Aktiviti Pengujian

Objektif:

Memastikan perkaitan pengujian dan perlindungan maklumat operasi yang digunakan untuk pengujian.

043301 Perlindungan Maklumat Untuk Aktiviti Pengujian	Tanggungjawab
Maklumat yang digunakan untuk aktiviti pengujian hendaklah dipilih dengan teliti, dilindungi, dikawal dan disediakan secukupnya sebelum ujian dilaksanakan. 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) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; (d) Permohonan penyalinan dan penggunaan data sebenar sebagai data pengujian hendaklah direkodkan; (e) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna serta sistem *output* untuk memastikan data yang telah diproses adalah tepat; (f) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan (g) Mengaktifkan/mewujudkan fungsi jejak audit (*audit trail*) bagi merekodkan sebarang penyalinan dan penggunaan data sebenar (*production*).	ICTSO dan Pengguna

0434 Perlindungan Keselamatan Maklumat Ketika Pengujian Audit

Objektif:

Meminimumkan kesan jejak audit (*audit trail*) dan lain-lain aktiviti jaminan terhadap sistem operasi dan proses dalam perkhidmatan PLANMalaysia.

043401 Pematuhan Keperluan Audit	Tanggungjawab
Pematuhan terhadap keperluan audit bagi meminimumkan ancaman dan memaksimumkan keberkesanan aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas operasi aset ICT perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.	ICTSO, PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT PLANMalaysia

LAMPIRAN

11.0 LAMPIRAN

Berikut ialah lampiran-lampiran yang berkaitan sebagai panduan.

(i) Lampiran 1: Surat Akuan Pematuhan Dasar Keselamatan Siber PLANMalaysia;
(ii) Lampiran 2: Borang Pengesahan Pegawai Bertukar Keluar Atau Tamat Perkhidmatan Di PLANMalaysia
(iii) Lampiran 3: Proses Kerja Pelaporan Insiden Keselamatan Siber PLANMalaysia; dan
(iv) Lampiran 4: Senarai Perundangan dan Peraturan.

LAMPIRAN 1

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN SIBER PLANMalaysia

Nama : .....

No. Kad Pengenalan : .....

Jawatan : .....

PLANMalaysia : .....

Adalah dengan sesungguhnya dan sebenarnya saya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan Siber (DKS) PLANMalaysia;

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

3. Saya tidak akan menyimpan atau membawa keluar data dan maklumat serta maklumat rasmi PLANMalaysia apabila saya tidak lagi berkhidmat di PLANMalaysia.

Pegawai

Tandatangan:

.....

Tarikh:

LAMPIRAN 2

LAMPIRAN 2

BORANG PENGESAHAN PEGAWAI BERTUKAR KELUAR ATAU TAMAT PERKHIDMATAN DI PLANMalaysia

Nama : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian/ Jabatan/ Agensi : .....

Adalah dengan sesungguhnya dan sebenarnya saya mengaku bahawa saya telah memulangkan dan mengaku perkara-perkara berikut:

Sila tandakan □ pada kotak status yang berkenaan.

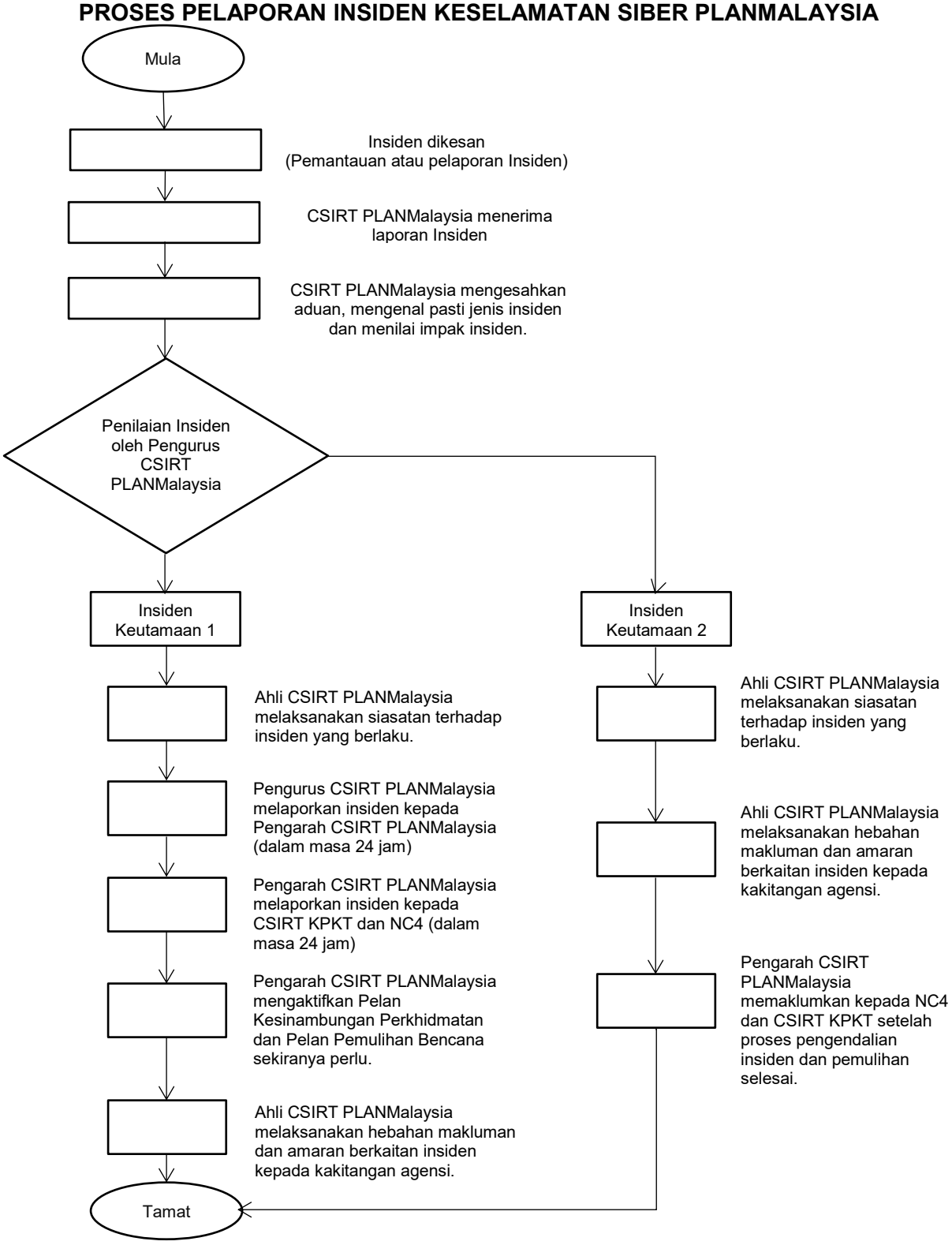
Bil.	Perkara	Status	Pengesahan
1.	Cop Nama		
2.	Kad Akses (Pas Keselamatan dan Parkir)		
3.	Aset ICT – Lampirkan senarai aset yang dipulangkan.		
4.	Saya tidak menyimpan atau membawa keluar data dan maklumat/ maklumat rasmi Jabatan.		
5.	Akses kepada sistem / perisian yang berkaitan: _____		

Pegawai	**Pengarah Bahagian/Pejabat Projek/Ketua Unit**	**Ketua Seksyen Sumber Manusia/Ketua Unit**
Tandatangan:	Tandatangan:	Tandatangan:
.....	.....	.....
Tarikh:	Tarikh:	Tarikh:

LAMPIRAN 3

LAMPIRAN 3

PROSES PELAPORAN INSIDEN KESELAMATAN SIBER PLANMALAYSIA



LAMPIRAN 4

LAMPIRAN 4

SENARAI PERUNDANGAN DAN PERATURAN

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
1.	Akta 88 - Akta Rahsia Rasmi 1972.	SPRM
2.	Akta 332 – Akta Hak Cipta Tahun 1987.	KPDNKK (Perbadanan Harta Intelek Malaysia)
3.	Akta 563 - Akta Jenayah Komputer 1997 bertarikh 30 Jun 1997.	Jabatan Peguam Negara
4.	Akta 588 - Akta Komunikasi dan Multimedia 1998 bertarikh 15 Oktober 1998.	SKMM
5.	Akta 589 - Akta Suruhanjaya Komunikasi dan Multimedia 1998 bertarikh 15 Oktober 1998.	SKMM
6.	Akta 562 - Akta Tandatangan Digital 1997 bertarikh 30 Jun 1997.	Jabatan Peguam Negara
7.	Akta 680 - Akta Aktiviti Kerajaan Elektronik 2007.	JDN
8.	Akta 629 - Akta Arkib Negara 2003.	Kementerian Pelancongan dan Kebudayaan Malaysia (Arkib Negara Malaysia)
9.	Akta 709 - Akta Perlindungan Data Peribadi 2010.	Kementerian Komunikasi dan Multimedia Malaysia (Jabatan Perlindungan Data Peribadi)
10.	Arahan Perbendaharaan Malaysia 150(i) bertarikh 31 Julai 2008.	Kementerian Kewangan Malaysia
11.	Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan bertarikh 1 Oktober 2000.	JDN
12.	Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) bertarikh 4 April 2001.	JDN
13.	Pekeliling Am Bilangan 2 Tahun 2002 - Penggunaan dan Pemakaian Data *Dictionary* Sektor Awam (DDSA) Sebagai *Standard* di Agensi- Agensi Kerajaan bertarikh 2 September 2002.	JDN
14.	Pekeliling Am Bilangan 2 Tahun 2006 - Pengukuhan Tadbir Urus Jawatankuasa IT dan Internet Kerajaan bertarikh 13 November 2006.	JDN
15.	Pekeliling Am Bil. 1 Tahun 2009 - Manual Pengurusan Aset Menyeluruh Kerajaan	JPM

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
	bertarikh 27 Mac 2009.	
16.	Pekeliling Am Bilangan 3 Tahun 2011 - Pemansuhan Keperluan Mengemukakan Laporan Polis Yang Tidak Merupakan Suatu Kehendak Undang-Undang dalam Berurusan Dengan Agensi Kerajaan bertarikh 29 September 2011.	JDN
17.	Pekeliling Am Bilangan 1 Tahun 2012 - Pemansuhan Keperluan Pengesahan Yang Tiada Nilai Tambah pada Borang Rasmi Kerajaan dan Salinan Dokumen Sokongan bertarikh 2 Mac 2012.	JDN
18.	Pekeliling Am Bilangan 2 Tahun 2012 - Tatacara Pengurusan Aset Tak Alih Kerajaan bertarikh 21 Jun 2012.	JPM
19.	Pekeliling Am Bilangan 3 Tahun 2012 - Sistem Kod Aset Tak Alih bertarikh 21 Jun 2012.	JPM
20.	Pekeliling Am Bilangan 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam bertarikh 30 September 2015.	JDN
21.	1 Pekeliling Perbendaharaan (1PP).	Kementerian Kewangan Malaysia
22.	Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 - Panduan Pengurusan Pejabat bertarikh 30 April 2007.	JPA
23.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi- Agensi Kerajaan bertarikh 28 November 2003.	JDN
24.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 - Pengurusan Laman Web Agensi Sektor Awam bertarikh 30 September 2015.	JDN
25.	Pekeliling Transformasi Pentadbiran Awam Bil.1 Tahun 2017 – Pelaksanaan Analitis Data Raya Sektor Awam (aDRSA).	JDN
26.	Pekeliling Transformasi Pentadbiran Awam Bil. 3 Tahun 2017 – Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan (*Government Unified Communication* (1GovUC))	JDN
27.	Surat Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2019 – Penyeragaman Lokasi Dan Reka Bentuk Pautan Borang	JDN

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
	Aduan Dan Maklum Balas Dalam Laman Web Agensi Sektor Awam.	
28.	Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2020 – MyGovEA: Pelaksanaan Pendekatan Reka Bentuk Berstruktur Ekosistem Organisasi Perkhidmatan Awam.	JDN
29.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021– Dasar Perkhidmatan Pengkomputeran Awam Sektor Awam.	JDN
30.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2021- Dasar Perkongsian Data Sektor Awam.	JDN
31.	Surat Arahan Ketua Setiausaha Negara - Langkah- langkah untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-agensi Kerajaan yang bertarikh 20 Oktober 2006.	JPM
32.	Surat Arahan Ketua Setiausaha Negara - Langkah- Langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit atau Lain-Lain Peralatan Komunikasi ICT Tanpa Kebenaran atau Kuasa yang Sah di Agensi-agensi Kerajaan bertarikh 31 Januari 2007.	JPM
33.	*Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002 bertarikh 15 Januari 2002	JDN
34.	Arahan Teknologi Maklumat 2007 bertarikh 19 Disember 2007.	JDN
35.	Arahan Keselamatan Kerajaan (Semakan dan Pindaan 2017).	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
36.	Surat Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 - Pematuhan Tatacara Penggunaan E-mel dan Internet	MKN
37.	Surat Arahan Ketua Pengarah MAMPU - Langkah- Langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan yang bertarikh 1 Jun	JDN

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
	2007.	
38.	Surat Arahan Ketua Pengarah MAMPU - Langkah- Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007.	JDN
39.	Surat Arahan Ketua Pengarah MAMPU - Pengaktifan Fail Log Server bertarikh 23 Mac 2009.	JDN
40.	Surat Arahan Ketua Pengarah MAMPU – Panduan Penyediaan dan Penyiaran Berita *Online* di Laman Web Agensi-agensi Kerajaan bertarikh 11 September 2009.	JDN
41.	Surat Arahan Ketua Pengarah MAMPU - Penggunaan *Smartphone*, *Personal Digital Assistant* dan Alat Komunikasi Mudah Alih Sebagai Saluran Komunikasi Tambahan bertarikh 15 September 2009.	JDN
42.	Surat Arahan Ketua Pengarah MAMPU - Penggunaan Media Sosial di Sektor Awam bertarikh 19 November 2009.	JDN
43.	Surat Arahan Ketua Pengarah MAMPU – Garis Panduan Transisi IPv6 Sektor Awam yang bertarikh 4 Januari 2010.	JDN
44.	Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.	JDN
45.	Surat Arahan Ketua Pengarah MAMPU – Panduan Pelaksanaan Pengurusan Projek ICT Sektor Awam yang bertarikh 5 Mac 2010.	JDN
46.	Surat Arahan Ketua Pengarah MAMPU – Pemantapan Penggunaan dan Pengurusan E-Mel di Agensi-Agensi Kerajaan yang bertarikh 1 Julai 2010.	JDN
47.	Surat Arahan Ketua Pengarah MAMPU – Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 dalam Sektor Awam yang bertarikh 24 November 2010.	JDN
48.	Surat Arahan Ketua Pengarah MAMPU - Amalan Terbaik Penggunaan Media Jaringan Sosial di Sektor Awam bertarikh 8 April 2011.	JDN
49.	Surat Arahan Ketua Pengarah MAMPU -	JDN

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
	Pelaksanaan dan Penggunaan Aplikasi *Digital Document Management System* (DDMS) Sektor Awam bertarikh 26 Januari 2015.	
50.	Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Rasionalisasi Laman Web bertarikh 26 Mei 2015.	JDN
51.	Surat Arahan Ketua Pengarah MAMPU – Pelaksanaan Penilaian Risiko Keselamatan Maklumat Menggunakan MyRAM App. 2.0 Di Agensi Sektor Awam bertarikh 12 Ogos 2015.	JDN
52.	Surat Arahan Ketua Pengarah MAMPU Bilangan 1 Tahun 2021 – Garis Panduan Perkhidmatan Galeri Aplikasi Mudah Alih Kerajaan Malaysia (GAMMA)	JDN
53.	Surat Pekeliling Am Bilangan 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di bawah Jawatankuasa IT dan Internet Kerajaan (JITIK) bertarikh 20 Disember 2000.	JDN
54.	Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005.	JDN
55.	Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam bertarikh 9 November 2006.	JDN
56.	Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009.	JDN
57.	Surat Pekeliling Am Bilangan 3 Tahun 2015 – Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan	JDN
58.	Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003	JDN
59.	Garis Panduan *IT Outsourcing* 2006 bertarikh Oktober 2006.	JDN
60.	Garis Panduan Penggunaan ICT ke arah	JDN

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
	ICT Hijau dalam Perkhidmatan Awam 2010 bertarikh 3 Ogos 2010.	
61.	Garis Panduan Pengurusan Projek Sektor Awam (PPriSA).	JDN
62.	Garis Panduan Pembangunan Aplikasi/ Kejuruteraan Sistem aplikasi Sektor Awam (KRISA).	JDN
63.	Garis Panduan Keselamatan KPKT.	KPKT
64.	Risalah Penerapan Etika Penggunaan Media Sosial dalam Sektor Awam – Mac 2015.	JDN
65.	*Standard Operating Procedure* (SOP) ICT KPKT.	KPKT
66.	Surat Pemberitahuan Mengenai Penyerahan Fungsi Keselamatan Siber Dan Dasar/ Pekeliling/ Penerbitan Berkaitan Keselamatan ICT Kerajaan Kepada Agensi Keselamatan Siber Negara rujukan MAMPU.700-5/12/1 Jld 3 (35) bertarikh 17 September 2021.	JDN / NACSA

12.0 PENGHARGAAN

AHLI JAWATANKUASA SEMAKAN DAN PENAMBAHBAIKAN DKS PLANMALAYSIA TAHUN 2025

A. Bahagian Khidmat Pengurusan

Seksyen Teknologi Maklumat

1. Ts. Mohd Aziri Bin Che Wil
2. Ts. Mas Al Hafiz bin Samsir
3. Puan Shaidatul Ezzan binti Mohamad Yusop
4. Puan Fahwani binti Mohd Ali
5. Encik Mohamad Farid Aidil bin Jamhadi
6. Encik Mohamad Eqmal Fareed Bin Md Yusof
7. Puan Nor Suhaida Binti Hashim
8. Encik Muhammad Ibrahimi bin Mazli

Seksyen Pentadbiran

9. Encik Muhamad Zuraini bin Yusoff

Seksyen Kewangan

10. Puan Nadia binti Mohamad

Seksyen Sumber Manusia

11. Puan Muazah binti Radzuan

B. Bahagian Maklumat Gunatanah Negara

1. Encik Muhamad Ikhwan bin Saadon
2. Encik Mohd Shazir bin Ashari
3. Encik Abdul Nur Aqeem bin Abdul Raffar

PLANMalaysia

Perancangan Melangkaui Kelaziman

Planning : Beyond Conventional