Teman Setia Anda

POLISI KESELAMATAN MAKLUMAT & PRIVASI

VERSI 1.1
25 SEPTEMBER 2025

1.0 PENGENALAN

Polisi Keselamatan Maklumat dan Privasi (PKMP), Jabatan Penyiaran Malaysia (RTM) mengandungi peraturan-peraturan yang MESTI DIBACA dan DIPATUHI semasa menggunakan aset dan pengoperasian di dalam perkhidmatan RTM.

Polisi ini juga menerangkan kepada semua pengguna (termasuk warga RTM dan pihak ketiga yang mempunyai urusan dengan perkhidmatan RTM) mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat aset RTM.

Maklumat ialah aset perkhidmatan penting (sama ada dalam bentuk fizikal atau elektronik) yang mempunyai nilai penting kepada RTM. Keselamatan maklumat adalah melindungi dari kerahsiaan, integriti dan ketersediaan maklumat aset perkhidmatan RTM. Ia juga bagi melindungi daripada risiko (ancaman dan kelemahan) yang boleh mengganggu kesinambungan perkhidmatan. Keselamatan maklumat juga dilaksanakan melalui perancangan, pembangunan, pengujian dan penyelenggaraan bagi mengekalkan keberkesanan dalam menyokong mencapai objektif perkhidmatan, mengekalkan imej dan meningkatkan pematuhan kepada undang-undang.

Pada era ini, pengurusan maklumat sangat bergantung kepada aset Teknologi Maklumat dan Komunikasi (ICT). Oleh itu, polisi ini juga menitikberatkan keselamatan ICT/siber di dalam pengurusan maklumat RTM.

Dokumen PKMP RTM ini dibangunkan bagi mematuhi keperluan standard :

i. ISO/IEC 27001:2013 *Information Security Management System* (*ISMS*); dan
ii. ISO/IEC 27701:2019 *Privacy Information Management System (PIMS)*

1.1 OBJEKTIF

Objektif dokumen PKMP RTM ini adalah:

a) Untuk menyediakan peranan dan tanggungjawab oleh semua pengguna, termasuk warga RTM dan pihak ketiga yang berurusan dengan perkhidmatan RTM;
b) Untuk memastikan jaminan keselamatan penyampaian perkhidmatan RTM, meningkatkan tahap keyakinan pihak berkepentingan termasuk pihak ketiga (pembekal perkhidmatan), orang awam/pelanggan RTMKLIK, industri dan kerajaan;
c) Untuk memastikan kelancaran operasi RTM dan meminimumkan kerosakan atau kemusnahan daripada sebarang insiden keselamatan, termasuk serangan siber, penyalahgunaan hak, dan kehilangan data termasuk data peribadi dan sensitif;
d) Untuk melindungi kepentingan pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan aset ICT; dan
e) Untuk menyediakan penambahbaikan dalam pengurusan kawalan keselamatan berterusan kepada RTM.

1.2 SKOP

Dokumen PKMP RTM ini adalah selaras dengan standard ISO/IEC 27002:2022 Keselamatan Maklumat, Keselamatan Siber Dan Perlindungan Privasi - Kawalan Keselamatan Maklumat yang meliputi bidang keselamatan berikut:

Seksyen 1: Tadbir Urus Keselamatan Maklumat dan Privasi

Seksyen 2: Pengurusan Risiko Keselamatan Maklumat dan Privasi

Seksyen 3: Keselamatan Sumber Manusia

Seksyen 4: Pengurusan Aset

Seksyen 5: Pengurusan Maklumat, Dokumen dan Rekod

Seksyen 6: Pengurusan Pihak Ketiga (Pembekal/Perunding)

Seksyen 7: Pengurusan Keselamatan Fizikal

Seksyen 8: Pengurusan Identiti dan Akses

Seksyen 9: Pengurusan Ancaman dan Kerentanan ICT

Seksyen 10: Pengurusan Insiden Keselamatan Maklumat

Seksyen 11: Pengurusan Kesinambungan Perkhidmatan

Seksyen 12: Pematuhan dan Undang-Undang

Seksyen 13: Pengurusan Keselamatan Rangkaian ICT

Seksyen 14: Pengurusan Keselamatan Sistem dan Aplikasi ICT

Seksyen 15: Pengurusan Keselamatan Data Peribadi (PII)

1.3 PERANAN DAN TANGGUNGJAWAB

Ketua Pengarah hendaklah bertanggungjawab sepenuhnya dalam melaksanakan kesemua bidang kawalan yang digariskan di dalam Polisi Keselamatan Maklumat dan privasi RTM dan memastikan polisi ini dipatuhi oleh warga RTM dan pihak ketiga yang mempunyai urusan dengan perkhidmatan RTM.

Peranan dan tanggungjawab setiap pengguna yang terlibat dalam mencapai objektif PKMP RTM diterangkan dengan lebih jelas di dalam Seksyen 1: TADBIR URUS KESELAMATAN MAKLUMAT DAN PRIVASI (1.2) Peranan dan Tanggungjawab Keselamatan Maklumat.

1.4 PEMAKAIAN

Polisi ini terpakai kepada semua warga RTM dan pihak ketiga yang mempunyai urusan perkhidmatan dengan RTM.

1.5 RUJUKAN

Tajuk Dokumen	Nombor Rujukan	Penerbit
Information Technology Security Techniques - Information Security Management Systems Requirements (3rd Revision)	ISO/IEC 27001:2022	*International Standard*
Information Technology Security Techniques- Code of Practices for Information Security Controls (3rd Revision)	ISO/IEC 27002:2022	*International Standard*
Surat Pekeliling Am Bil. 1 Tahun 2020 – Pemakluman Pemakaian dan Penguatkuasaan Arahan Keselamatan (Semakan dan Pindaan 2017)	KPKK(R)100-1/5/4 Jld.2(15)	Ketua Pengarah Keselamatan Kerajaan (CGSO)
Akta Perlindungan Data Peribadi 2010 dan Pindaan 2024	[Akta 709 dan Akta A1727]	Kementerian Komunikasi dan Digital

1.6 PERTANYAAN

Sebarang pertanyaan mengenai PKMP RTM ini boleh dikemukakan kepada:

- Seksyen Aplikasi ICT (SAICT)
- No. Telefon : +603-26364154
- Emel : saict_team@rtm.gov.my

1.7 PENGUATKUASAAN DAN SEMAKAN

Polisi ini berkuatkuasa dari mula ia ditandatangani oleh Ketua Pengarah Penyiaran dan disemak tiga (3) tahun sekali atau jika terdapat arahan terkini atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan, dan polisi Kerajaan bagi memastikan dokumen sentiasa relevan.

Pelanggaran terhadap PKMP RTM ini boleh mengakibatkan tindakan tatatertib, amaran atau teguran. Perbuatan seperti tidak tahu, berniat tidak baik atau menggunakan pertimbangan yang buruk tidak akan digunakan sebagai alasan untuk ketidakpatuhan.

Dengan berkuatkuasanya PKMP RTM ini, Polisi Keselamatan Siber (PKS) RTM versi 1.1 bertarikh 25 September 2025 adalah terbatal.

"MALAYSIA MADANI"
"BERKHIDMAT UNTUK NEGARA"

Saya yang menjalankan amanah,

(DATUK SUHAIMI SULAIMAN)
Ketua Pengarah Penyiaran
Jabatan Penyiaran Malaysia

25 September 2025

RTM/ICT/05/12 (5)

Diedarkan kepada :

Semua warga RTM

2.0 PRINSIP-PRINSIP KESELAMATAN MAKLUMAT DAN PRIVASI

a) Keselamatan maklumat adalah melindungi semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, dicipta, dimusnahkan, disimpan, dijana, dicetak, diakses, diedarkan, dalam penghantaran dan disalin untuk memastikan keselamatan dan ketersediaan maklumat kepada semua pengguna yang dibenarkan.

b) Prinsip keselamatan maklumat dan privasi berikut menyediakan tadbir urus menyeluruh untuk keselamatan dan pengurusan maklumat di RTM.

c) Ciri-ciri utama keselamatan maklumat adalah seperti berikut:
   - Kerahsiaan: Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan di akses tanpa kebenaran;
   - Integriti: Maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan; dan
   - Ketersediaan: Maklumat hendaklah boleh diakses pada bila-bila masa.

d) Kategori maklumat termasuk:
   i. **Maklumat Rahsia Rasmi** mempunyai erti yang diberikan kepadanya di bawah Akta Rahsia Rasmi 1972 (Akta 88). Apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.
   ii. **Maklumat Rasmi** ialah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh RTM semasa menjalankan urusan rasmi. Maklumat Rasmi ini juga merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

Maklumat rasmi mesti dibuat, digunakan, diterima, atau dikeluarkan secara rasmi oleh RTM semasa urusan operasi dan perkhidmatan.

iii. **Maklumat Pengenalan Peribadi** (PII[1]) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenal pasti individu tertentu. Data Peribadi mengandungi data sensitif individu. Data Peribadi boleh juga terkandung dalam Maklumat Rahsia Rasmi.

iv. **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. Data Peribadi dikecualikan daripada Data Terbuka.

e) Semua pengguna bertanggungjawab:
   i. Untuk memastikan klasifikasi maklumat itu diwujudkan mengikut tiga (3) klasifikasi maklumat iaitu Sulit, Terhad dan Terbuka;
   ii. Untuk mengendalikan maklumat tersebut mengikut tahap klasifikasi/pengelasannya;
   iii. Untuk mematuhi polisi, prosedur, dan sebarang keperluan kontrak/perjanjian RTM; dan
   iv. Untuk melindungi Data Peribadi yang terdiri daripada data sensitif individu.

f) Maklumat mesti dilindungi daripada akses dan pemprosesan yang tidak dibenarkan.

g) Kawalan keselamatan maklumat dan polisi/konfigurasi yang dipasang hendaklah disemak secara berkala, termasuk audit dalaman/luaran tahunan dan ujian penembusan. Di samping itu, langkah ke arah memastikan kawalan keselamatan maklumat hendaklah berdasarkan penilaian risiko yang sesuai terhadap perubahan ancaman/kelemahan kepada aset maklumat tersebut.

[1] *Personally Identifiable Information*

3.0 PENYATAAN POLISI

No. Polisi	Polisi	Tanggungjawab
Seksyen 1	**TADBIR URUS KESELAMATAN MAKLUMAT DAN PRIVASI**	
1.1	**Polisi Keselamatan Maklumat dan Privasi**	
	Objektif: Untuk memastikan kesesuaian, kecukupan dan keberkesanan berterusan hala tuju pengurusan dan sokongan untuk keselamatan maklumat selaras dengan keperluan perkhidmatan, undang-undang, berkanun, peraturan dan kontrak.	
1.1.1	Polisi Keselamatan Maklumat dan Privasi hendaklah ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan RTM kepada warga RTM dan pihak ketiga yang mempunyai urusan dengan perkhidmatan RTM.	JPICT/CDO/ Pengarah Bahagian / Pengarah Negeri
1.1.2	a. Polisi ini hendaklah dikaji semula sekurang-kurangnya tiga (3) tahun sekali atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	JPICT/CDO/ ICTSO / ICTO
	b. Memaklumkan pindaan yang telah disahkan kepada warga RTM, pembekal dan pihak yang mempunyai urusan dengan RTM.	JPICT/CDO/ ICTSO / ICTO
1.1.3	Penguatkuasaan Polisi Keselamatan Maklumat dan Privasi adalah seperti berikut: a. Polisi Keselamatan Maklumat dan Privasi RTM mestilah dipatuhi oleh warga RTM dan pihak ketiga yang mempunyai urusan dengan perkhidmatan RTM.	Pengguna
	b. Pelaksanaan polisi ini akan dijalankan oleh Urus Setia ISPMS dengan disokong oleh Pengurusan Tertinggi RTM.	Pengurusan Tertinggi RTM
1.1.4	Sebarang pelanggaran polisi ini sama ada yang disengajakan atau tidak disengajakan tertakluk	Pengguna

No. Polisi	Polisi	Tanggungjawab
	kepada tindakan pembetulan atau tatatertib yang sewajarnya.	
1.2	**Peranan dan Tanggungjawab Keselamatan Maklumat dan Privasi**	
	Objektif: Untuk mewujudkan struktur yang ditakrifkan, diluluskan dan difahami untuk pelaksanaan, operasi dan pengurusan keselamatan maklumat dalam organisasi.	
1.2.1	Tanggungjawab adalah seperti yang berikut: a. Memastikan penguatkuasaan pelaksanaan Polisi ini; b. Memastikan warga RTM, pembekal dan pihak yang mempunyai urusan dengan RTM memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini; c. Memastikan semua keperluan RTM seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi; d. Memastikan pengurusan risiko dan program keselamatan maklumat dilaksanakan seperti yang ditetapkan di dalam Polisi ini; dan e. Melantik Ketua Pegawai Digital (CDO), ICTO dan ICTSO .	Ketua Pengarah Penyiaran
1.2.2	Tanggungjawab adalah seperti yang berikut: a. Menjalankan penilaian risiko keselamatan maklumat dan menentukan tahap risiko; b. Mengenal pasti dan menilai pilihan untuk Pentaksiran Risiko dan menghasilkan Pelan Penguraian Risiko; c. Kenal pasti kawalan keselamatan yang berkaitan untuk mengurangkan risiko. d. Pilih kawalan keselamatan yang sesuai dan pastikan keberkesanan;	Pasukan Pelaksana ISPMS RTM

No. Polisi	Polisi	Tanggungjawab
	e. Memantau dan menyampaikan pelaksanaan keselamatan maklumat secara dalaman.	
1.2.3	Tanggungjawab adalah seperti yang berikut: a. Membantu CDO dalam melaksanakan tugas-tugas yang melibatkan keselamatan maklumat seperti yang ditetapkan di dalam Polisi ini; b. Memastikan kawalan keselamatan maklumat dalam RTM diseragam dan diselaraskan dengan sebaiknya; c. Menyelaras pelan latihan dan program kesedaran keselamatan maklumat; d. Berperanan sebagai Pengarah CERT RTM e. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini; f. Merangka pengurusan risiko dan audit keselamatan maklumat berpandukan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat yang berkuat kuasa; g. Memaklumkan sebarang perkara atau penemuan mengenai keselamatan maklumat kepada CDO; h. Melaporkan insiden keselamatan maklumat kepada Pengurus Besar bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan (PKP); i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan maklumat dan memastikan langkah-langkah baik pulih diambil dengan segera;	CDO/ ICTSO / ICTO

No. Polisi	Polisi	Tanggungjawab
	j. Mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan; k. Menguatkuasakan pelaksanaan Polisi Keselamatan Maklumat RTM; dan l. Melaksanakan pematuhan Polisi ini oleh warga RTM dan pihak ketiga yang mempunyai urusan dengan perkhidmatan RTM.	
1.2.4	Tanggungjawab adalah seperti yang berikut: a. Merancang dan menyelaras penyediaan Pelan Strategik ICT (PSP) RTM untuk tempoh setiap 5 (lima) tahun bagi menyediakan hala tuju strategik ICT selaras dengan visi dan misi negara. b. Membangunkan sistem atau aplikasi baharu ICT mengikut keperluan jabatan sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; c. Memantau pembangunan dan penyelenggaraan portal radio berdasarkan permintaan pengguna dan keperluan jabatan bagi memastikan kelancaran operasi portal radio. d. Mengurus, memantau dan melaksana penyediaan infrastruktur termasuk perolehan perkakasan ICT untuk semua warga RTM bagi Ibu Pejabat dan RTM Negeri; e. Membantu dalam melaksanakan Pensijilan ISO/IEC 27001:2013 *Information Security Management System*	ICTO

No. Polisi	Polisi	Tanggungjawab
	(ISMS) di Jabatan Penyiaran Malaysia bagi memastikan proses kerja mengikut prosedur yang ditetapkan. f. Menguruskan pelaksanakan Mesyuarat Jawatankuasa Pemandu ICT bagi mendapatkan kelulusan Permohonan Projek ICT g. Mengendalikan perisian dan peralatan sidang video di Ibu Pejabat; h. Perolehan teknologi dan perkhidmatan komunikasi ICT baharu; i. Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat kerajaan yang berkuatkuasa. j. Menentukan kawalan akses semua pengguna terhadap aset ICT RTM.	
1.2.5	Tanggungjawab adalah seperti yang berikut: a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai personel yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ini; c. Memantau aktiviti capaian sistem aplikasi; d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan	Pentadbir Sistem ICT

No. Polisi	Polisi	Tanggungjawab
	atau memberhentikannya dengan serta-merta; e. Menganalisis dan menyimpan rekod jejak audit; dan f. Menyediakan laporan mengenai aktiviti capaian secara berkala;	
1.2.6	Tanggungjawab adalah seperti yang berikut: a. Membaca, memahami dan mematuhi Polisi yang berkaitan; b. Mengetahui dan memahami implikasi keselamatan maklumat kesan daripada tindakannya; c. Menjalani tapisan keselamatan sekiranya diperlukan apabila dikehendaki berurusan dengan maklumat rasmi RTM; d. Mematuhi prinsip-prinsip keselamatan Polisi ini dan menjaga kerahsiaan maklumat dan privasi RTM. e. Bertanggungjawab menjaga setiap perkakasan ICT yang diterima dengan baik.	Pengguna
1.3	**Pengasingan Tugas**	
	Objektif: Untuk mengurangkan risiko penipuan, kesilapan dan memintas kawalan keselamatan maklumat.	
1.3.1	Mestilah menyemak, memahami dan mematuhi tanggungjawab keselamatan yang diluluskan oleh pihak pengurusan. Sekiranya tidak jelas, mereka hendaklah mendapatkan penjelasan daripada pengurus/penyelia.	ICTO
1.4	**Pengurusan Kawalan Keselamatan**	
	Objektif: Untuk memastikan pengurusan memahami peranan mereka dalam keselamatan maklumat dan privasi serta melaksanakan tindakan yang sebaiknya.	

No. Polisi	Polisi	Tanggungjawab
1.4.1	Tanggungjawab adalah seperti yang berikut: a. Memastikan semua pengguna menggunakan polisi keselamatan maklumat dan privasi serta melaksanakan kawalan keselamatan mengikut peranan masing-masing. b. Memastikan pemantauan dan penyelarasan dengan semua jabatan dalam melaksanakan kawalan keselamatan maklumat di RTM.	CDO Pengarah Bahagian
1.5	**Hubungan Dengan Pihak Berkuasa**	
	Objektif: Untuk memastikan aliran maklumat yang sesuai berlaku berkenaan dengan keselamatan maklumat antara organisasi dan pihak berkuasa undang-undang, kawal selia dan penyeliaan yang berkaitan.	
1.5.1	Hubungan yang baik dengan pihak berkuasa dan pembekal berkaitan hendaklah dibangunkan dan diselaraskan bagi melancarkan urusan berkaitan pematuhan, insiden keselamatan, kecemasan atau pembekalan perkhidmatan.	BKP, Pasukan ERT, CERT RTM
1.6	**Hubungan Dengan Kumpulan Berkepentingan Yang Khusus**	
	Objektif: Untuk memastikan aliran maklumat yang sesuai berlaku berkenaan dengan keselamatan maklumat.	
1.6.1	a. Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah diadakan dan diselaraskan. b. Menjadi ahli *(membership)* atau forum dengan kumpulan berkepentingan khas mestilah diambil kira sebagai satu cara untuk meningkatkan pengetahuan tentang amalan terbaik dan mengikuti perkembangan	Warga RTM (Mengikut Bidang Kepakaran)

No. Polisi	Polisi	Tanggungjawab
	maklumat keselamatan yang berkaitan; seperti menerima amaran awal, nasihat dan tampalan *(patches)* yang berkaitan dengan serangan dan kelemahan; dan mendapat akses kepada nasihat keselamatan maklumat pakar.	

No. Polisi	Polisi	Tanggungjawab
Seksyen 2	**PENGURUSAN RISIKO KESELAMATAN MAKLUMAT DAN PRIVASI**	
2.1	**Pengurusan Risiko Keselamatan Maklumat & Strategi Perkhidmatan**	
	Objektif: Pengurusan Risiko Keselamatan Maklumat dan Privasi menyediakan pengurusan risiko keselamatan dan privasi bagi menjamin pematuhan kepada undang-undang dan peraturan yang berkenaan, melindungi komponen kerahsiaan, integriti dan ketersediaan (CIA), melindungi sumber ICT dan tahap penerimaan risiko yang dapat menyokong operasi perkhidmatan.	
2.1.1	Tanggungjawab adalah seperti berikut: a. Pengurusan Risiko Keselamatan Maklumat dan Privasi mestilah selaras dengan proses pengurusan risiko perkhidmatan dan menyediakan peranan dan tanggungjawab yang jelas. b. Menyediakan kaedah untuk pelaksanaan pengurusan risiko keselamatan maklumat dan privasi yang jelas.	Warga RTM (Pasukan Projek)
2.1.2	a. Melaksanakan pentaksiran risiko keselamatan maklumat dan privasi; memilih kawalan keselamatan dan proses yang bersesuaian untuk mengurangkan risiko ke tahap yang boleh diterima; b. Melaksanakan penguraian risiko keselamatan maklumat dan privasi bagi mengurangkan risiko; c. Memilih tindakan penguraian risiko seperti berikut: i. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian; ii. Menerima dan/atau bersedia	CDO RTM Pengarah Bahagian JKK ISPMS

No. Polisi	Polisi	Tanggungjawab
	berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi; iii. Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan iv. Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak lain yang berkepentingan. d. Memantau keberkesanan kawalan keselamatan secara berkala; dan e. Menyediakan komunikasi bagi mencapai persetujuan pengurusan risiko dengan bertukar-tukar dan berkongsi maklumat di antara pemilik risiko dan pihak berkepentingan lain yang berkaitan.	
2.2	**Keselamatan Maklumat dalam Pengurusan Projek**	
	Objektif: Untuk memastikan risiko keselamatan maklumat yang berkaitan dengan projek dan penghantaran ditangani dengan berkesan dalam pengurusan projek sepanjang kitaran hayat projek.	
2.2.1	Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek seperti berikut: a. Keselamatan maklumat perlu di integrasikan dan diselaraskan bagi setiap pengurusan projek RTM b. objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan	Warga RTM (Pasukan Projek)

No. Polisi	Polisi	Tanggungjawab
	metodologi projek; c. pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan; d. kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan kawalan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan maklumat RTM ; dan e. penyediaan spesifikasi perolehan hendaklah mengambil kira keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat yang setara.	
2.3	**Kajian Bebas Keselamatan ICT**	
	Objektif: Untuk memastikan kesesuaian, kecukupan dan keberkesanan berterusan pendekatan organisasi untuk mengurus risiko keselamatan ICT.	
2.3.1	Penilaian keselamatan ICT oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur. Contoh: Ujian Penembusan atau Penilaian Postur Keselamatan atau yang setara.	ICTSO / ICTO dan Pemilik Perkhidmatan

No. Polisi	Polisi	Tanggungjawab
Seksyen 3	**KESELAMATAN SUMBER MANUSIA**	
3.1	**Sebelum Perkhidmatan**	
	Objektif: Memastikan semua pengguna RTM dapat melaksanakan peranan dan tanggungjawab melalui penilaian keselamatan atas kelayakan dan kesesuaian semasa mereka bekerja.	
3.1.1	Membuat tapisan keselamatan terhadap semua calon warga RTM (termasuk sepenuh masa, sambilan dan sementara), pembekal dan pihak ketiga yang terlibat selaras dengan keperluan perkhidmatan yang dinyatakan di dalam skim perjawatan RTM atau kontrak.	Pengguna
3.1.2	Semakan latar belakang pada penglibatan pembekal dan pihak ketiga hendaklah mengikut undang-undang, peraturan dan etika yang berkaitan, dan ia harus berdasarkan kepada keperluan perkhidmatan, klasifikasi maklumat yang akan diakses bagi mengurangkan risiko.	Pengguna
3.2	**Terma dan Syarat Perkhidmatan**	
	Objektif: Untuk memastikan semua pengguna RTM memahami tanggungjawab keselamatan maklumat mereka untuk peranan yang mereka dipertimbangkan.	
3.2.1	a. Perjanjian kontrak dengan warga RTM hendaklah menyatakan tanggungjawab untuk keselamatan maklumat dan privasi. b. Mendapatkan persetujuan dan pengesahan dengan mengisi Akuan Pematuhan Polisi Keselamatan Maklumat dan Privasi seperti pautan berikut: i) Warga RTM : https://forms.gle/pHLxHQFcAc8YTpXx6 ii) Pihak ketiga: https://forms.gle/nUPQ2ja4hWS8Qw5bA	Pengguna

No. Polisi	Polisi	Tanggungjawab
3.2.2	a. Perjanjian kontrak dengan pembekal dan pihak ketiga hendaklah menyatakan tanggungjawab keselamatan maklumat dan privasi. b. Mendapatkan persetujuan dengan mengisi borang Akuan Pematuhan Polisi Keselamatan Maklumat dan Privasi secara atas talian seperti 3.2.1b	Pengguna
3.3	**Kesedaran, Pendidikan dan Latihan Keselamatan Maklumat dan Privasi**	
	Objektif: Untuk memastikan semua pengguna RTM dan pihak berkepentingan yang berkaitan memenuhi tanggungjawab terhadap keselamatan maklumat dan privasi di organisasi.	
3.3.1	Warga RTM dan pihak ketiga yang mempunyai urusan perkhidmatan dengan RTM hendaklah diberikan program kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan maklumat dan privasi bagi meningkatkan kompetensi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program yang harus dilaksanakan termasuk kesedaran tentang pelaporan insiden, bagi memastikan pengguna mengetahui akibatnya terhadap organisasi (contoh: akibat undang-undang, kehilangan perkhidmatan dan jenama atau kerosakan reputasi). Bagi pengguna mereka perlu sedar tentang tindakan disiplin yang boleh diambil dan kesan fizikal, kesan material dan emosi apabila melanggar peraturan dan prosedur privasi atau keselamatan, terutama bagi mereka yang menguruskan atau	Pengguna

No. Polisi	Polisi	Tanggungjawab
	mengendali data peribadi.	
3.4	**Proses Tatatertib**	
	Objektif: Untuk memastikan warga RTM dan pihak berkepentingan lain agar memahami akibat pelanggaran polisi keselamatan maklumat dan privasi, untuk menghalang dan berurusan dengan sewajarnya dengan warga RTM dan pihak berkepentingan lain yang melakukan pelanggaran tersebut.	
3.4.1	Proses tatatertib yang formal hendaklah disampaikan kepada warga RTM dan tersedia bagi membolehkan tindakan sewajarnya diambil.	CDO / Unit Integriti
3.5	**Penamatan atau Pertukaran Tanggungjawab Perkhidmatan**	
	Objektif: Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas warga RTM diurus dengan teratur.	
3.5.1	Tanggungjawab dan tugas keselamatan maklumat dan privasi adalah kekal sah selepas pemberhentian atau pertukaran pekerjaan hendaklah ditakrifkan, dikuatkuasakan dan disampaikan kepada pengguna yang berkaitan.	Pentadbir Sistem ICT dan warga RTM

No. Polisi	Polisi	Tanggungjawab
Seksyen 4	**PENGURUSAN ASET**	
4.1	**Inventori Maklumat dan Aset**	
	Objektif: Untuk mengenal pasti maklumat organisasi dan aset yang berkaitan dapat dilindungi dan menetapkan pemilikan yang sesuai.	
4.1.1	a. Memastikan semua aset maklumat dan ICT RTM direkodkan dan dikemaskini dari semasa ke semasa; b. Memastikan semua aset maklumat dan ICT RTM yang direkodkan mempunyai pemilik. c. Memastikan pengurusan aset adalah mematuhi Pekeliling Pengurusan Aset Kerajaan.	Pegawai Penerima Aset, Pegawai Aset dan warga RTM
4.1.2	a. Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan; b. Semua perisian aplikasi dan perisian sumber ICT mesti mempunyai lesen yang sah; c. Semua perolehan hendaklah mematuhi proses Perolehan RTM; d. Memastikan semua jenis aset maklumat dan ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.	Pegawai Aset dan warga RTM
4.2	**Penerimaan Penggunaan Maklumat dan Aset**	
	Objektif: Untuk memastikan maklumat dan aset yang berkaitan dilindungi, digunakan dan dikendalikan dengan sewajarnya.	
4.2.1	Peraturan untuk penggunaan maklumat yang boleh diterima dan aset yang dikaitkan dengan kemudahan pemprosesan maklumat dan maklumat mesti dikenal pasti, didokumenkan	Warga RTM

	dan dilaksanakan;	
4.2.2	Prosedur pengendalian aset hendaklah dibangunkan dan dilaksanakan mengikut tiga(3) klasifikasi iaitu Sulit, Terhad dan Terbuka;	Pegawai Aset dan warga RTM
4.2.3	Maklumat hendaklah dikelaskan berdasarkan keperluan undang-undang, nilai dan sensitiviti maklumat tersebut serta dilabel mengikut peringkat keselamatan maklumat.	Pegawai Pengelasan
4.3	**Pemulangan Aset**	
	Objektif: Untuk melindungi aset organisasi ketika proses penukaran atau penamatan pekerjaan, kontrak atau perjanjian.	
4.3.1	Semua aset organisasi mesti dikembalikan dalam simpanan mereka selepas penamatan pekerjaan, kontrak atau perjanjian mereka.	Warga RTM
4.4	**Media Storan**	
	Objektif: Untuk memastikan hanya pendedahan yang dibenarkan, pengubahsuaian, penyingkiran atau pemusnahan maklumat pada media storan.	
4.4.1	Pengurusan media storan hendaklah: a. Media dilupuskan dengan selamat apabila tidak lagi diperlukan, menggunakan prosedur formal; b. Maklumat yang disimpan dalam media fizikal mesti disimpan/*backup* (sebelum media dilupuskan) dan sebarang rekod pelupusan hendaklah disimpan dalam bentuk jejak audit; c. Peranti rosak yang mengandungi data sensitif mesti dinilai sebelum dimusnahkan secara fizikal; d. Semua peralatan yang mengandungi media storan mesti disahkan untuk memastikan bahawa sebarang data sensitif dan perisian berlesen telah dialih keluar atau *backup*	Pentadbir Sistem ICT dan Jawatankuasa yang dilantik untuk pelupusan aset.

	dengan selamat sebelum dilupuskan atau digunakan semula; dan e. Semua media storan yang mengandungi maklumat Sulit dan Terhad hendaklah dilindungi semasa pemindahan di luar premis RTM daripada akses yang tidak dibenarkan, penyalahgunaan dan kerosakan.	
4.5	**Penyelenggaraan Peralatan**	
	Objektif: Untuk mengelakkan kehilangan, kerosakan, kecurian atau kompromi maklumat dan aset yang berkaitan yang mengakibatkan gangguan kepada operasi organisasi yang disebabkan oleh kelemahan penyelenggaraan.	
4.5.1	Peralatan mesti diselenggara dengan betul untuk memastikan ketersediaan dan integritinya yang berterusan.	Pengguna
4.6	**Pelupusan Selamat atau Penggunaan Semula Peralatan**	
	Objektif: Untuk mengelakkan kebocoran maklumat daripada peralatan yang akan dilupuskan atau digunakan semula.	
4.6.1	Peralatan atau perisian ICT yang terletak di kawasan selamat (contoh: Pusat Data/ Bilik Pelayan); tidak boleh dialih keluar dari premis tanpa kebenaran terlebih dahulu.	Pentadbir Sistem ICT dan Jawatankuasa yang dilantik untuk pelupusan aset.
4.7	**Peranti Pengguna**	
	Objektif: Untuk melindungi maklumat daripada risiko kepada peranti pengguna.	
4.7.1	Peranti pengguna termasuk peranti yang disediakan oleh RTM dan peranti peribadi (BYOD) hendaklah: a. Melindungi peranti secara fizikal dengan kunci berkunci atau setara jika peranti berada di dalam kawasan yang tidak selamat (contoh: di tempat awam, kenderaan, bilik hotel, persidangan, dan kawasan terbuka);	Pengguna

	b. Mengaktifkan mod tidur atau menggunakan penyelamat skrin dengan kata laluan ke atas komputer. c. Peranti hendaklah dipasang dengan perisian berlesen dan perisian perlindungan dan dikemas kini; d. Data RTM yang disimpan dalam peranti mesti dilindungi pada setiap masa; e. RTM mempunyai hak untuk mengakses data pada peranti peribadi untuk sebarang urusan keselamatan. Menyusun, menyalin, menyebarkan, melaksanakan atau cuba memperkenalkan sebarang virus[2] atau kod komputer yang direka untuk mereplikasi sendiri, merosakkan atau sebaliknya menghalang prestasi komputer atau rangkaian RTM adalah tidak dibenarkan; dan f. Mana-mana peranti yang memerlukan akses wi-fi mesti mendapat kebenaran daripada Seksyen Media Teknologi Aplikasi (MTA).	

[2] sejenis program komputer yang, apabila dilaksanakan, mereplikasi dirinya sendiri dengan mengubah suai program komputer lain dan memasukkan kodnya sendiri ke dalam program tersebut.

No. Polisi	Polisi	Tanggungjawab
Seksyen 5	**PENGURUSAN MAKLUMAT DAN DOKUMEN**	
5.1	**Klasifikasi maklumat**	
	Objektif: Untuk mengenalpasti kefahaman tentang keperluan perlindungan maklumat selaras dengan kepentingannya kepada organisasi.	
5.1.1	Perlindungan maklumat mestilah selaras dengan yang berikut: a. Maklumat mesti diklasifikasikan dari segi keperluan undang-undang, nilai, kritikal, dan kepekaan terhadap pendedahan atau pengubahsuaian yang tidak dibenarkan; dan b. Maklumat dikelaskan mengikut skema klasifikasi maklumat RTM.	Pegawai Pengelas
5.1.2	Semua dokumen dan rekod hendaklah diklasifikasikan mengikut fungsi tugasan masing-masing.	Pegawai Pengelas
5.2	**Pelabelan Maklumat**	
	Objektif: Untuk memudahkan komunikasi klasifikasi maklumat dan menyokong automasi pemprosesan dan pengurusan maklumat.	
5.2.1	Proses yang sesuai untuk pelabelan maklumat mestilah dibangunkan dan dilaksanakan mengikut skema klasifikasi maklumat yang diterima pakai oleh RTM.	Warga RTM
5.2.2	Semua dokumen dan rekod hendaklah dilabelkan mengikut klasifikasi maklumat yang ditetapkan.	Warga RTM
5.3	**Pemindahan maklumat**	
	Objektif: Untuk mengekalkan keselamatan maklumat yang dipindahkan dalam organisasi dan dengan mana-mana pihak luar yang berkepentingan.	
5.3.1	Pemindahan maklumat boleh berlaku melalui pemindahan elektronik, pemindahan media storan fizikal dan pemindahan lisan.	Pentadbir Sistem ICT dan Jawatankuasa yang dilantik untuk

No. Polisi	Polisi	Tanggungjawab
	Keselamatan maklumat yang dipindahkan mestilah mengikut perkara berikut: a. Pemindahan maklumat melalui kemudahan komunikasi elektronik (termasuk mel elektronik, audio, faksimili dan video) mesti dilindungi daripada pemintasan, penyalinan dan pengubahsuaian yang tidak dibenarkan; b. Pemindahan maklumat media storan fizikal (termasuk kertas dokumen/rekod) mesti dilindungi melalui sebarang jenis kemudahan termasuk perkhidmatan kurier, pengangkutan dan sebagainya; dan c. Pemindahan maklumat secara lisan juga mesti dilindungi termasuk tidak membuat perbualan lisan sulit di tempat awam atau menggunakan saluran komunikasi yang tidak selamat yang boleh didengari oleh orang yang tidak dibenarkan.	pelupusan aset
5.4	**Perlindungan Rekod**	
	Objektif: Untuk memastikan pematuhan kepada keperluan undang-undang, berkanun, peraturan dan kontrak, serta kepentingan komuniti atau masyarakat yang berkaitan dengan perlindungan dan ketersediaan rekod	
5.4.1	Proses yang sesuai untuk penyimpanan, pengendalian, penyimpanan dan pelupusan rekod dan maklumat mesti mematuhi keperluan keselamatan RTM atau kewajipan kontrak yang berkenaan.	Pengguna
5.4.2	Perlindungan rekod mestilah mengikut perkara berikut: a. Rekod yang sesuai mesti diselenggara untuk mengesan semua aset maklumat termasuk	Warga RTM

No. Polisi	Polisi	Tanggungjawab
	peralatan atau perisian ICT di premis RTM; dan b. Rekod mesti disimpan berdasarkan tempoh pengekalan yang dikenal pasti oleh pemilik data dan/atau pemilik sistem.	
5.5	**Perjanjian Kerahsiaan**	
	Objektif: Untuk mengekalkan kerahsiaan maklumat yang boleh diakses oleh warga RTM atau pihak luar.	
5.5.1	Keperluan untuk perjanjian kerahsiaan untuk melindungi maklumat RTM mesti disemak, didokumenkan dan dikuatkuasakan mengikut keperluan keselamatan maklumat atau kontrak yang berkenaan.	ICTSO, ICTO, Pentadbir Sistem ICT, Pengguna dan Pihak Ketiga
5.6	**Perlindungan Terhadap Perisian Hasad (*Malware*)**	
	Objektif: Untuk memastikan maklumat dan aset lain yang berkaitan dilindungi daripada perisian hasad.	
5.6.1	Perlindungan maklumat dari perisian hasad mestilah mengikut perkara berikut: a. Kawalan pengesanan, pencegahan dan pemulihan untuk melindungi daripada perisian hasad mesti dilaksanakan, digabungkan dengan kesedaran pengguna yang sesuai; Contoh: *antivirus, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Content Filtering dan Web Application Firewall (WAF)* dan mengikut prosedur penggunaan yang betul dan selamat; b. Perisian pengesanan dan pembaikan antivirus yang diluluskan oleh RTM mesti dipasang pada setiap pelayan, *desktop* dan komputer riba dengan *update* yang terkini;	Pentadbir Sistem ICT, Pengguna

No. Polisi	Polisi	Tanggungjawab
	c. Pelan pemulihan sistem untuk insiden keselamatan ICT yang merangkumi data dan perisian sandaran dan pengaturan pemulihan yang diperlukan mesti diwujudkan; d. Melaksanakan peraturan dan kawalan yang menghalang atau mengesan penggunaan perisian yang tidak dibenarkan; dan e. Melaksanakan kawalan yang menghalang atau mengesan penggunaan laman web yang diketahui atau disyaki berniat jahat (contoh: *blocklisting*)	
5.6.2	Memuat turun atau memasang perisian daripada mana-mana sistem lain di luar RTM adalah tidak dibenarkan tanpa kelulusan terlebih dahulu.	Warga RTM
5.7	**Pemadaman Maklumat**	
	Objektif: Untuk mengelakkan pendedahan maklumat sensitif dan untuk mematuhi keperluan undang-undang, berkanun, peraturan dan kontrak untuk pemadaman maklumat.	
5.7.1	Perlindungan pemadaman maklumat mestilah mengikut perkara berikut: a. Memastikan bahawa mana-mana sistem dan peranti yang menyimpan maklumat sensitif yang diiktiraf oleh RTM dimusnahkan dengan selamat menggunakan aplikasi pemadaman yang diluluskan; dan b. Bagi peranti yang tidak boleh ditulis ganti (contoh: pemacu keras yang rosak, CD/DVD), hendaklah memastikan peranti dimusnahkan sebelum dilupuskan.	Pentadbir Sistem ICT dan Jawatankuasa yang dilantik untuk pelupusan aset.
5.8	**Perlindungan Data**	
	Objektif: Untuk mengehadkan pendedahan data sensitif, termasuk PII, dan untuk mematuhi keperluan undang-undang, berkanun,	

No. Polisi	Polisi	Tanggungjawab
	peraturan dan kontrak.	
5.8.1	Penopengan[3] data mesti digunakan untuk sebarang kawalan akses kritikal berdasarkan keperluan perkhidmatan atau perundangan yang berkenaan (jika ada)	Pengguna
5.9	**Pencegahan Kebocoran Data**	
	Objektif: Untuk mengesan dan mencegah pendedahan dan pengekstrakan maklumat yang tidak dibenarkan oleh individu atau sistem.	
5.9.1	Menggunakan kaedah pencegahan kebocoran data pada sistem kritikal, rangkaian dan peranti lain yang memproses, menyimpan atau menghantar maklumat sensitif atau PII.	Pengguna
5.10	**Pengujian Maklumat**	
	Objektif: Untuk memastikan keperluan ujian dan perlindungan maklumat operasi yang digunakan untuk ujian.	
5.10.1	Maklumat ujian mestilah mengikut perkara berikut: a. Jenis data yang akan digunakan untuk objektif ujian mesti ditentukan dan dibenarkan oleh pemilik data yang berkaitan; b. Jika ujian memerlukan maklumat sensitif RTM, maka maklumat tersebut mesti disemak dengan teliti supaya maklumat sensitif tidak didedahkan kepada pihak yang tidak dibenarkan; dan c. Data ujian mesti dikeluarkan daripada sistem ujian apabila tidak diperlukan lagi.	ICTSO, ICTO, Pentadbir Sistem ICT, Pengguna
5.11	**Perlindungan Sistem Maklumat ICT Semasa Pengujian/Pengauditan**	
	Objektif: Untuk meminimumkan kesan pengauditan dan aktiviti pengujian ke atas sistem maklumat ICT dan proses perkhidmatan yang lain.	
5.11.1	Perlindungan sistem maklumat semasa	ICTSO, ICTO,

[3] Penopengan data (*Data Masking*)

No. Polisi	Polisi	Tanggungjawab
	pengujian/pengauditan mestilah mengikut perkara berikut: a. Jejak audit (log) hendaklah diaktifkan untuk merekodkan perubahan kepada maklumat sensitif dalam semua sistem ICT , termasuk menjejaki setiap penambahan, pengubahsuaian dan pemadaman maklumat; dan b. Jejak audit (log) peristiwa keselamatan maklumat mesti disemak secara berkala dengan pengetahuan/kemahiran yang sesuai. Kekerapan semakan mesti bergantung kepada risiko yang terlibat.	Pentadbir Sistem ICT, Pengguna
5.12	**Prosedur Operasi Berdokumen**	
	Objektif: Untuk memastikan operasi yang betul dan selamat bagi sistem dan fasiliti pemprosesan maklumat ICT serta pemprosesan maklumat perkhidmatan organisasi.	
5.12.1	Prosedur operasi untuk semua pemprosesan maklumat dan kemudahan mesti didokumenkan dan disediakan kepada pengguna yang memerlukannya.	ICTO dan Pentadbir Sistem ICT
5.12.2	Prosedur pengendalian mesti menyatakan arahan yang betul untuk pelaksanaan terperinci sistem maklumat kritikal RTM termasuk rangkaian, aplikasi, pangkalan data, keselamatan ICT, storan dan sistem ICT lain.	Pengguna
5.12.3	Dokumentasi prosedur mesti dilindungi seperti berikut: a. Prosedur operasi yang didokumenkan mesti disemak dan dikemaskini apabila diperlukan; dan b. Perubahan kepada prosedur operasi yang	Pengguna

No. Polisi	Polisi	Tanggungjawab
	didokumenkan mesti dibenarkan.	
5.12.4	Dokumentasi sistem perlindungan (manual teknikal, panduan pentadbiran, manual pengguna, proses kebenaran) mesti dilaksanakan, termasuk: a. Disimpan dalam persekitaran yang selamat dan dilindungi secara fizikal daripada akses yang tidak dibenarkan; b. Disimpan dalam inventori, dan inventori mesti dikemaskini dengan kerap; c. Storan pada rangkaian awam/luar atau dibekalkan melalui rangkaian awam/luar mesti dilindungi dengan sewajarnya; dan d. Senarai pengedaran untuk dokumentasi sistem mesti disimpan pada tahap minimum dan mesti mendapat kebenaran dari pemilik proses.	Pengguna

No. Polisi	Polisi	Tanggungjawab
Seksyen 6	**PENGURUSAN PIHAK KETIGA (PEMBEKAL/PERUNDING)**	
6.1	**Keselamatan Maklumat dalam Pengurusan Pembekal**	
	Objektif: Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dalam pengurusan pembekal.	
6.1.1	Pengurusan keperluan keselamatan maklumat mestilah mengikut perkara berikut: a. Keperluan keselamatan maklumat untuk mengurangkan risiko yang berkaitan dengan kepada aset dan maklumat RTM hendaklah didokumenkan di dalam kontrak perjanjian dan dipersetujui oleh pembekal; b. Menggunapakai prinsip dan perjanjian *escrow* bagi melindungi perisian, perkakasan dan infrastruktur atau perkhidmatan awan yang kritikal (jika perlu); c. Semua keperluan keselamatan maklumat yang berkaitan mesti diwujudkan dan dipersetujui dengan setiap pembekal RTM termasuk mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan sistem, aplikasi dan komponen infrastruktur ICT; d. Menerangkan fungsi keselamatan yang dilaksanakan di dalam produk dan perkhidmatan pembekal dan konfigurasi yang diperlukan untuk operasi selamat digunakan; e. Proses pemantauan berkala dan kaedah yang boleh diterima (contoh: laporan penyelenggaraan, borang perkhidmatan) untuk mengesahkan bahawa produk dan perkhidmatan yang diberikan mematuhi keperluan perkhidmatan dan keselamatan	ICTSO, ICTO, Pentadbir Sistem ICT

No. Polisi	Polisi	Tanggungjawab
	yang dinyatakan di dalam kontrak; dan f. Perubahan kepada perkhidmatan oleh pembekal, termasuk mengekalkan dan menambahbaik polisi, prosedur dan kawalan keselamatan maklumat sedia ada, mesti diurus, dengan mengambil kira maklumat perkhidmatan, sistem dan proses yang terlibat; penilaian semula risiko hendaklah dilakukan.	
6.2	**Keselamatan Maklumat untuk Penggunaan Perkhidmatan Awan**	
	Objektif: Untuk memastikan pengurusan keselamatan maklumat yang berkesan bagi penggunaan perkhidmatan awan.	
6.2.1	Pengurusan keselamatan maklumat bagi perkhidmatan awan hendaklah mengikut perkara berikut: a. Proses yang sesuai untuk keperluan perkhidmatan keselamatan awan mesti ditentukan untuk memastikan keselamatan maklumat; b. Menyemak inventori dan perjanjian peringkat perkhidmatan awan *(Service Level Agreement)*, dan menganalisis audit keselamatan penyedia awan secara berkala; dan c. Melaksanakan pemantauan perkhidmatan awan secara berkala bagi menganalisis prestasi penyedia awan tersebut.	Pentadbir Sistem ICT, Pentadbir Rangkaian ICT

No. Polisi	Polisi	Tanggungjawab
Seksyen 7	**PENGURUSAN KESELAMATAN FIZIKAL**	
7.1	**Keselamatan Sempadan Fizikal**	
	Objektif: Untuk mengelakkan capaian fizikal yang tidak dibenarkan, kerosakan dan gangguan terhadap maklumat organisasi dan aset lain yang berkaitan.	
7.1.1	Pengurusan keselamatan fizikal mestilah mengikut perkara berikut: a. Sempadan keselamatan fizikal mesti ditakrifkan dengan jelas untuk melindungi kawasan yang mengandungi maklumat sensitif dan fasiliti pemprosesan maklumat; b. Kawasan penghantaran dan pemunggahan hendaklah direkabentuk/diletakkan supaya bekalan boleh dipunggah dan dimuatkan tanpa mendapat akses ke bilik komputer dan komunikasi premis RTM.	Pejabat Keselamatan, BKP
7.2	**Kemasukan Fizikal**	
	Objektif: Untuk memastikan hanya akses fizikal yang dibenarkan kepada maklumat organisasi dan aset lain yang berkaitan.	
7.2.1	Kemasukan ke kawasan selamat RTM mesti dikawal untuk memastikan hanya pengguna dibenarkan. Prosedur mesti mempertimbangkan untuk melaksanakan kawalan berikut: a. Pelawat dan pengguna tidak dibenarkan akses tanpa pengawasan ke kawasan selamat; dan b. Log akses fizikal (contoh: tarikh, masa masuk dan keluar, dan objektif lawatan) untuk pelawat dan pengguna mestilah direkodkan dalam buku log atau setara.	Pengguna

No. Polisi	Polisi	Tanggungjawab
7.3	**Keselamatan Pejabat, Bilik, dan Kemudahan (Fasiliti)**	
	Objektif: Untuk mengelakkan akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada maklumat organisasi dan aset lain yang berkaitan di pejabat, bilik dan kemudahan.	
7.3.1	Kawalan keselamatan hendaklah memastikan perkara berikut: a. Satu proses untuk bekerja di kawasan selamat mesti dibangunkan dan dilaksanakan;	Pengguna
	b. Sebarang dokumentasi mengenai kemudahan pemprosesan maklumat sensitif atau direktori telefon dalaman mesti disimpan dengan selamat; dan	Pengarah Bahagian
	c. Semua peralatan elektronik (contoh: pelayan, storan, desktop, komputer riba) dan peralatan komunikasi (contoh: suis, hab, penghala (*router)*, tembok api *(firewall),* dsb.) mesti disimpan di lokasi yang selamat.	Pegawai Aset, Pentadbir Sistem ICT
	d. Memastikan keselamatan pejabat adalah selamat dari dicerobohi.	Warga RTM
7.4	**Pemantauan Keselamatan Fizikal**	
	Objektif: Untuk mengesan dan menghalang akses fizikal yang tidak dibenarkan.	
7.4.1	Akses kepada bangunan yang menempatkan sistem kritikal harus dipantau secara berterusan oleh sistem pengawasan bagi mengesan akses yang tidak dibenarkan atau tingkah laku yang mencurigakan. Contoh sistem pengawasan: pengawal, penggera penceroboh, sistem pemantauan video seperti televisyen litar tertutup (CCTV) dan perisian pengurusan maklumat keselamatan fizikal yang diuruskan secara	Pentadbir Pusat Data dan BKP

No. Polisi	Polisi	Tanggungjawab
	dalaman atau oleh penyedia perkhidmatan pemantauan.	
7.5	**Perlindungan Terhadap Ancaman Fizikal dan Alam Sekitar**	
	Objektif: Untuk mencegah atau mengurangkan akibat kejadian yang berpunca daripada ancaman fizikal dan alam sekitar.	
7.5.1	Perlindungan fizikal terhadap ancaman kebakaran, banjir, letupan dan kerosakan pergolakan awam mestilah dibangunkan.	BKP
7.5.2	Perlindungan peralatan ICT daripada ancaman fizikal dan alam sekitar mestilah mengikut perkara berikut: a. Peralatan ICT yang berada di Bilik Pelayan mesti diletakkan dengan sewajarnya dan dilindungi daripada ancaman dan bahaya alam sekitar (contoh: kebakaran, asap, banjir, habuk, gangguan bekalan elektrik) dan akses tanpa kebenaran (contoh: kecurian) untuk memastikan peralatan berterusan dalam operasi; dan b. Semua peralatan ICT mesti diselenggara secara berkala dan spesifikasi perkhidmatan yang disyorkan oleh pembekal.	Pentadbir Pusat Data dan BKP
7.6	**Bekerja di Kawasan Selamat**	
	Objektif: Untuk melindungi maklumat dan aset yang berkaitan di kawasan pejabat dan selamat daripada kerosakan dan gangguan oleh pengguna lain.	
7.6.1	Semua pengguna yang diberi kebenaran mestilah memakai pengenalan yang boleh dilihat apabila memasuki semua kawasan selamat.	Pentadbir Sistem ICT dan BKP
7.7	**Meja Kosong dan Skrin Kosong *(Clear Desk dan Clear Screen)***	
	Objektif: Untuk mengurangkan risiko akses tanpa kebenaran, kehilangan dan kerosakan maklumat pada meja, skrin dan di lokasi lain yang boleh diakses semasa dan di luar waktu kerja biasa.	

No. Polisi	Polisi	Tanggungjawab
7.7.1	Polisi meja kosong untuk dokumen kertas dan media storan boleh-alih dan skrin kosong untuk peralatan pemprosesan maklumat hendaklah diamalkan. Polisi ini bermaksud tidak meninggalkan dan mendedahkan bahan-bahan/dokumen yang sensitif sama ada atas meja pengguna atau di paparan skrin peralatan ICT apabila pengguna tidak berada di tempatnya.	Pengguna
7.8	**Perlindungan Peralatan**	
	Objektif: Untuk mengurangkan risiko peralatan daripada ancaman fizikal dan alam sekitar, kerosakan dan akses yang tidak dibenarkan.	
7.8.1	Lokasi dan kedudukan peralatan mestilah mematuhi peraturan/keperluan kesihatan dan keselamatan.	Pengguna
7.9	**Keselamatan Aset Luar Premis**	
	Objektif: Untuk mengelakkan kehilangan, kerosakan, kecurian atau kompromi peranti luar tapak dan gangguan kepada operasi organisasi.	
7.9.1	Keselamatan aset di luar premis mesti dilindungi seperti berikut: a. Peralatan, maklumat atau perisian tidak boleh dibawa keluar dari premis tanpa kebenaran terlebih dahulu; dan b. Kawalan keselamatan mesti dikenakan ke atas aset lain dengan mengambil kira risiko yang berbeza untuk bekerja di luar premis RTM.	Pengguna
7.10	**Utiliti Sokongan**	
	Objektif: Untuk mengelakkan kehilangan, kerosakan atau kompromi maklumat dan aset lain yang berkaitan, atau gangguan kepada operasi organisasi akibat kegagalan dan gangguan utiliti sokongan.	
7.10.1	Utiliti sokongan mesti dilindungi daripada	Pengguna

No. Polisi	Polisi	Tanggungjawab
	kehilangan, kerosakan atau kompromi atau gangguan seperti berikut: a. Peralatan mesti dilindungi daripada kegagalan dan gangguan lain utiliti sokongan; dan b. Semua utiliti sokongan, seperti elektrik, bekalan air, kumbahan, pemanasan/pengudaraan, dan penghawa dingin, mestilah mencukupi untuk sistem yang disokongnya.	
7.11	**Keselamatan Kabel**	
	Objektif: Untuk mengelakkan kehilangan, kerosakan, kecurian atau kompromi maklumat dan aset lain yang berkaitan dan gangguan kepada operasi organisasi yang berkaitan dengan kabel kuasa dan komunikasi.	
7.11.1	Keselamatan kabel mesti dilindungi daripada pemintasan, gangguan atau kerosakan seperti berikut: a. Kabel rangkaian mesti dilindungi daripada pemintasan atau kerosakan yang tidak dibenarkan akibat bahaya alam sekitar, contohnya, dengan menggunakan saluran atau dengan mengelak laluan melalui kawasan awam; b. Kabel kuasa mesti diasingkan daripada kabel komunikasi untuk mengelakkan gangguan; c. Kabel mesti dilabel dengan jelas untuk meminimumkan ralat tidak sengaja; dan d. Jenis pengikat kabel yang betul mesti digunakan mengikut jenis kabel.	Pentadbir Sistem ICT

No. Polisi	Polisi	Tanggungjawab
Seksyen 8	**PENGURUSAN IDENTITI DAN AKSES**	
8.1	**Kawalan Akses**	
	Objektif: Untuk memastikan akses yang dibenarkan dan untuk menghalang capaian yang tidak dibenarkan kepada maklumat dan aset lain yang berkaitan.	
8.1.1	Menentukan peraturan kawalan akses yang sesuai, hak akses dan sekatan untuk peranan pengguna tertentu terhadap aset mereka.	Pemilik perkhidmatan digital dan Pentadbir Sistem ICT.
8.1.2	a. Mematuhi pengurusan kata laluan dan kaedah log masuk dan polisi kawalan akses yang dibenarkan. b. Pengurusan kata laluan mestilah mematuhi amalan terbaik yang ditetapkan oleh RTM	ICTSO, ICTO, Pentadbir Sistem ICT, Pengguna
8.1.3	a. Sistem pengurusan kata laluan hendaklah interaktif dan mengambilkira kualiti kata laluan yang dicipta. b. Panjang kata laluan mestilah sekurang-kurangnya **DUA BELAS (12) AKSARA** dengan gabungan antara huruf, aksara khas dan nombor (alphanumeric), **KECUALI** bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad. c. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara.	ICTSO, ICTO, Pentadbir Sistem ICT, Pengguna
8.2	**Pengurusan Identiti**	
	Objektif: Untuk membenarkan pengenalan unik individu bagi mengakses sistem maklumat organisasi dan aset lain yang berkaitan serta membolehkan penyerahan hak akses yang sesuai.	
8.2.1	Prosedur untuk pendaftaran pengguna dan penyah daftaran mesti ditakrifkan, didokumenkan dan dilaksanakan untuk memberikan akses kepada semua sistem maklumat/ICT.	Pentadbir Sistem ICT

No. Polisi	Polisi	Tanggungjawab
8.3	**Maklumat Pengesahan Entiti**	
	Objektif: Untuk memastikan pengesahan entiti yang betul dan mencegah kegagalan proses pengesahan.	
8.3.1	Menentukan dan mengekalkan senarai kawalan akses untuk aplikasi dan data.	Pemilik perkhidmatan digital dan Pentadbir Sistem ICT
8.4	**Hak Akses**	
	Objektif: Untuk memastikan akses kepada maklumat dan aset lain yang berkaitan ditakrifkan dan dibenarkan mengikut keperluan perkhidmatan.	
8.4.1	Proses peruntukan untuk menyerahkan atau membatalkan hak akses fizikal dan sistem ICT yang diberikan kepada identiti pengguna mestilah termasuk: a. Hak akses pengguna mesti disemak dengan kerap, dan kekerapan semakan mesti bergantung pada risiko yang terlibat. Contoh: kebenaran untuk hak akses istimewa mesti disemak lebih kerap daripada hak akses pengguna biasa; b. Hak capaian semua pengguna kepada kemudahan pemprosesan maklumat dan maklumat mesti dihapuskan selepas penamatan pekerjaan, kontrak, atau perjanjian mereka atau diselaraskan apabila bertukar; dan c. Hak akses pengguna kepada aplikasi dan data mesti diwujudkan dan dikekalkan setelah menerima permintaan bertulis yang diluluskan.	Pentadbir Sistem ICT
8.5	**Hak Akses Istimewa**	

No. Polisi	Polisi	Tanggungjawab
	Objektif: Untuk memastikan hanya pengguna yang dibenarkan, komponen perisian dan perkhidmatan disediakan dengan hak akses istimewa.	
8.5.1	ID Pengguna dengan keistimewaan sistem khas mesti dikawal dan dihadkan kepada bilangan pengguna yang terhad; Contoh: ID pentadbir yang digunakan untuk mentadbir, mengubahsuai kepada pengendalian sistem, fungsi keselamatan dan log audit.	ICTSO dan Pentadbir Sistem ICT
8.6	**Sekatan Capaian Maklumat**	
	Objektif: Untuk memastikan hanya akses yang dibenarkan dan untuk menghalang capaian yang tidak dibenarkan kepada maklumat dan aset lain yang berkaitan.	
8.6.1	a. Pentadbir sistem mestilah log masuk sebagai diri mereka sendiri, menggunakan ID pengguna semasa menjalankan tugas kerja biasa dan bukannya log masuk sebagai Penyelia/Pentadbir; dan b. Log masuk sebagai Penyelia/Pentadbir sistem mestilah terhad kepada aktiviti pentadbiran sahaja.	ICTSO, ICTO, Pentadbir Sistem ICT, Pengguna
8.7	**Pengesahan Selamat**	
	Objektif: Untuk memastikan pengguna atau entiti disahkan dengan selamat, apabila mengakses sistem ICT, aplikasi dan rangkaian perkhidmatan diberikan.	
8.7.1	Akses kepada perkhidmatan maklumat mesti dikawal dengan menggunakan 'ID Pengguna' unik supaya pengguna boleh dikaitkan dan bertanggungjawab ke atas tindakan mereka.	ICTSO, ICTO, Pentadbir Sistem ICT

No. Polisi	Polisi	Tanggungjawab
Seksyen 9	**PENGURUSAN ANCAMAN DAN KERENTANAN**	
9.1	**Kecerdasan Ancaman *(Threat intelligence)***	
	Objektif: Memberi kesedaran tentang persekitaran ancaman organisasi supaya tindakan mitigasi yang sewajarnya dapat diambil.	
9.1.1	Menyediakan maklumat tentang ancaman yang sedia ada atau yang berkemungkinan dikumpul dan dianalisis untuk memudahkan tindakan yang lebih berkesan.	Pengguna
9.2	**Pengurusan Kelemahan Teknikal**	
	Objektif: Untuk mengelakkan eksploitasi kelemahan teknikal kepada sistem, aplikasi, pangkalan data dan rangkaian ICT.	
9.2.1	Pengurusan kelemahan teknikal mestilah mengikut perkara berikut: a. Mewujudkan dan mengekalkan sumber kelemahan teknikal terkini dan tampalan/pembetulan/*patch* senarai yang dikeluarkan untuk semua sistem ICT; b. Pengurusan *patch* mesti dibangunkan, dan risiko yang berkaitan dengan pemasangan *patch* mesti dinilai (risiko yang ditimbulkan oleh kelemahan harus dibandingkan dengan risiko memasang *patch*); c. Peranan dan tanggungjawab untuk pemantauan kerentanan, penilaian risiko kerentanan, inventori aplikasi, dan sebarang tanggungjawab penyelarasan lain yang diperlukan mesti ditakrifkan dan didokumenkan; dan d. Keperluan audit dan aktiviti yang melibatkan pengesahan sistem operasi	Pentadbir Sistem ICT dan CERT RTM

No. Polisi	Polisi	Tanggungjawab
	mesti dirancang dan dipersetujui untuk meminimumkan gangguan kepada proses perkhidmatan.	

No. Polisi	Polisi	Tanggungjawab
Seksyen 10	**PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT**	
10.1	**Perancangan Insiden Keselamatan Maklumat**	
	Objektif: Untuk memastikan tindak balas yang cepat, berkesan, konsisten dan teratur terhadap insiden keselamatan maklumat, termasuk komunikasi mengenai insiden keselamatan maklumat.	
10.1.1	Tanggungjawab dan prosedur pengurusan mesti diwujudkan untuk memastikan tindak balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat.	ICTSO, CERT RTM dan Pemilik Projek/Sistem Aplikasi
10.2	**Penilaian dan Keputusan Insiden Keselamatan Maklumat**	
	Objektif: Untuk memastikan pengkategorian dan keutamaan insiden keselamatan maklumat yang berkesan.	
10.2.1	Penilaian dan keputusan mengenai insiden keselamatan maklumat mestilah mengikut perkara berikut: a. Insiden keselamatan maklumat mestilah dinilai dan diputuskan jika ia akan diklasifikasikan sebagai insiden sebenar keselamatan maklumat; b. Keputusan penilaian dan keputusan hendaklah direkodkan secara terperinci untuk tujuan rujukan dan pengesahan masa hadapan; dan c. Membangunkan prosedur untuk proses mengenalpasti, mengumpul, memperoleh dan memelihara maklumat yang boleh menjadi bukti.	ICTSO
10.3	**Tindakbalas Terhadap Insiden Keselamatan Maklumat**	
	Objektif: Untuk memastikan tindak balas yang cekap dan berkesan terhadap insiden keselamatan maklumat.	
10.3.1	Prosedur tindak balas insiden keselamatan maklumat hendaklah didokumenkan.	ICTSO, CERT RTM

10.4	**Pengajaran dari Insiden Keselamatan Maklumat**	
	Objektif: Untuk mengurangkan kemungkinan atau akibat insiden masa hadapan.	
10.4.1	Pengetahuan yang diperoleh daripada menganalisis dan menyelesaikan insiden keselamatan maklumat mesti digunakan untuk mengurangkan kemungkinan atau kesan insiden masa hadapan.	ICTSO, CERT RTM
10.5	**Pengumpulan Bukti Insiden Keselamatan Maklumat**	
	Objektif: Untuk memastikan pengurusan bukti yang konsisten dan berkesan berkaitan insiden keselamatan maklumat bagi mengambil tindakan tatatertib dan undang-undang.	
10.5.1	Mewujudkan dan melaksanakan prosedur untuk mengenal pasti, mengumpul, memperoleh dan memelihara bukti yang berkaitan dengan insiden keselamatan maklumat.	ICTSO, CERT RTM
10.6	**Pelaporan Insiden Keselamatan Maklumat**	
	Objektif: Untuk menyokong pelaporan tepat pada masanya, konsisten dan berkesan tentang insiden keselamatan maklumat yang boleh dikenal pasti oleh pengguna.	
10.6.1	Insiden keselamatan maklumat mesti dilaporkan melalui saluran pengurusan yang sesuai dengan cepat.	ICTSO, CERT RTM
10.6.2	Melaporkan sebarang kelemahan keselamatan maklumat yang diperhatikan atau disyaki dalam sistem atau perkhidmatan.	ICTSO, CERT RTM
10.7	**Maklumat Log Sistem ICT**	
	Objektif: Untuk merekodkan insiden, menjana bukti, memastikan integriti maklumat log, mencegah capaian yang tidak dibenarkan, mengenal pasti insiden keselamatan maklumat yang boleh menyokong penyiasatan.	
10.7.1	Log yang merekodkan aktiviti, pengecualian, kesalahan dan insiden lain yang berkaitan mesti dihasilkan, disimpan, dilindungi dan dianalisis seperti berikut: a. Peralatan dan maklumat log hendaklah	Pentadbir Sistem ICT

	dilindungi sewajarnya daripada gangguan dan capaian yang tidak dibenarkan; b. Log audit yang mengandungi semua maklumat yang berkaitan mesti disimpan, terutamanya untuk perubahan kepada program operasi; dan c. Log aktiviti pentadbir dan pengendali mesti direkod, dan semakan dijalankan untuk mengekalkan akauntabiliti bagi pengguna yang mempunyai keistimewaan.	
10.8	**Pemantauan Aktiviti ICT**	
	Objektif: Untuk mengesan tingkah laku anomali dan kemungkinan insiden keselamatan maklumat.	
10.8.1	Memastikan alat pemantauan automatik dipasang untuk mencatat aktiviti dan pelanggaran keselamatan terhadap data pengeluaran yang kritikal dan sensitif; Alat automatik ini mesti diluluskan dan diuji secara meluas sebelum penggunaan.	Pentadbir Sistem ICT dan CERT RTM
10.9	**Penyegerakan Jam**	
	Objektif: Untuk membolehkan korelasi dan analisis insiden berkaitan keselamatan dan data lain yang direkodkan bagi menyokong penyiasatan terhadap insiden keselamatan maklumat.	
10.9.1	Jam sistem (iaitu, jam masa nyata dalam komputer atau peranti komunikasi) mesti disegerakkan merentasi rangkaian dalaman RTM.	Pentadbir Sistem ICT

No. Polisi	Polisi	Tanggungjawab
Seksyen 11	**PENGURUSAN KESINAMBUNGAN PERKHIDMATAN**	
11.1	**Keselamatan Maklumat Semasa Gangguan**	
	Objektif: Untuk melindungi maklumat dan aset lain yang berkaitan semasa gangguan.	
11.1.1	a. Prosedur dan tanggungjawab mesti diwujudkan untuk memastikan tindak balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat; dan b. Kesinambungan keselamatan maklumat mesti dimasukkan dalam pelan dan prosedur pengurusan kesinambungan perkhidmatan RTM.	Direktorat RTM
11.2	**Penyediaan ICT bagi Kesinambungan Perkhidmatan**	
	Objektif: Untuk memastikan ketersediaan maklumat organisasi dan aset lain yang berkaitan semasa gangguan.	
11.2.1	Pelan Pemulihan Bencana (DRP) mesti dibangunkan dan diselenggara untuk menyokong pelan kesinambungan perkhidmatan (PKP) RTM.	Koordinator PKP, Pasukan Tindak Balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT
11.2.2	a. Mewujudkan, mendokumentasikan, melaksana dan menyelenggara proses, prosedur dan kawalan untuk memastikan tahap kesinambungan yang diperlukan untuk keselamatan maklumat semasa situasi buruk; dan b. Mengesahkan kawalan kesinambungan keselamatan maklumat yang telah ditetapkan dan dilaksanakan pada selang	Pengurus Bahagian Pengarah Negeri

No. Polisi	Polisi	Tanggungjawab
	masa yang tetap untuk memastikan ia sah dan berkesan semasa situasi buruk.	
11.3	**Pengurusan Kapasiti**	
	Objektif: Untuk memastikan kapasiti yang diperlukan oleh fasiliti pemprosesan maklumat (ICT), sumber manusia, pejabat dan kemudahan lain.	
11.3.1	Prosedur perancangan kapasiti mestilah ditakrifkan, didokumenkan dan dilaksanakan untuk mengekalkan tahap perkhidmatan yang mencukupi untuk sistem maklumat kritikal RTM	Pemilik Sistem, Pentadbir Sistem ICT
11.4	**Sandaran Maklumat (*Back-up*)**	
	Objektif: Untuk membolehkan pemulihan daripada kehilangan data atau sistem ICT.	
11.4.1	a. Prosedur sandaran dan pemulihan *(recovery)* mestilah didokumenkan untuk aplikasi dan data kritikal perkhidmatan RTM; b. Maklumat kritikal perkhidmatan mesti disandarkan di luar premis utama, dipisahkan dari premis utama. c. Bilik penyimpanan di luar premis utama mestilah mempunyai perlindungan fizikal dan alam sekitar yang sesuai; contoh: Pusat Pemulihan Bencana (penyedia luar), Perkhidmatan Awan; dan d. Media sandaran mesti diuji secara berkala untuk memastikan keupayaan untuk memulihkan data sandaran.	Pentadbir Sistem ICT
11.4.2	Menentukan keperluan sandaran bergantung pada klasifikasi dan keperluan data dan mengesahkan kepada Pentadbir Sistem ICT.	Pemilik Sistem

No. Polisi	Polisi	Tanggungjawab
11.5	**Replikasi Fasiliti Pemprosesan Maklumat**	
	Objektif: Untuk memastikan fasilitasi kemudahan pemprosesan maklumat terus beroperasi.	
11.5.1	Replikasi fasilitasi pemprosesan maklumat mestilah mengikut perkara berikut: a. Fasiliti pemprosesan maklumat (ICT) mesti dilaksanakan untuk memenuhi keperluan ketersediaan; dan b. Fasiliti pemprosesan maklumat (ICT) (termasuk infrastruktur, sistem, aplikasi, pangkalan data dan storan) hendaklah diuji untuk memastikan failover dari satu komponen ke komponen lain berfungsi dengan baik.	Pentadbir Pusat Data, Pemilik Perkhidmatan dan Pentadbir Sistem ICT

No. Polisi	Polisi	Tanggungjawab
Seksyen 12	**PEMATUHAN DAN UNDANG-UNDANG**	
12.1	**Keperluan Undang-undang, Berkanun, Kawal Selia dan Kontrak**	
	Objektif: Untuk memastikan pematuhan kepada keperluan undang-undang, berkanun, peraturan dan kontrak yang berkaitan dengan keselamatan maklumat.	
12.1.1	Senarai akta yang berkenaan, perundangan, kewajipan kontrak dan keperluan keselamatan mesti dibangunkan.	Pengguna
12.2	**Hak harta Intelek**	
	Objektif: Untuk memastikan pematuhan terhadap keperluan undang-undang, berkanun, peraturan dan kontrak yang berkaitan dengan hak harta intelek dan penggunaan produk proprietari.	
12.2.1	Memastikan penggunaan bahan berkenaan dengan Hak Harta Intelek (control: hak cipta, lesen perisian, tanda dagangan, hak reka bentuk dan sebagainya) dipatuhi dengan keperluan undang-undang, statutori, peraturan dan kontrak yang berkaitan.	Pengguna
12.2.2	Hak harta intelek bagi program perisian, dokumentasi dan maklumat lain yang dijana oleh atau disediakan oleh pengguna dan pembekal RTM mestilah menjadi hak milik RTM.	Pengarah Bahagian
12.3	**Privasi dan Perlindungan Maklumat Pengenalan Peribadi**	
	Objektif: Untuk memastikan pematuhan kepada keperluan undang-undang, berkanun, peraturan dan kontrak yang berkaitan dengan aspek keselamatan maklumat perlindungan PII.	
12.3.1	Maklumat peribadi hendaklah dikenalpasti dan diuruskan bagi mematuhi Akta Perlindungan Data Peribadi (PDPA), Standard dan Garis Panduan Kerajaan Malaysia.	Pengguna

No. Polisi	Polisi	Tanggungjawab
12.4	**Pematuhan dengan Polisi, Prosedur, Peraturan dan Standard untuk Keselamatan Maklumat**	
	Objektif: Untuk memastikan keselamatan maklumat dilaksanakan dan dikendalikan mengikut polisi keselamatan maklumat organisasi, prosedur, peraturan dan standard yang ditetapkan.	
12.4.1	Pematuhan terhadap prosedur operasi dan keselamatan maklumat hendaklah dikaji semula mengikut polisi keselamatan maklumat, standard dan pekeliling/peraturan keselamatan lain.	Pengarah Bahagian
12.4.2	Prosedur sistem maklumat ICT yang dilaksanakan mestilah sentiasa disemak untuk mematuhi polisi keselamatan maklumat organisasi dan standard yang bersesuaian.	ICTO

No. Polisi	Polisi	Tanggungjawab
Seksyen 13	**PENGURUSAN KESELAMATAN RANGKAIAN**	
13.1	**Telekerja *(Remote working)***	
	Objektif: Untuk memastikan keselamatan maklumat apabila pengguna bekerja dari jauh.	
13.1.1	a. Kawalan keselamatan hendaklah sentiasa digunakan untuk melindungi daripada risiko menggunakan kemudahan pengkomputeran dan komunikasi mudah alih ketika bekerja dari luar pejabat. b. Prosedur untuk mendapatkan dan menggunakan kemudahan pengkomputeran mudah alih dengan sewajarnya mesti diwujudkan dan dilaksanakan.	Warga RTM
13.1.2	a. Kawalan keselamatan mesti dilaksanakan untuk melindungi maklumat yang diakses, diproses atau disimpan semasa telekerja. b. Menggunakan ID pengguna dan kata laluan yang sah untuk mengakses perkhidmatan RTM melalui Internet.	Pengguna
13.2	**Pengurusan Konfigurasi**	
	Objektif: Untuk memastikan perkakasan, perisian dan perkhidmatan rangkaian berfungsi dengan betul dengan tetapan keselamatan yang diperlukan, dan konfigurasi tidak diubah oleh perubahan yang tidak dibenarkan atau tidak betul.	
13.2.1	Mentakrif dan melaksanakan proses dan peralatan untuk menguatkuasakan konfigurasi yang ditetapkan (termasuk konfigurasi keselamatan) ke atas perkakasan, perisian, perkhidmatan dan sistem operasi rangkaian sepanjang hayatnya.	SAICT/MTA

No. Polisi	Polisi	Tanggungjawab
13.3	**Penggunaan Program Utiliti[4]**	
	Objektif: Untuk memastikan penggunaan program utiliti tidak membahayakan rangkaian dan keselamatan maklumat.	
13.3.1	Penggunaan program utiliti bagi menguruskan operasi rangkaian dan keselamatan mestilah dikawal.	ICTSO, Pentadbir Sistem ICT
13.4	**Keselamatan Rangkaian**	
	Objektif: Untuk melindungi maklumat dalam rangkaian dan fasilitasi pemprosesan maklumat rangkaian.	
13.4.1	a. Rangkaian mesti diurus dan dikawal untuk melindungi maklumat dalam sistem dan aplikasi. b. Akses kepada dokumentasi senibina rangkaian RTM, seperti rajah senibina rangkaian, inventori infrastruktur, fail konfigurasi, dsb., mestilah dihadkan kepada pengguna yang dibenarkan sahaja.	ICTSO, Pentadbir Sistem Rangkaian
	Keselamatan Perkhidmatan Rangkaian[5]	
	Objektif: Untuk memastikan keselamatan dalam penggunaan perkhidmatan rangkaian.	
13.5.1	Keselamatan perkhidmatan rangkaian mestilah mengikut perkara berikut: a. Mekanisme keselamatan, tahap perkhidmatan dan keperluan pengurusan semua perkhidmatan rangkaian mesti dikenalpasti dan dimasukkan dalam perjanjian perkhidmatan rangkaian sama ada perkhidmatan ini disediakan secara dalaman atau penyedia luar;	ICTSO, Pentadbir Sistem Rangkaian dan Pihak Ketiga

[4] Program utiliti ialah sebarang perisian yang direka untuk menganalisis atau menyelenggara sistem atau rangkaian komputer. Contoh: Alat diagnostik, program antivirus, defragmenter cakera, perisian sandaran, alat rangkaian dsb.

[5] 'Perkhidmatan Rangkaian' adalah aplikasi yang dijalankan pada lapisan aplikasi rangkaian menggunakan protokol rangkaian seperti *Domain Name System, Internet Protocol, World Wide Web, e-Mail, File Server* dsb.

No. Polisi	Polisi	Tanggungjawab
	b. Risiko keselamatan yang berkaitan dengan perkhidmatan rangkaian mesti dinilai untuk mencapai keperluan keselamatan; c. Sebarang perkhidmatan rangkaian yang tidak digunakan atau tidak diperlukan mesti dikeluarkan atau dilumpuhkan; dan d. Tahap perkhidmatan untuk semua perkhidmatan rangkaian kritikal mesti dikenalpasti dan dipantau secara berkala.	
13.6	**Pengasingan Rangkaian**	
	Objektif: Untuk memisahkan rangkaian dalaman sempadan keselamatan dan untuk mengawal lalu lintas antara mereka berdasarkan keperluan perkhidmatan.	
13.6.1	a. Perkhidmatan maklumat, pengguna dan sistem maklumat RTM mesti diasingkan pada rangkaian melalui LAN Maya (VLAN) dan mesti dikawal pada perimeter menggunakan *Gateway* (contoh: *firewall, router*); b. Rangkaian tanpa-wayar yang digunakan untuk penghantaran data mesti sentiasa dikonfigurasikan dengan *firewall* untuk menapis komunikasi dengan peranti jauh; c. Semua sambungan rangkaian tanpa-wayar mesti disahkan sebelum memberikan akses kepada rangkaian dalaman/ *intranet* RTM; d. *Wireless Access Point* (WAP) mesti ditempatkan di kawasan selamat secara fizikal di dalam premis RTM; dan e. Pengimbasan berkala mesti dijalankan untuk mencari akses WAP yang tidak dibenarkan.	ICTSO dan Pentadbir Sistem Rangkaian

No. Polisi	Polisi	Tanggungjawab
13.7	**Penapisan Laman (Web)**	
	Objektif: Untuk melindungi sistem daripada dikompromi oleh perisian hasad dan untuk menghalang akses kepada sumber *web* yang tidak dibenarkan.	
13.7.1	a. Menggunakan kaedah tertentu bagi mengurangkan risiko pengguna mengakses laman web yang mengandungi maklumat haram atau diketahui mengandungi virus atau bahan pancingan data; dan b. Mengenal pasti laman web yang patut atau tidak boleh diakses oleh pengguna.	Pentadbir Laman Web
13.8	**Penggunaan Kriptografi**	
	Objektif: Untuk memastikan penggunaan kriptografi yang betul dan berkesan untuk melindungi kerahsiaan dan integriti maklumat mengikut keperluan keselamatan perkhidmatan dan maklumat, dengan mengambil kira keperluan undang-undang, berkanun, peraturan dan kontrak yang berkaitan dengan kriptografi.	
13.8.1	Penggunaan kawalan kriptografi untuk perlindungan maklumat mesti dibangunkan dan dilaksanakan sepanjang kitaran hayat aset ICT.	Warga RTM dan ICTO

No. Polisi	Polisi	Tanggungjawab
Seksyen 14	**PENGURUSAN KESELAMATAN SISTEM DAN APLIKASI**	
14.1	**Akses kepada kod sumber**	
	Objektif: Untuk mengelakkan fungsi yang tidak dibenarkan, perubahan yang tidak disengajakan atau berniat jahat bagi mengekalkan kerahsiaan harta intelek yang berharga.	
14.1.1	a. Akses baca dan tulis kepada kod sumber, alat pembangunan (*development tools*) dan perpustakaan perisian (*software libraries*) hendaklah diuruskan dengan baik; b. Akses kepada kod sumber program dan item yang berkaitan (seperti reka bentuk, spesifikasi, pelan penentusahan (*verification*) dan pelan pengesahsahihan (*validation*) mesti dikawal untuk menghalang perubahan fungsi yang tidak dibenarkan dan yang tidak disengajakan serta mengekalkan kerahsiaan harta intelek; dan c. Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik RTM.	Pengarah Projek, Pengurus Projek dan Pentadbir Sistem ICT
14.2	**Pengurusan Konfigurasi**	
	Objektif: Untuk memastikan perkakasan, perisian dan perkhidmatan sistem dan aplikasi berfungsi dengan betul dengan tetapan keselamatan yang diperlukan, dan konfigurasi tidak diubah oleh perubahan yang tidak dibenarkan atau tidak betul.	
14.2.1	a. Konfigurasi, termasuk konfigurasi keselamatan, perkakasan, perisian, perkhidmatan (contoh: perkhidmatan awan) sistem dan aplikasi hendaklah diwujudkan, didokumenkan, dilaksanakan, disemak dan dipantau. b. Peranan, tanggungjawab dan prosedur hendaklah memastikan kawalan yang berkesan untuk semua perubahan	SAICT/MTA

	konfigurasi.	
14.3	**Penggunaan Kriptografi**	
	Objektif: Untuk memastikan penggunaan kriptografi yang betul dan berkesan untuk melindungi kerahsiaan, integriti maklumat mengikut keperluan keselamatan perkhidmatan dan maklumat serta menyokong keperluan undang-undang, berkanun, peraturan dan kontrak yang berkaitan dengan kriptografi.	
14.3.1	a. Peraturan untuk penggunaan kriptografi yang berkesan, termasuk pengurusan kunci kriptografi, hendaklah ditakrifkan dan dilaksanakan; b. Menggunakan teknik kriptografi yang berkesan apabila maklumat sensitif/kritikal merentas sempadan ke luar dari organisasi; dan c. Mengadakan kandungan perjanjian atau kontrak peringkat perkhidmatan dengan pembekal luar perkhidmatan kriptografi (*Certification Authority*) hendaklah meliputi isu liabiliti, kebolehpercayaan perkhidmatan dan tindakbalas masa untuk penyediaan perkhidmatan.	Pengarah Projek
14.4	**Pemasangan Perisian Pada Sistem Operasi**	
	Objektif: Untuk memastikan integriti sistem operasi dan mencegah eksploitasi kelemahan teknikal.	
14.4.1	Pemasangan perisian mestilah mengikut perkara berikut: a. Keperluan untuk aplikasi atau perisian baharu mesti dikenal pasti dan didokumenkan; b. Semakan berkala terhadap penggunaan perisian pada desktop, komputer riba dan pelayan RTM mestilah dijalankan untuk memastikan penggunaan perisian yang	Pentadbir Sistem ICT, Pengguna

	dibenarkan dan pematuhan dengan perjanjian pelesenan yang berkaitan; c. Prosedur dan kawalan keselamatan hendaklah dilaksanakan untuk mengurus pemasangan perisian sistem operasi dengan selamat; dan d. Bagi menaik taraf kepada produk perisian baharu, hendaklah mengambil kira keperluan perkhidmatan untuk perubahan dan keselamatan produk tersebut (contoh: fungsi keselamatan maklumat baharu atau kelemahan keselamatan maklumat yang menjejaskan versi semasa).	
14.4.2	Perisian tulen RTM mesti dilindungi seperti berikut: a. Tidak dibenarkan mengedarkan sebarang perisian berlesen RTM; b. Semua bentuk perisian untuk kegunaan peribadi adalah tidak dibenarkan; c. Tidak dibenarkan memuat turun, memasang dan menggunakan perisian yang tidak dibekalkan oleh RTM; dan d. Melaporkan kepada SAICT/MTA jika terdapat masalah semasa menggunakan perisian yang dimiliki oleh RTM.	Pentadbir Sistem ICT, Pengguna
14.5	**Kitaran Hayat Pembangunan Yang Selamat**	
	Objektif: Untuk memastikan keselamatan maklumat direka dan dilaksanakan dalam kitaran hayat pembangunan perisian dan sistem yang selamat.	
14.5.1	Pembangunan perisian dan sistem yang selamat mesti diwujudkan dan digunakan termasuk: a. Pembangunan selamat ialah keperluan untuk membina perkhidmatan, senibina, perisian dan sistem yang selamat (iaitu,	Pentadbir Sistem ICT

	keselamatan dalam kitaran hayat pembangunan perisian); b. Perubahan kepada sistem dalam kitaran hayat pembangunan mesti dikawal dengan menggunakan prosedur kawalan perubahan formal; c. Apabila platform pengendalian ditukar, aplikasi kritikal perkhidmatan mesti disemak dan diuji untuk memastikan tiada kesan buruk terhadap operasi atau keselamatan organisasi; dan d. Pengubahsuaian pada pakej perisian dan semua perubahan mesti dikawal dengan ketat.	
14.6	**Keperluan Keselamatan Aplikasi**	
	Objektif: Untuk memastikan semua keperluan keselamatan maklumat dikenalpasti dan ditangani semasa membangunkan atau memperolehi aplikasi.	
14.6.1	Keperluan keselamatan aplikasi mestilah mengikut perkara berikut: a. Keperluan berkaitan keselamatan maklumat mesti dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan kepada sistem maklumat sedia ada; b. Maklumat yang terlibat dalam perkhidmatan aplikasi yang melalui rangkaian awam/luar mesti dilindungi daripada aktiviti penipuan, pertikaian kontrak, dan pendedahan dan pengubahsuaian tanpa kebenaran; dan c. Maklumat dalam urus niaga perkhidmatan aplikasi mesti dilindungi untuk mengelakkan penghantaran yang tidak lengkap, salah laluan, pengubahan mesej yang tidak	ICTSO, ICTO dan Pentadbir Sistem ICT

	dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau main semula.	
14.7	**Senibina Sistem Selamat Dan Prinsip Kejuruteraan**	
	Objektif: Untuk memastikan sistem maklumat direka bentuk, dilaksanakan dan dikendalikan dengan selamat dalam kitaran hayat pembangunan.	
14.7.1	Senibina sistem dan prinsip kejuruteraan mesti dilindungi seperti berikut: a. Keselamatan mesti direkabentuk ke dalam semua lapisan senibina (*business*, data, aplikasi dan teknologi), mengimbangi keperluan untuk keselamatan maklumat dengan keperluan untuk kebolehcapaian; dan b. Persekitaran pembangunan yang selamat untuk pembangunan sistem dan usaha penyepaduan yang meliputi keseluruhan kitaran hayat pembangunan sistem mesti diwujudkan.	ICTSO, ICTO dan Pentadbir Sistem ICT
14.7.2	Prinsip kejuruteraan sistem yang selamat termasuk, tapi tidak terhad kepada: a. Menyediakan panduan mengenai kaedah pengesahan pengguna; b. Menyediakan panduan kawalan sesi selamat; c. Menyediakan panduan mengenai prosedur sanitasi dan pengesahan data; d. Menganalisis secara menyeluruh tentang semua langkah keselamatan yang diperlukan untuk melindungi aset dan sistem maklumat daripada ancaman yang diketahui; e. Menganalisis secara menyeluruh tentang keupayaan langkah keselamatan untuk	ICTSO, Pentadbir Sistem ICT

	mengenalpasti, menghapuskan dan bertindakbalas terhadap ancaman keselamatan. f. Menganalisis langkah keselamatan yang digunakan untuk aktiviti perkhidmatan tertentu seperti penyulitan maklumat; g. Menyediakan langkah keselamatan bagi pelaksanaan penyepaduan kawalan keselamatan khusus bagi infrastruktur teknikal; dan h. Menyediakan kawalan keselamatan yang berbeza, yang boleh berfungsi dan beroperasi sebagai set kawalan gabungan.	
14.8	**Ujian Keselamatan Dalam Pembangunan Dan Penerimaan**	
	Objektif: Untuk mengesahkan jika keperluan keselamatan maklumat dipenuhi apabila aplikasi atau kod digunakan ke persekitaran pengeluaran (*production*)	
14.8.1	Ujian dalam pembangunan dan penerimaan mestilah mengikut perkara berikut: a. Ujian kefungsian keselamatan mesti dijalankan semasa pembangunan; b. Program ujian penerimaan dan kriteria yang berkaitan mesti diwujudkan untuk sistem baharu, naik taraf dan versi baharu; c. Persekitaran ujian dan operasi mesti diasingkan untuk mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran Operasi; dan d. Kriteria penerimaan untuk sistem maklumat baharu, naik taraf, dan versi baharu mesti diwujudkan dan ujian yang sesuai bagi sistem hendaklah dijalankan sebelum penerimaan.	Pentadbir Sistem ICT

14.9	**Pembangunan oleh Sumber Luar *(Outsource)***	
	Objektif: Untuk memastikan langkah keselamatan maklumat yang diperlukan oleh organisasi dilaksanakan dalam pembangunan sistem oleh sumber luar.	
14.9.1	Aktiviti pembangunan sistem oleh sumber luar hendaklah diselia dan dipantau termasuk: a. Pengurusan lesen sistem, pemilikan kod & hak intelek; b. Jaminan kualiti; c. Pengurusan hak akses; dan d. Ujian keselamatan	ICTSO, ICTO, Pentadbir Sistem ICT
14.10	**Pengasingan Persekitaran Pembangunan, Pengujian dan Pengeluaran (*Production*)**	
	Objektif: Untuk melindungi persekitaran pengeluaran dan data daripada kompromi oleh aktiviti pembangunan dan pengujian.	
14.10.1	Tahap pengasingan antara persekitaran pengeluaran, pengujian dan pembangunan yang diperlukan mesti dikenalpasti dan dilaksanakan.	Pentadbir Sistem ICT
14.11	**Pengurusan Perubahan**	
	Objektif: Untuk memelihara keselamatan maklumat semasa melaksanakan perubahan.	
14.11.1	Tanggungjawab dan prosedur pengurusan perubahan formal mesti ditakrifkan untuk memastikan kawalan yang memuaskan terhadap semua peralatan, perisian, atau perubahan proses.	Pentadbir Sistem ICT

PENGGUNA DATA (PII CONTROLLERS)

No. Polisi	Polisi	Tanggungjawab
Seksyen 15	**PENGURUSAN KESELAMATAN DATA PERIBADI (PII)**	
15.1	**Syarat Untuk Pengumpulan Dan Pemprosesan bagi Pengguna Data *(Conditions for collection and processing)***	
	Objektif: Untuk menentukan dan mendokumentasikan bahawa pemprosesan adalah sah, dengan asas undang-undang mengikut bidang kuasa yang berkenaan, dan dengan tujuan yang jelas dan sah.	
15.1.1	Kenalpasti **tujuan dokumen**, dengan: a. Memastikan Data Subjek (*PII Principal*) RTM (seperti pelanggan, pengedar, pembekal, pembekal perkhidmatan, rakan kongsi usaha sama/perkhidmatan, kakitangan) memahami tujuan PII diambil dan diproses; b. Mendokumentasikan dan menyampaikan perkara ini dengan jelas kepada Data Subjek tersebut.	Pengarah Bahagian
15.1.2	Kenal pasti **asas yang sah**, dengan: a. Menentukan, mendokumenkan dan mematuhi asas undang-undang yang berkaitan untuk memproses data peribadi (PII) bagi tujuan yang dikenalpasti sahaja.	Pengarah Bahagian
15.1.3	Tentukan **bila dan bagaimana persetujuan** akan diperoleh, dengan: a. Mendapatkan persetujuan untuk memproses data peribadi (PII) melainkan dikecualikan daripada undang-undang, akta atau perjanjian lain. b. Bila dan persetujuan diperolehi dan keperluan untuk mendapatkan persetujuan mestilah didokumenkan dengan jelas berserta penerangan berkaitan dengan tujuan	Pengarah Bahagian

No. Polisi	Polisi	Tanggungjawab
	memproses dan maklumat tentang jika dan bagaimana termaktub di dalam persetujuan tersebut.	
15.1.4	Rekod persetujuan didapati dengan: 1. Kebenaran memproses Data Peribadi hendaklah diperolehi daripada Data Subjek (*PII Principal*) melalui dokumen persetujuan merangkumi butiran seperti masa, Data Subjek dan penyataan persetujuan; 2. Maklumat persetujuan yang jelas mestilah diberikan kepada Data Subjek sebelum proses persetujuan dilakukan dengan mengambil kira perkara di bawah: ▪ diberi secara percuma; ▪ tujuan pemprosesan; dan ▪ kenyataan yang jelas dan eksplisit.	Pengarah Bahagian
15.1.5	**Penilaian impak privasi (PIA):** Menilai keperluan untuk memproses Data Peribadi melalui penilaian impak privasi bagi pemprosesan baharu atau perubahan kepada pemprosesan data peribadi (PII) sedia ada hendaklah dirancang dan dilaksanakan.	Pengarah Bahagian, DPO
15.1.6	**Kontrak dengan Pemproses PII**: Kontrak bertulis dengan mana-mana Pemproses Data (*PII Processor*) yang digunakan oleh RTM hendaklah diperolehi serta kawalan keselamatan yang bersesuaian dilaksanakan.	Pengarah Bahagian
15.1.7	**Pengguna bersama PII *(Joint PII Controller):*** Menentukan peranan dan tanggungjawab masing-masing untuk pemprosesan PII (termasuk keperluan perlindungan dan keselamatan PII) dengan mana-mana pengguna	Pengarah Bahagian

No. Polisi	Polisi	Tanggungjawab
	bersama PII.	
15.1.8	**Rekod berkaitan pemprosesan data peribadi (PII)**: Rekod memproses Data Peribadi hendaklah diwujudkan dan dikawal mengikut prosedur kawalan dokumen dan rekod bagi menyokong keperluan memproses PII.	Pengarah Bahagian
15.2	**Komitmen kepada Data Subjek *(Obligations to PII principals)***	
	Objektif: Untuk memastikan bahawa Data Subjek diberikan maklumat yang sesuai tentang pemprosesan Data Peribadi dan untuk memenuhi sebarang komitmen lain yang terpakai kepada Data Subjek yang berkaitan dengan pemprosesan Data Peribadi.	
15.2.1	Menentukan dan mendokumenkan **keperluan undang-undang, kawal selia dan perkhidmatan** kepada Data Subjek berkaitan pemprosesan Data Peribadi dan menyediakan kaedah untuk memenuhi komitmen ini.	Pengarah Bahagian
15.2.2	Data Subjek mestilah dimaklumkan mengenai **tujuan data peribadi diproses**, keperluan undang-undang, implikasi sekiranya Data Peribadi tidak dapat dipenuhi, permohonan pembatalan atau pertukaran Data Peribadi (sekiranya tidak tepat) serta tempoh penyimpanan Data Peribadi.	Pengarah Bahagian
15.2.3	Data Subjek yang merasakan bahawa data peribadinya mungkin telah diproses dan melanggar peruntukan Akta boleh membuat aduan kepada Pesuruhjaya Perlindungan Data Peribadi. Berikut adalah amalan yang disyorkan untuk Data Subjek (Pengadu):	Data Subjek, DPO

No. Polisi	Polisi	Tanggungjawab
	Pengadu mesti membuat aduan terlebih dahulu dan meminta penjelasan dengan organisasi yang berkenaan; Sekiranya pengadu masih tidak berpuas hati dengan tindak balas dan tindakan yang diambil oleh organisasi, maka pengadu boleh terus mengemukakan aduan kepada Pesuruhjaya Perlindungan Data Peribadi untuk membolehkan siasatan dijalankan; dan Sekiranya pengadu masih tidak berpuas hati dengan keputusan Pesuruhjaya mengenai perkara itu, pengadu boleh mengajukan kepada Tribunal Rayuan dengan mengemukakan notis rayuan. Aduan dapat dilakukan melalui salah satu mekanisme berikut: Laporkan dan tinjau aduan melalui Sistem Perlindungan Data Peribadi (SPDP) melalui pautan https://daftar.pdp.gov.my/; atau Hantarkan E-mel ke Jabatan Perlindungan Data Peribadi (aduan@pdp.gov.my); atau Hantar surat kepada Jabatan Perlindungan Data Peribadi, yang ditujukan kepada; Jabatan Perlindungan Data Peribadi Level 6, Kompleks Kementerian Komunikasi & Multimedia Lot 4G9, Persiaran Perdana, Presint 4 Pusat Pentadbiran Kerajaan Persekutuan 62100 Putrajaya	

No. Polisi	Polisi	Tanggungjawab
15.2.4	Data Subjek hendaklah diberikan **maklumat yang jelas mengenai pemprosesan data peribadi** mereka serta diberikan hak bagi mengakses Data Peribadi mereka.	Pengarah Bahagian
15.2.5	Data Subjek hendaklah diberi **hak untuk membuat pembatalan atau penukaran kebenaran memproses data peribadi** mereka yang terdahulu melalui permohonan secara rasmi kepada RTM.	Pengarah Bahagian
15.2.6	Data Subjek hendaklah diberikan **hak untuk menolak pemprosesan data peribadi** mereka, semasa proses permohonan, kebenaran perlu diperolehi dan hendaklah diproses di dalam tempoh tertentu.	Pengarah Bahagian
15.2.7	Pemberian **akses kepada Data Subjek,** termasuk untuk pembetulan atau pembatalan; oleh Data Subjek hendaklah mematuhi polisi kawalan akses.	Pengarah Bahagian
15.2.8	Memaklumkan kepada **pihak ketiga yang telah berkongsi data peribadi** tentang sebarang pengubahsuaian, penarikan balik atau bantahan berkaitan data peribadi yang dikongsi, dan melaksanakan polisi, prosedur dan/atau mekanisme yang sesuai untuk berbuat demikian.	Pengarah Bahagian, DPO
15.2.9	Data Peribadi yang disimpan atau diproses oleh RTM hendaklah diberikan **salinan kepada Data Subjek.**	Pengarah Bahagian
15.2.10	Mentakrifkan dan mendokumenkan **polisi dan prosedur untuk mengendalikan dan menjawab permintaan yang sah** daripada Data Subjek.	Pengarah Bahagian

No. Polisi	Polisi	Tanggungjawab
15.2.11	**Proses kelulusan tidak boleh dibuat secara automatik oleh sistem** sebaliknya kelulusan perlu disemak dan diluluskan oleh pembuat keputusan.	Pengarah Bahagian
15.3	**Rekabentuk dan Asas Privasi *(Privacy by design and privacy by default)***	
	Objektif: Untuk memastikan proses dan sistem direkabentuk supaya pengumpulan dan pemprosesan (termasuk penggunaan, pendedahan, penyimpanan, penghantaran dan pelupusan) adalah terhad kepada apa yang perlu untuk tujuan yang dikenal pasti.	
15.3.1	**Mengehadkan permintaan terhadap jenis Data Peribadi** hanya kepada maklumat yang diperlukan dan relevan sahaja.	Pengarah Bahagian
15.3.2	**Mengehadkan pemprosesan terhadap jenis Data Peribadi** hanya kepada maklumat yang diperlukan, relevan dan menepati tujuan.	Pengarah Bahagian
15.3.3	**Memastikan dan mendokumentasikan data peribadi adalah tepat, lengkap dan terkini** seperti yang diperlukan untuk tujuan ia diproses, sepanjang kitaran hayat data peribadi (PII).	Pengarah Bahagian
15.3.4	**Mentakrifkan dan mendokumenkan had pengumpulan data peribadi** kepada perkara yang berkaitan secara langsung dan hendaklah mencapai tujuan tertentu. Juga hendaklah menyimpan data dalam masa yang diperlukan bagi memenuhi tujuan tersebut.	Pengarah Bahagian
15.3.5	**Memastikan bahawa data peribadi yang dipadam atau dibatalkan** tidak boleh diwujudkan semula dengan apa cara sekalipun.	Pengarah Bahagian
15.3.6	Bagi **fail sementara** yang digunakan bagi memproses data peribadi hendaklah **dilupuskan** mengikut prosedur yang ditetapkan.	Pengarah Bahagian
15.3.7	Data Peribadi mestilah disimpan tidak melebihi	Pengarah Bahagian

No. Polisi	Polisi	Tanggungjawab
	tempoh **tujuh (7) tahun** bagi yang **melibatkan kewangan** dan **lima (5) tahun bagi yang bukan kewangan** serta bertepatan dengan tujuan pemprosesan.	
15.3.8	**Pelupusan Data Peribadi** hendaklah mengikut prosedur pelupusan aset.	Pengarah Bahagian
15.3.9	**Data Peribadi yang dihantar melalui rangkaian luar hendaklah dikawal** daripada kebocoran atau kesalahan maklumat tersebut.	Pengarah Bahagian
15.4	**Perkongsian, Pemindahan Dan Pendedahan Data Peribadi *(*PII *sharing, transfer, and disclosure)***	
	Objektif: Untuk menentukan dan mendokumenkan apabila PII dikongsi, dipindahkan ke bidang kuasa/undang-undang lain atau pihak ketiga dan/atau didedahkan mengikut keperluan yang berkenaan.	
15.4.1	Mengenal pasti **undang-undang** yang berkaitan serta menyediakan dokumentasi yang diperlukan apabila memindahkan Data Peribadi tertakluk kepada perundangan dalam dan luar negara.	Pengarah Bahagian
15.4.2	Menyatakan dengan jelas dan **mendokumentasi** maklumat bagi negara dan organisasi antarabangsa yang terlibat di dalam pemindahan Data Peribadi.	Pengarah Bahagian
15.4.3	Data Peribadi yang **dipindahkan** daripada atau kepada **pihak ketiga** hendaklah **direkodkan**.	Pengarah Bahagian
15.4.4	Data Peribadi yang **dikongsi bersama pihak ketiga** hendaklah **direkodkan**.	Pengarah Bahagian

PEMPROSES DATA (PII *PROCESSORS*)

	Tidak Terpakai bagi RTM

LAMPIRAN 1

BORANG PKM01

SURAT AKUAN PEMATUHAN POLISI KESELAMATAN MAKLUMAT DAN PRIVASI JABATAN PENYIARAN MALAYSIA

Nama :

No Kad Pengenalan :

Jawatan :

Kementerian / Jabatan :

*****Bagi Pihak Ketiga Sahaja

Syarikat : _____

Alamat Berdaftar : _____

_____

_____

No. Telefon :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya juga telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Maklumat dan Privasi RTM;
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka Tindakan sewajarnya boleh diambil ke atas diri saya

.....
( )
Tarikh:

– Cop Syarikat –

Pengesahan Pegawai Keselamatan Maklumat

.....
( )
b.p. Ketua Pengarah Penyiaran
Jabatan Penyiaran Malaysia

Tarikh:___/___/_____

***Bagi pihak ketiga bukan penjawat awam, sila lampirkan satu (1) salinan MyKad**

LAMPIRAN 2: UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI

1. Akta Komunikasi dan Multimedia 1998;
2. Akta Jenayah Komputer 1997;
3. Akta Tandatangan Digital 1997;
4. Akta Hak Cipta (Pindaan) Tahun 1997;
5. Akta Rahsia Rasmi 1972;
6. Arahan Keselamatan (Semakan dan Pindaan 2017);
7. Akta Perlindungan Data Peribadi 2010
8. Akta Perlindungan Data Peribadi (Pindaan) 2024
9. Akta Keselamatan Siber 2024
10. Akta Perkongsian Data 2025
11. Standard Perlindungan Data Peribadi 2015
12. Panduan Peranan Ketua Jabatan, Pegawai Pengelas dan Pendaftar Rahsia dalam Menguruskan Dokumen Rahsia Rasmi Kerajaan (2018)

LAMPIRAN 3

PERAKUAN UNTUK DITANDATANGANI OLEH PENJAWAT AWAM BERKENAAN DENGAN AKTA RAHSIA RASMI 1972

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkahlaku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

Saya faham bahawa segala maklumat rasmi yang saya perolehi dalam perkhidmatan Seri Paduka Baginda Yang Di Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan Seri Paduka Baginda Yang Di Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani suatu akuan selanjutnya bagi maksud ini apabila meninggalkan Perkhidmatan Kerajaan.

Tandatangan : .....

Nama dengan huruf besar : .....

No. Kad Pengenalan : .....

Jawatan : .....

Tarikh : .....

Disaksikan oleh : .....
(Tandatangan)

Nama dengan huruf besar : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan : .....

Tarikh : .....

Cap Jabatan : .....

LAMPIRAN 3

AKTA 88

8. (1) Jika seseorang yang ada dalam miliknya atau kawalannya sesuatu perkataan kod, isyarattimbal atau kata jodoh rasmi yang rahsia atau sesuatu benda, suratan atau maklumat yang

(a) berhubung dengan atau digunakan di sesuatu tempat larangan atau berhubung dengan apa-apa jua di sesuatu tempat itu; atau
(b) berhubung dengan kelengkapan perang; atau
(c) telah dibuat atau didapatkan bersalahan dengan Akta ini; atau
(d) telah diamanahkan sebagai rahsia kepadanya oleh seseorang pegawai awam; atau
(e) telah dibuat atau didapatkan atau dilihat olehnya, oleh kerana kedudukannya sebagai seorang yang memegang atau telah memegang jawatan dalam perkhidmatan awam, atau sebagai seorang yang memegang atau telah memegang suatu kontrak yang dibuat bagi pihak Kerajaan, atau sebagai seorang yang bekerja atau telah bekerja dengan atau di bawah seseorang yang memegang atau telah memegang jawatan atau kontrak itu,

Melakukan mana-mana yang berikut:--

(i) menyampaikan secara langsung atau secara tak langsung sesuatu maklumat atau benda tersebut kepada sesuatu negeri asing yang lain daripada negeri asing yang kepadanya diberikuasa dengan sempurna bagi menyampaikannya atau kepada seseorang lain yang lain daripada orang yang kepadanya ia diberikuasa dengan sempurna bagi menyampaikannya atau yang kepadanya ia adalah berkewajipan bagi menyampaikannya; atau
(ii) menggunakan sesuatu maklumat atau benda seperti tersebut di atas untuk faedah sesuatu negeri asing yang lain daripada negeri asing yang bagi faedahnya ia diberi kuasa dengan sempurna bagi menggunakannya atau dengan apa-apa cara lain yang mudarat kepada keselamatan atau kepentingan Malaysia; atau
(iii) menyimpan dalam milik atau kawalannya mana-mana benda seperti yang tersebut di atas manakala ia tidak berhak menyimpannya, atau manakala berlawanan dengan kewajipannya bagi menyimpannya, atau tidak mematuhi segala arahan yang sah yang dikeluarkan oleh pihak-berkuasa yang sah berkenaan dengan pemulangan atau pelupusan benda itu; atau
(iv) tidak menjaga dengan cara yang berpatutan, atau bertingkah-laku sehingga membahayakan keselamatan atau rahsia, sesuatu maklumat atau benda seperti tersebut di atas,

maka orang itu adalah melakukan suatu kesalahan yang boleh dihukum dengan penjara tidak lebih daripada tujuh tahun atau denda tidak lebih daripada sepuluh ribu ringgit atau penjara dan denda itu kedua-duanya.

(2) Jika seseorang menerima sesuatu perkataan kod, isyarattimbal, atau kata jodoh rasmi yang rahsia, atau apa-apa benda, suratan atau maklumat dengan mengetahui atau ada alasan yang munasabah bagi mempercayai, pada waktu ia menerimanya itu, bahawa perkataan kod, isyarattimbal, kata jodoh, benda, suratan atau maklumat itu adalah disampaikan kepadanya bersalahan dengan Akta ini, maka ia adalah melakukan suatu kesalahan yang boleh dihukum dengan penjara tidak lebih daripada tujuh tahun atau denda tidak lebih daripada sepuluh ribu ringgit atau penjara dan denda itu kedua-duanya melainkan jika ia membuktikan bahawa perkataan kod, isyarattimbal, kata jodoh, benda, suratan atau maklumat itu telah disampaikan kepadanya dengan tidak dikehendaki olehnya.

SINGKATAN DAN TAKRIFAN

Pemakaian PKMP RTM ini adalah ditakrifkan seperti berikut:

Bil.	Perkataan	Keterangan
1.	*Antivirus*	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk* akan sebarang kemungkinan adanya virus.
2.	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
3.	*Backup*	Proses penduaan/sandaran sesuatu dokumen atau maklumat.
4.	CCTV	*Closed-Circuit Television System* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
5.	CDO	*Chief Digital Officer* Ketua Pegawai Digital yang menentukan strategi dan melaksanakan inisiatif ICT bagi mencapai visi dan objektif pembangunan dan penggunaan ICT.
6.	CERT RTM	*Computer Emergency Response Team RTM* atau Pasukan Tindak Balas Insiden Keselamatan ICT RTM

7.	*Clear Desk dan Clear Screen*	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
8.	*Firewall*	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
9.	Hab *(Hub)*	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
10.	ICT	*Information and Communication Technology/* Teknologi Maklumat dan Komunikasi
11.	ICTSO	*ICT Security Officer* Pegawai Keselamatan Maklumat Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
12.	ICTO	*ICT Officer* Timbalan Pengarah SAICT
13.	Insiden Keselamatan	Musibah (adverse event) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
14.	Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.

15.	*Internet Gateway*	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik- trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
16.	Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
17.	*Intrusion Detection System (IDS)*	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
18.	*Intrusion Prevention System (IPS)*	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS*
19.	ISMS	*Information Security Management System* Sistem Pengurusan Keselamatan Maklumat
20.	RTM	Radio Televisyen Malaysia

21.	Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan
22.	Kriptografi	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
23.	LAN	Local Area Network Rangkaian Kawasan Setempat yang menghubungkan komputer.
24.	*Malicious Code*	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
25.	*Mobile Code*	*Mobile code* merupakan suatu perisian yang boleh dipindahkan di antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh Java Applet, ActiveX dan sebagainya pada pelayar internet.
26.	*Outsource*	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
27.	Pasukan ERT	Pasukan Tindakan Kecemasan/*Emergency Response Team* (ERT)

28.	Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
29.	Pentadbir Sistem ICT	Pentadbir Sistem ICT termasuk Pentadbir Perkakasan dan Perisian, Pentadbir Aplikasi, Pentadbir Rangkaian dan Keselamatan ICT, Pentadbir Pusat Data, Pentadbir Pangkalan Data, Pentadbir E-mel.
30.	Pentaksiran risiko	Keseluruhan proses pengenalpastian risiko, analisis risiko dan penilaian risiko
31.	Penguraian risiko	Proses untuk mengubahsuai risiko.
32.	Perisian Aplikasi	Merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* atau pun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan
33.	*Perjanjian Escrow*	Perjanjian/kontrak bersama pembekal perisian untuk memastikan kesinambungan penyelenggaraan perisian dari semasa ke semasa, walaupun jika pembekal perisian tersebut telah menamatkan perkhidmatan atau muflis atau gagal mengekalkan dan mengemas kini sumber kod perisian.

34.	Data Peribadi	*Personally Identifiable Information (PII)* apa-apa maklumat yang (a) boleh digunakan untuk mewujudkan hubungan antara maklumat dengan orang sebenar dengan siapa maklumat tersebut berkaitan, atau (b) adalah atau boleh dikaitkan secara langsung atau tidak langsung dengan orang sebenar.
35.	Data Subjek	*PII Principal* Orang perseorangan yang memberikan maklumat pengenalan peribadi (PII) berkaitan; Contoh, personel yang disenaraikan dalam sistem sumber manusia syarikat, pengguna yang disebut dalam laporan kredit dan pesakit yang disenaraikan dalam rekod kesihatan elektronik.
36.	Pengguna	Warga RTM dan Pihak Ketiga.
37.	Pihak Ketiga	Merangkumi pembekal/ perunding/ kontraktor/ pengguna agensi kerajaan/swasta/ pihak yang berurusan dengan RTM.
38.	Pengarah Bahagian	Memantau kemajuan pelaksanaan projek mengikut pelan carta perbatuan dari mula sehingga tamat projek (Dalam Konteks Pengurusan Maklumat Pengenalan Peribadi (PII)).
39.	Pengguna Data	*PII Controller* Organisasi yang menentukan mengapa (tujuan) dan bagaimana (kaedah) pemprosesan PII berlaku.

40.	Pemproses PII	*PII Processor* Pihak berkepentingan yang memproses maklumat pengenalan peribadi (PII) bagi pihak dan mengikut arahan Pengguna Data.
41.	Penilaian Impak Privasi (*Privacy Impact Assessment* (PIA))	Keseluruhan proses mengenal pasti, menganalisis, menilai, berunding, berkomunikasi dan merancang rawatan potensi kesan privasi berkaitan dengan pemprosesan data peribadi (PII), yang dirangka dalam kerangka pengurusan risiko organisasi yang lebih luas.
42.	*Public-Key Infrastructure* (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
43.	PKP	Pelan Kesinambungan Perkhidmatan adalah dokumen yang mengandungi maklumat kritikal yang diperlukan oleh organisasi untuk terus beroperasi semasa bencana/krisis. PKP menyatakan fungsi penting perkhidmatan, mengenal pasti sistem dan proses yang mesti dikekalkan, dan memperincikan cara mengekalkannya.
44.	*Router*	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.

45.	*Screen saver*	Imej yang akan diaktifkan pada sistem/komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
46.	*Source Code*	Kod Sumber atau kod program (biasanya hanya dipanggil sumber atau kod) merujuk kepada sebarang siri pernyataan yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia.
47.	*Switches*	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense *Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu sistem penghantaran dengan mengurangkan pelanggaran yang berlaku.
48.	*Threat Intelligence*	Proses mengumpul, menganalisis dan mengkontekstualisasikan maklumat tentang serangan siber semasa dan masa hadapan, memberikan organisasi pemahaman yang lebih mendalam tentang ancaman.
49.	*Uninterruptible Power Supply* (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
50.	Virus	Program komputer yang bertujuan merosakkan data atau sistem aplikasi.

51.	WAN	*Wide Area Network* Rangkaian yang merangkumi kawasan yang luas.
52.	Warga RTM	Personel yang berkhidmat di RTM sama ada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan ICT RTM.
53.	*Wireless LAN*	Jaringan komputer yang terhubung tanpa melalui kabel.
54.	*Web Application Firewall (WAF)*	Melindungi aplikasi web dengan menapis, memantau dan menyekat sebarang trafik HTTP/S berniat jahat yang pergi ke aplikasi web dan menghalang sebarang data yang tidak dibenarkan daripada meninggalkan aplikasi.

JABATAN PENYIARAN MALAYSIA
RADIO TELEVISYEN MALAYSIA, ANGKASAPURI KOTA MEDIA

Telefon: +603-2288 7675

Laman web: https://www.rtm.gov.my/ | e- mel: aduan@rtm.gov.my