DASAR KESELAMATAN ICT

JKSM/JKSN/MSN
Versi 4.0

DASAR KESELAMATAN ICT

JKSM/JKSN/MSN

JABATAN KEHAKIMAN SYARIAH MALAYSIA (JKSM)

JABATAN KEHAKIMAN SYARIAH NEGERI (JKSN)

MAHKAMAH SYARIAH NEGERI (MSN)

Versi 4.0

1.0 INFORMASI DOKUMEN

Jenis Dokumen:	Versi Dokumen :	Tarikh Berkuatkuasa:
Manual Keselamatan	4.0	1 November 2019

2.0 REKOD PINDAAN

KELUARAN / PINDAAN	TARIKH	KETERANGAN RINGKAS PINDAAN	BAB / MUKA SURAT	DILULUSKAN OLEH
2.0	10/12/2010			Jawatankuasa Pemandu ICT
3.0	09/03/2016	Pindaan keseluruhan Bidang Keselamatan dengan merujuk kepada ISO/IEC 27001:2013 (Information Security Management System)		Jawatankuasa Keselamatan ICT JKSM
4.0	18/10/2019	1) Pindaan Sub Bidang 0102 2) Pindaan Sub Bidang 020102, 020103, 020108, 020110, 020111.		Jawatankuasa Keselamatan ICT JKSM

KELUARAN / PINDAAN	TARIKH	KETERANGAN RINGKAS PINDAAN	BAB / MUKA SURAT	DILULUSKAN OLEH
		3) Pindaan Sub Bidang 040101, 040301. 4) Tambahan Sub Bidang 040204: Pengurusan Ketirisan Maklumat Elektronik 5) Pindaan Sub Bidang 040302: Pelupusan Media 6) Pindaan Sub Bidang 050101, 050204, 7) Tambahan Sub Bidang 050402: Capaian Jarak		

KELUARAN / PINDAAN	TARIKH	KETERANGAN RINGKAS PINDAAN	BAB / MUKA SURAT	DILULUSKAN OLEH
		Jauh 8) Pindaan Sub Bidang 050404 9) Tambahan Sub Bidang 060102: Penggunaan Kriptografi Terpercaya (*Trusted Cryptography Mechanism*) 10) Pindaan Sub Bidang 070101. 070102, 070201, 070206, 070208 11) Tambahan Sub Bidang 0703 : Bring Your Own Device		

KELUARAN / PINDAAN	TARIKH	KETERANGAN RINGKAS PINDAAN	BAB / MUKA SURAT	DILULUSKAN OLEH
		(BYOD) 12) Pindaan Sub Bidang 080301 13) Pindaan Sub Bidang 090203 14) Pindaan Sub Bidang 100205, 100209 15) Pindaan Sub Bidang 120102 16) Pindaan Sub Bidang 1401 17) Pindaan Glosari dan Rujukan		

KANDUNGAN **HALAMAN**

1.0 PENGENALAN

Dasar Keselamatan ICT (DKICT) Jabatan Kehakiman Syariah Malaysia (JKSM)/ Jabatan Kehakiman Syariah Negeri (JKSN)/ Mahkamah Syariah Negeri (MSN) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna di JKSM/JKSN/MSN mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT di JKSM/JKSN/MSN.

2.0 TUJUAN

DKICT ini mengandungi peraturan-peraturan berkaitan penggunaan sumber ICT JKSM/JKSN/MSN yang perlu dipatuhi oleh kakitangan JKSM/JKSN/MSN, pengguna dan pembekal yang memberikan perkhidmatan. Tujuan DKICT ini disediakan adalah untuk menerangkan tanggungjawab dan peranan kakitangan JKSM/JKSN/MSN, pengguna dan pembekal.

3.0 OBJEKTIF

Dasar Keselamatan ICT JKSM/JKSN/MSN diwujudkan untuk menjamin kesinambungan urusan JKSM/JKSN/MSN dengan meminimumkan kesan insiden keselamatan ICT.

Objektif utama Dasar Keselamatan ICT JKSM/JKSN/MSN ialah seperti berikut:

(a) Memastikan kelancaran operasi JKSM/JKSN/MSN dan meminimumkan

kerosakan atau kemusnahan;

(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan, dan kesahihan (CIA);

(c) Mencegah salah guna atau kecurian aset ICT JKSM/JKSN/MSN;

(d) Memperkemaskan pengurusan risiko; dan

(e) Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal.

4.0 PERNYATAAN DASAR KESELAMATAN ICT JKSM/JKSN/MSN

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

Keselamatan ICT adalah bermaksud keadaan bagi segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan.
Empat (4) komponen asas keselamatan ICT adalah:

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan daripada capaian tanpa kuasa yang sah;

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

(c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

(d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar Keselamatan ICT JKSM/JKSN/MSN merangkumi perlindungan ke atas semua bentuk maklumat elektronik dan bukan elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

(a) **Kerahsiaan**

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

(b) **Integriti**

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

(c) **Tidak Boleh Disangkal**

Punca data dan maklumat hendaklah daripada punca yang sah dan tidak

boleh disangkal;

(d) **Kesahihan**
Data dan maklumat hendaklah dijamin kesahihannya; dan

(e) **Ketersediaan**
Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

5.0 SKOP

Aset ICT JKSM/JKSN/MSN terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT JKSM/JKSN/MSN menetapkan keperluan-keperluan asas berikut:

(a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

(b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan JKSM/JKSN/MSN.

Bagi memastikan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT JKSM/JKSN/MSN ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran dan yang dibuat salinan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara- perkara berikut:

(a) **Perkakasan**

Semua aset yang digunakan untuk pemprosesan maklumat, kemudahan storan dan peralatan sokongan. Contoh komputer, pelayan, peralatan komunikasi, pencetak, *Uninterruptible Power Supply* (UPS), punca kuasa dan sebagainya;

(b) **Perisian**

Semua jenis perisian yang digunakan untuk mengendali, memproses, menyimpan dan menghantar data atau maklumat. Ini termasuklah sistem aplikasi seperti Sistem E-Syariah, Sistem Pertukaran Pegawai dan sistem pengoperasian seperti Windows, LINUX dan perisian utiliti, perisian komunikasi, sistem pengurusan pangkalan data, fail program, fail data dan lain-lain.

(c) **Perkhidmatan**

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

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

(d) **Data atau Maklumat**

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

(e) **Media Storan**

Semua media storan dan peralatan yang berkaitan seperti storan mudah alih, CD-ROM, pemacu pita, pemacu cakera, pita *backup* dan lain-lain.

(f) **Dokumentasi**

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

(g) **Premis Komputer dan Komunikasi**

Semua kemudahan serta premis yang diguna untuk menempatkan perkara (a) hingga (e) di atas.

(h) **Manusia**

Semua pengguna infrastruktur ICT JKSM/JKSN/MSN yang dibenarkan termasuk kakitangan JKSM/JKSN/MSN, pengguna dan pembekal.

6.0 PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas Dasar Keselamatan ICT JKSM/JKSN/MSN adalah seperti berikut:

(a) **Akses Atas Dasar Perlu Mengetahui**

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan.

(b) **Hak Akses Minimum**

Hak akses kepada pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan / atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau menghapuskan sesuatu maklumat.

(c) **Akauntabiliti**

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

(d) **Pengasingan**

Pengasingan hendaklah dilaksana bagi mengelak capaian yang tidak dibenarkan serta melindungi aset daripada kesilapan, kebocoran maklumat terperingkat atau manipulasi. Prinsip pengasingan hendaklah diamalkan dalam empat (4) keadaan berikut:

1) Infrastruktur
   i) Rangkaian perlu dibezakan antara – LAN, WAN, VPN;
   ii) Saluran komunikasi – *packet segmentation;* dan
   iii) Platform aplikasi – *client server, web based* atau *stand-alone.*

2) Persekitaran Pembangunan Sistem

Pengasingan dari segi persekitaran pembangunan sistem dilaksana berdasarkan persekitaran yang berikut:

i) Persekitaran Pembangunan;
ii) Persekitaran Pengujian; dan
iii) Persekitaran Pengoperasian.

3) Kawalan Capaian

Pengasingan daripada segi kawalan capaian terhadap aset dilaksana mengikut keperluan fungsi bidang tugas yang ditetapkan sama ada sebagai pengguna biasa atau pentadbir sistem.

4) Peranan dan Tanggungjawab

Pengasingan daripada segi penyediaan dokumen dan kelulusan sesuatu permohonan dilaksana berdasarkan peranan dan tanggungjawab sebagai:

i) Penyedia atau pemohon;
ii) Penyemak atau penyokong; dan
iii) Pelulus.

(e) **Pengauditan**

Pengauditan melibatkan pemeliharaan semua rekod berkaitan tindakan keselamatan maklumat bagi mengenalpasti ancaman dan insiden berkaitan keselamatan. Semua aset yang terlibat hendaklah dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit.

(f) **Pematuhan**

Dasar Keselamatan ICT JKSM/JKSN/MSN hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

(g) **Pemulihan**

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelanpemulihan bencana/kesinambungan perkhidmatan.

(h) **Tidak Boleh Disangkal**

Prinsip tidak boleh disangkal dilaksana bagi memastikan punca data dan maklumat adalah daripada punca yang sah dan tidak diragui.

(i) **Saling Bergantungan**

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

7.0 PENILAIAN RISIKO KESELAMATAN ICT

JKSM hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat daripada ancaman dan *vulnerability* yang semakin meningkat. Justeru itu JKSM/JKSN/MSN perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

JKSM/JKSN/MSN hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat JKSM/JKSN/MSN termasuklah aplikasi, perisian, perkakasan, pelayan, rangkaian, pangkalan data, sumber manusia, proses, dan prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan,

kemudahan utiliti dan sistem-sistem sokongan lain.

JKSM/JKSN/MSN bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

JKSM/JKSN/MSN perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

1. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

2. Menerima dan/ atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan atasan;

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

4. Memindahkan risiko ke pihak lain seperti kontraktor, pakar runding dan pihak-pihak lain yang berkepentingan.

8.0 SINGKATAN

a) JKSM	-	Jabatan Kehakiman Syariah Malaysia
b) JKSN	-	Jabatan Kehakiman Syariah Negeri
c) MSN	-	Mahkamah Syariah Negeri
d) RAKSSA	-	Rangka Kerja Keselamatan Siber Sektor Awam
e) MAMPU	-	*Malaysian Administrative Modernisation and Management Planning Unit* / Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
f) CGSO	-	*Chief of Government Security Office* / Pejabat Ketua Pegawai Keselamatan Kerajaan
g) NACSA	-	*National Cyber Security Agency* / Agensi Keselamatan Siber Negara
h) NC4	-	*National Coordination and Control Centre* / Pusat Kawalan dan Koordinasi Keselamatan Negara
i) DRC	-	*Disaster Recovery Centre* / Pusat Pemulihan Bencana
j) DRP	-	*Disaster Recovery Plan* / Pelan Pemulihan Bencana
k) ISMS	-	*Information Security Management System* / Sistem Pengurusan Keselamatan Maklumat
l) ICT	-	*Information and Communication Technology* / Teknologi Maklumat dan Komunikasi
m) GCERT	-	*Government Computer Emergency Response Team* / Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan

BIDANG 01 **DASAR KESELAMATAN**	
0101 Pengurusan Keselamatan Maklumat ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan JKSM/JKSN/MSN dan perundangan yang berkaitan.	
010101 Dasar Keselamatan Maklumat	
Satu set dasar untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan JKSM/JKSN/MSN kepada kakitangan JKSM/JKSN/MSN, pengguna dan pembekal. Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah JKSM dibantu oleh Jawatankuasa Keselamatan ICT JKSM dan Jawatankuasa Keselamatan ICT JKSN/MSN yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan ahli-ahli yang dilantik oleh Ketua Pengarah/ Ketua Hakim Syarie.	Ketua Pengarah/ Ketua Hakim Syarie
0102 Kajian Semula Dasar Keselamatan Maklumat	
Dasar Keselamatan ICT JKSM/JKSN/MSN perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan, dan polisi Kerajaan.	ICTSO / JKICT

Berikut adalah prosedur yang berhubung dengan kajian semula Dasar Keselamatan ICT JKSM/JKSN/MSN: a) Mengenalpasti dan menentukan perubahan yang diperlukan; b) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan Jawatan Kuasa Keselamatan ICT (JKICT) JKSM/JKSN/MSN; (c) Memaklumkan cadangan pindaan yang telah dipersetujui oleh JKICT kepada JPICT bagi tujuan pengesahan; (d) Memaklumkan pindaan yang telah disahkan oleh JPICT kepada semua kakitangan JKSM/JKSN/MSN, pengguna dan pembekal; dan (e) Dasar ini hendaklah dikaji semula secara berkala sekurang-kurangnya dua (2) tahun sekali atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	
0103 Pematuhan Dasar	
DKICT JKSM/JKSN/MSN mestilah dipatuhi oleh semua kakitangan JKSM/JKSN/MSN, pengguna dan pembekal.	Kakitangan JKSM/JKSN/MSN, Pengguna, Pembekal

BIDANG 02 **KESELAMATAN ORGANISASI**	
0201 Struktur Organisasi Keselamatan	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT JKSM/JKSN/MSN.	
020101 Ketua Pengarah/Ketua Hakim Syarie	
Peranan dan tanggungjawab Ketua Pengarah / Ketua Hakim Syarie adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JKSM/JKSN/MSN; (b) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT JKSM/JKSN/MSN; (c) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT JKSM/JKSN/MSN; (d) Memastikan semua keperluan organisasi seperti sumber kewangan, sumber Kakitangan dan perlindungan keselamatan adalah mencukupi; dan (e) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT JKSM/JKSN/MSN;	Ketua Pengarah/ Ketua Hakim Syarie

020102 Ketua Pegawai Maklumat (CIO)	
Jawatan Ketua Pegawai Maklumat (CIO) JKSM adalah disandang oleh Ketua Pendaftar JKSM manakala Jawatan Ketua Pegawai Maklumat (CIO) JKSN/MSN adalah disandang oleh Ketua Pendaftar. Kedua-duanya hendaklah dilantik secara rasmi oleh Ketua Pengarah/Ketua Hakim Syarie JKSM/JKSN/MSN. Peranan dan tanggungjawab CIO adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JKSM/JKSN/MSN; (b) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT JKSM/JKSN/MSN; (c) Memastikan kawalan keselamatan maklumat dalam organisasi diseragam dan diselaraskan dengan sebaiknya; (d) Menentukan keperluan keselamatan ICT; (e) Mempengerusikan Jawatankuasa Keselamatan ICT (JKICT); dan (f) Memastikan program-program kesedaran mengenai Keselamatan ICT dilaksanakan.	CIO

020103 Pegawai Keselamatan ICT (ICTSO)	
Jawatan ICTSO bagi JKSM adalah disandang oleh Pengarah Bahagian Teknologi Maklumat dan Komunikasi (BTMK) manakala jawatan ICTSO bagi JKSN/MSN adalah disandang oleh Ketua Unit ICT JKSN/MSN yang merupakan Pegawai Teknologi Maklumat (PTM). Kedua-duanya hendaklah dilantik secara rasmi oleh Ketua Pengarah/Ketua Hakim Syarie JKSM/JKSN/MSN. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JKSM/JKSN/MSN; (b) Mengurus keseluruhan program keselamatan ICT JKSM/JKSN/MSN; (c) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT di JKSM/JKSN/MSN; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT JKSM/JKSN/MSN; (e) Menjalankan pengurusan risiko dan audit keselamatan ICT berpandukan *Malaysian Public Sector Management of Information and Communication* (MyMIS) untuk mengenalpasti ketidakpatuhan kepada DKICT JKSM/JKSN/MSN; (f) Menyedia dan menyebarkan amaran-amaran yang	ICTSO

sesuai terhadap kemungkinan berlaku ancaman keselamatan ICT dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (g) Melaporkan insiden keselamatan ICT kepada pihak NACSA dan seterusnya membantu dalam penyiasatan atau pemulihan; (h) Melaporkan insiden keselamatan ICT kepada CIO bagi insiden yang memerlukan Pelan Kesinambungan Perkhidmatan (PKP); (i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; (j) Memastikan pematuhan DKICT JKSM/JKSN/MSN oleh pihak luar seperti pembekal dan kontraktor yang mencapai dan menggunakan aset ICT JKSM/JKSN/MSN untuk tujuan penyelenggaraan dan sebagainya; (k) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan; dan (l) Memastikan Pelan Strategik ICT (ICT Strategic Plan - ISP) JKSM mengandungi aspek keselamatan.	

020104 Pengurus ICT	
Pengurus ICT JKSM/JKSN/MSN ialah Pengarah Bahagian Teknologi Maklumat Komunikasi (BTMK) JKSM. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JKSM/JKSN/MSN; (b) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan JKSM/JKSN/MSN; (c) Menentukan kawalan akses pengguna terhadap aset ICT JKSM/JKSN/MSN; (d) Melaporkan sebarang penemuan mengenai keselamatan ICT kepada JKICT JKSM; (e) Menyimpan rekod atau laporan terkini tentang ancaman keselamatan ICT JKSM; (f) Memastikan semua kakitangan JKSM/JKSN/MSN, kontraktor dan pembekal yang terlibat dengan aset ICT JKSM/JKSN/MSN mematuhi dasar, piawaian dan garis panduan keselamatan ICT; (g) Melaksanakan keperluan DKICT dalam operasi semasa seperti berikut: i. Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu;	Pengurus ICT

ii. Pembelian atau peningkatan perisian dan sistem komputer; iii. Perolehan teknologi dan perkhidmatan komunikasi baharu; dan iv. Menentukan pembekal dan rakan usahasama menjalani tapisan keselamatan.	
020105 Pentadbir Sistem	
Pentadbir Sistem di JKSM ialah Pegawai Teknologi Maklumat di setiap unit di BTMK JKSM manakala Pentadbir Sistem di JKSN/MSN ialah Ketua Unit ICT di JKSN/MSN. Pentadbir Sistem terdiri seperti berikut: (i) Pentadbir Rangkaian dan Keselamatan; (ii) Pentadbir Pangkalan Data; (iii) Pentadbir Portal Rasmi JKSM (*Web Master*); (iv) Pentadbir Pusat Data; (v) Pentadbir Sistem Aplikasi; dan/atau (vi) Pentadbir E-mel.	Pentadbir Sistem
Pentadbir Rangkaian dan Keselamatan	
Peranan dan tanggungjawab Pentadbir Rangkaian dan Keselamatan adalah seperti berikut: (a) Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di JKSM beroperasi sepanjang	Pentadbir Rangkaian dan Keselamatan

masa; (b) Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; (c) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; (d) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; (e) Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; (f) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian JKSM secara tidak sah seperti melalui peralatan modem dan *dial-up*; (g) Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian; dan (h) Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT (*Security Posture Assessment* - SPA) serta penilaian risiko keselamatan maklumat.	
Pentadbir Pangkalan Data	
Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut: (a) Melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan	Pentadbir Pangkalan Data

dengan pangkalan data; (b) Memastikan pangkalan data boleh digunakan pada setiap masa; (c) Melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data; (d) Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur; (e) Melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip DKICT; (f) Melaksanakan proses pembersihan data (*housekeeping*) di dalam pangkalan data; dan (g) Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.	
Pentadbir Portal/ Laman Web JKSM	
Peranan dan tanggungjawab Pentadbir Portal/ Laman Web JKSM adalah seperti berikut: (a) Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah; (b) Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar; (c) Memantau dan menganalisis log untuk mengesan	Pentadbir Portal/ Laman Web

sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman; (d) Menghadkan capaian Pentadbir Portal/ Laman Web ke *web server;* (e) Mengasingkan kandungan dan aplikasi atas talian untuk capaian secara Intranet dan Internet ke portal JKSM; (f) Memastikan data-data SULIT tidak boleh disalin atau dicetak oleh orang yang tidak berhak; (g) Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; (h) Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*; (i) Melaksanakan proses *backup* dan *restore* secara berkala; (j) Melaporkan sebarang pelanggaran keselamatan laman portal kepada ICTSO; dan (k) Menjadi ahli Jawatankuasa Keselamatan ICT (JKICT) JKSM.	
Pentadbir Pusat Data	
Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut: (a) Memastikan persekitaran fizikal dan keselamatan	Pentadbir Pusat Data

Pusat Data berada dalam keadaan baik dan selamat; (b) Memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data; (c) Menjadualkan dan melaksanakan proses salinan *(backup and restore)* ke atas pangkalan data secara berkala; (d) Menyediakan perancangan pemulihan bencana mengikut prinsip Pengurusan Kesinambungan Perkhidmatan (PKP) dalam DKICT; (e) Melaksanakan prinsip-prinsip DKICT; (f) Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan; dan (g) Menjadi ahli Jawatankuasa Keselamatan ICT JKSM (JKICT).	
Pentadbir Sistem Aplikasi	
Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut: (a) Mengkaji cadangan pembangunan/ penyelarasan sistem/ modul di JKSM; (b) Membuat kajian semula serta memperbaiki sistem/ modul sedia ada di JKSM; (c) Membuat pertimbangan dan mengusulkan cadangan pelaksanaan sistem/ modul di JKSM; (d) Membuat pemantauan dan penyelenggaraan	Pentadbir Sistem Aplikasi

terhadap sistem / modul dari semasa ke semasa; (e) Bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem/ modul; (f) Menyediakan dokumentasi sistem/ modul dan manual pengguna; (g) Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; (h) Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaanya; (i) Memastikan *virus pattern*, *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemas kini supaya terhindar daripada ancaman virus dan penggodam; (j) Mematuhi dan melaksanakan prinsip-prinsip DKICT dalam pewujudkan akaun pengguna ke atas setiap sistem aplikasi; (k) Melaksanakan sandaran (*backup*) sistem aplikasi pangkalan data yang berkaitan dengannya dibuat secara berjadual; (l) Menghadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan daripada penyalahgunaannya; (m) Melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya; dan (n) Menjadi ahli Jawatankuasa Keselamatan ICT JKSM (JKICT).	

Pentadbir E-mel	
Peranan dan tanggungjawab Pentadbir E-mel adalah seperti berikut: (a) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; (b) Membekukan akaun pengguna jika perlu bagi pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; (c) Memastikan akaun e-mel pengguna sentiasa di dalam keadaan baik dan berfungsi; (d) Memastikan pengguna e-mel JKSM berkemahiran menggunakan e-mel melalui penyediaan dokumen panduan penggunaan e-mel dan kursus pembudayaan penggunaan e-mel secara berterusan; dan (e) Menjadi ahli Jawatankuasa Keselamatan ICT (JKICT) JKSM.	Pentadbir E-mel

020106 Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JKSM/JKSN/MSN; (b) Mengetahui dan memahami implikasi keselamatan ICT daripada tindakannya; (c) enjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; (d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT JKSM/JKSN/MSN dan menjaga kerahsiaan maklumat JKSM/JKSN/MSN; (e) Melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan	Pengguna

vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum. (e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; (f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan (g) Menandatangani "Surat Akuan Pematuhan" (**LAMPIRAN 1**) bagi mematuhi Dasar Keselamatan ICT JKSM/JKSN/MSN.	
020107 Jawatankuasa Keselamatan ICT JKSM	
Keanggotaan JKICT JKSM adalah seperti berikut: **<u>Pengerusi</u>:** CIO **<u>Ahli</u>:** • ICTSO • Pengarah Kanan (Pengurusan) • Pengarah Bahagian Khidmat Pengurusan & Sumber Manusia • Pengarah Bahagian Latihan • Pengarah Bahagian Pusat Sumber Maklumat dan Penerbitan • Pengarah Bahagian Dasar dan Penyelidikan • Pengarah Bahagian Sokongan Keluarga • Pengarah Bahagian Pendaftaran, Keurusetiaan dan Rekod	CIO

• Ketua Unit Integriti • Ketua Unit Komunikasi Korporat **Urusetia:** BTMK JKSM Carta struktur organisasi JKICT JKSM seperti di **LAMPIRAN 2**. **Bidang Kuasa:** (a) Menyelenggara dokumen DKICT JKSM; (b) Memantau tahap pematuhan DKICT JKSM; (c) Menilai aspek teknikal keselamatan projek-projek ICT; (d) Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam jabatan yang mematuhi keperluan DKICT JKSM; (e) Menyemak semula sistem ICT supaya sentiasa mematuhi keperluan keselamatan dari semasa ke semasa; (f) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; (g) Memastikan DKICT JKSM selaras dengan dasar-dasar ICT Kerajaan semasa; (h) Bekerjasama dengan JKSMCERT untuk mendapatkan maklum balas dan insiden untuk tindakan pengemaskinian DKICT JKSM; dan	

(i) Membincang tindakan yang melibatkan pelanggaran DKICT JKSM.	
020108 Jawatankuasa Keselamatan ICT JKSN/MSN	
Keanggotaan JKICT JKSN/MSN adalah seperti berikut: **Pengerusi:** CIO **Ahli :** • ICTSO • Wakil Mahkamah Tinggi Syariah yang dilantik • Wakil Mahkamah Rendah Syariah yang dilantik **Urusetia:** ICT JKSN/MSN Carta struktur organisasi JKICT JKSN/MSN seperti di **LAMPIRAN 2**. **Bidang Kuasa:** (a) Memantau tahap pematuhan DKICT JKSN/MSN; (b) Menilai aspek teknikal keselamatan projek-projek ICT di JKSN/MSN; (c) Mengkaji keperluan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam jabatan yang mematuhi keperluan DKICT JKSM/JKSN/MSN;	JKICT JKSN/MSN

(d) Menyemak semula sistem ICT supaya sentiasa mematuhi keperluan keselamatan dari semasa ke semasa; (e) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; (f) Memastikan DKICT JKSM/JKSN/MSN selaras dengan dasar-dasar ICT kerajaan semasa; dan (g) Menyediakan laporan keselamatan ICT kepada JKICT JKSM dan membincangkan serta menyelesaikan isu-isu berbangkit.	
020109 Pasukan Tindak Balas Insiden Keselamatan ICT JKSM (JKSMCERT)	
Keanggotaan JKSMCERT adalah seperti berikut: **Pengerusi:** Pengarah BTMK **Ahli :** • Pegawai Teknologi Maklumat di JKSM • Penolong Pegawai Teknologi Maklumat di JKSM **Urusetia:** BTMK	Pengarah BTMK

Bidang Kuasa: (a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; (b) Merekod dan menjalankan siasatan awal insiden yang diterima; (c) Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; (d) Menghubungi dan melaporkan insiden yang berlaku kepada ICTSO dan NACSA sama ada sebagai *input* atau untuk tindakan seterusnya; (e) Menasihati JKSN/MSN untuk mengambil tindakan pemulihan dan pengukuhan; (f) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baharu dapat dielakkan; (g) Mengguna pakai *Standard Operating Procedure* (SOP) bagi pengurusan pengendalian insiden keselamatan; dan (h) Melaporkan sebarang maklum balas dan insiden keselamatan ICT kepada ICTSO; dan (i) Merujuk insiden keselamatan siber yang melibatkan Maklumat Rahsia Rasmi kepada pihak CGSO.	

020110 Jawatankuasa Pemandu ICT (JPICT) JKSM	
Keanggotaan JPICT JKSM adalah seperti berikut: **Pengerusi:** Ketua Pengarah/Ketua Hakim Syarie **Ahli :** • Ketua Pendaftar JKSM • Pengarah Kanan Pengurusan • Pengarah Bahagian Khidmat Pengurusan & Sumber Manusia • Pengarah Bahagian Latihan • Pengarah Bahagian Pusat Sumber Maklumat dan Penerbitan • Pengarah Bahagian Dasar dan Penyelidikan • Pengarah Bahagian Sokongan Keluarga • Pengarah Bahagian Pendaftaran, Keurusetiaan dan Rekod • Pengarah Bahagian Teknologi Maklumat & Komunikasi • Ketua Unit Integriti • Ketua Unit Komunikasi Korporat **Bidang Kuasa:** (a) Menetapkan arah tuju dan strategi ICT untuk pelaksanaan ICT JKSM/JKSN/MSN; (b) Merancang, menyelaras dan memantau pelaksanaan	Ketua Pengarah/Ketua Hakim Syarie JKSM

program/projek ICT JKSM/JKSN/MSN; (c) Menyelaras dan menyeragamkan pelaksanaan ICT agar selari dengan Pelan Strategik Teknologi Maklumat (ICT Strategic Plan - ISP) JKSM; (d) Meluluskan projek-projek ICT JKSM; (e) Mengikuti dan memantau perkembangan program ICT serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT di JKSM; (f) Merancang dan menentukan langkah-langkah keselamatan ICT; (g) Mengemukakan perolehan ICT yang telah diluluskan di peringkat JPICT JKSM kepada Jawatankuasa Teknikal ICT Sektor Awam (JTISA) MAMPU untuk kelulusan pelaksanaan; (h) Mengemukakan laporan kemajuan projek ICT yang diluluskan kepada JTISA MAMPU; dan (i) Menetapkan dasar dan prosedur pengurusan portal rasmi JKSM.	
020111 Jawatankuasa Pelaksana Pengurusan Sistem Keselamatan Maklumat (ISMS) JKSM	
Keanggotaan jawatankuasa adalah seperti berikut: **<u>Pengerusi</u>:** ICTSO	Jawatankuasa Pelaksana ISMS

Ahli: • Ketua Penolong Pengarah Bahagian Teknologi Maklumat dan Komunikasi • Ketua Penolong Pengarah Bahagian Latihan • Ketua Penolong Pengarah Bahagian Khidmat Pengurusan & Sumber Manusia • Pegawai Teknologi Maklumat • Penolong Pegawai Teknologi Maklumat **Urusetia:** BTMK **Bidang Kuasa:** (a) Merancang dan menyelaras struktur organisasi ISMS; (b) Menghadiri kursus kesedaran ISMS; (c) Menyediakan skop ISMS; (d) Menyediakan penyataan dasar ISMS, *Statement of Applicability* (SoA), penilaian risiko, *Risk Treatment Plan (RTP)*, kaedah pengukuran kawalan dan prosedur-prosedur ISMS; (e) Mengemukakan isu dan masalah ISMS, sekiranya ada; dan (f) Mengukur keberkesanan kawalan ISMS.	

020112 Keperluan Keselamatan Kontrak dengan Pihak Luar Ketiga	
Memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak luar dikawal. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JKSM/JKSN/MSN; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pengguna; (d) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak luar/ asing; (e) Perjanjian yang dimeterai perlu mematuhi perkara-perkara berikut: (i) Dasar Keselamatan ICT JKSM / JKSN / MSN; (ii) Tapisan Keselamatan; (iii) Perakuan Akta Rahsia Rasmi 1972; (iv) Hak Harta Intelek; dan (v) Arahan Teknologi Maklumat. (f) Capaian kepada aset ICT JKSM/JKSN/MSN perlu berlandaskan kepada perjanjian kontrak atau lain-lain persetujuan bertulis yang diberikan oleh JKSM/JKSN/MSN;	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem dan Pihak Luar/ Asing.

(g) Menandatangani Surat Akuan Pematuhan DKICT JKSM/JKSN/MSN seperti di **LAMPIRAN 1;** (h) Pihak pembekal perlu menjalani Tapisan Keselamatan melalui Sistem e-Vetting CGSO dan melengkapkan borang *Declaration To Be Signed By Contractors, Official Secrets Act* (OSA) 1972 bagi perakuan untuk tidak membocorkan sebarang maklumat rasmi yang diperolehi sepanjang berkhidmat dengan JKSM.	

BIDANG 03 **KESELAMATAN SUMBER MANUSIA**	
0301 Sebelum Perkhidmatan	
Objektif: Memastikan kakitangan JKSM/JKSN/MSN dan pihak pembekal memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.	
030101 Tapisan Keselamatan (*Screening*)	
Menjalankan tapisan keselamatan terhadap kakitangan JKSM/JKSN/MSN, pembekal, pakar runding dan pihak-pihak lain yang terlibat selaras dengan keperluan perkhidmatan.	Semua
030102 Terma dan Syarat	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab kakitangan JKSM/JKSN/MSN, pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam menjamin keselamatan aset ICT; dan (b) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua

0302 Dalam Perkhidmatan	
Memastikan kakitangan JKSM/JKSN/MSN dan pihak luar seperti pembekal dan pakar runding mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua kakitangan JKSM/JKSN/MSN dan pihak luar hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.	Semua
030201 Tanggungjawab Pengurusan	
(a) Memastikan kakitangan JKSM/JKSN/MSN, pembekal dan pakar runding mematuhi dasar keselamatan maklumat JKSM/JKSN/MSN; dan (b) Memastikan kakitangan JKSM/JKSN/MSN, pembekal dan pakar runding mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh JKSM/JKSN/MSN.	Semua
030202 Latihan kesedaran dan Pendidikan Keselamatan Maklumat	
Kakitangan JKSM/JKSN/MSN dan pihak pembekal perlu diberikan program kesedaran mengenai keselamatan ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka.	Semua
030203 Tindakan Tatatertib	
(a) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas kakitangan JKSM/JKSN/MSN	Semua

sekiranya berlaku pelanggaran dengan perundangan dan peraturan yang ditetapkan oleh JKSM/JKSN/MSN; dan (b) Pengguna yang melanggar DKICT JKSM/JKSN/MSN akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT JKSM/JKSN/MSN.	
0303 Bertukar Atau Tamat Perkhidmatan	
Objektif: Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas kakitangan JKSM/JKSN/MSN diurus dengan teratur.	
030301 Tamat Perkhidmatan Atau Perubahan Bidang Tugas	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT dikembalikan kepada JKSM/JKSN/MSN mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan JKSM/JKSN/MSN dan terma perkhidmatan yang ditetapkan.	Semua

BIDANG 04 **PENGURUSAN ASET**	
0401 Akauntabiliti/Tanggungjawab Aset	
Objektif: Untuk mengenal pasti aset bagi memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT JKSM/JKSN/MSN.	
040101 Inventori Aset	
Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT JKSM/JKSN/MSN. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: (a) Memastikan semua aset ICT dikenal pasti, dikelas (dikategori), didokumen, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini di dalam Sistem Pengurusan Pemantauan Aset (SPPA) dan dokumen lain berdasarkan kepada Pekeliling berkaitan Tatacara Pengurusan Aset (TPA) yang terkini; (b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di JKSM/JKSN/MSN; (d) Memastikan semua peraturan pengendalian aset dikenalpasti, didokumenkan dan dilaksanakan; (e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; (f) Semua pengguna JKSM/JKSN/MSN hendaklah	Pegawai Aset dan Pengguna

memulangkan semua aset ICT kepada JKSM/JKSN/MSN selepas bersara, bertukar jabatan atau penamatan perkhidmatan/kontrak di JKSM/JKSN/MSN; dan (h) Semua aset ICT sewaan haruslah dipelihara dengan baik oleh pemegang aset yang dipertanggungjawabkan.	
0402 Klasifikasi Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
040201 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad	Semua
040202 Pelabelan Maklumat	
Prosedur pelabelan maklumat hendaklah dibangunkan dan dilaksanakan mengikut skim klasifikasi maklumat yang digunapakai oleh JKSM.	Semua

040203 Pengendalian Maklumat/Data	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) Menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.	Semua

040204 Pengurusan Ketirisan Maklumat Elektronik	
Ketirisan maklumat terperingkat adalah kebocoran atau kehilangan sesuatu data, berita atau laporan organisasi yang melibatkan ICT sama ada dengan sengaja atau tidak sengaja. Perisian *data leak protection* haruslah dipasang pada komputer riba dan *laptop* bagi membolehkan kawalan ke atas perkongsian atau penyebaran maklumat terperingkat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Gambar dokumen rasmi / rahsia rasmi TIDAK BOLEH diambil menggunakan telefon bimbit atau pelbagai peranti elektronik milik peribadi; (b) *Public e-mail* (Contoh: yahoo mail, Gmail) TIDAK BOLEH diguna dalam urusan rasmi Kerajaan. (c) Dokumen terperingkat TIDAK BOLEH dimuat naik dalam media sosial dan storan awan awam (seperti *dropbox*); (d) Maklumat log masuk dan kata laluan komputer/sistem ICT TIDAK BOLEH ditulis dan ditampal di skrin komputer atau mana-mana ruang kerja; dan (e) Penghantaran e-mel maklumat terperingkat haruslah menggunakan kaedah penyulitan *(encryption).*	Semua

0403 Pengendalian Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
040301 Pengurusan Media Mudah Alih (*Removable Media*)	
Prosedur pengurusan media mudah alih hendaklah dilaksanakan mengikut skim pengelasan yang diguna pakai oleh JKSM. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan (e) Menyimpan semua media di tempat yang selamat.	CIO, Pegawai Teknologi Maklumat dan Pengguna
040302 Pelupusan Media	
Pelupusan media perlu mendapat kelulusan daripada pihak pengurusan ICT dan mengikut prosedur JKSM/JKSN/MSN yang mana berkenaan.	CIO, Pegawai Teknologi Maklumat dan Pengguna

Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul serta selamat dan dengan kebenaran JKSM/JKSN/MSN. Pelupusan media storan perlu dirujuk kepada CGSO dan Jabatan Arkib Negara bagi menentukan sama ada ianya mengandungi maklumat terperingkat dan/atau mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara. Pelupusan maklumat/data boleh dilaksanakan dalam bentuk pemusnahan fizikal dan/atau sanitasi data. Sanitasi data hendaklah mengikut garis panduan yang dikeluarkan oleh Kerajaan.	
040303 Pemindahan Media Fizikal	
JKSM hendaklah memastikan media yang mengandungi maklumat dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan.	Semua

BIDANG 05 **KAWALAN CAPAIAN**	
0501 Keperluan Kawalan Capaian	
Objektif: Menghadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.	
050101 Dasar Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak secara berkala berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian pengguna sedia ada. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Keperluan keselamatan aplikasi JKSM; (b) Kebenaran untuk menyebarkan maklumat; (c) Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian; (d) Undang-undang Malaysia/ Persekutuan yang berkaitan dan obligasi kontrak mengenai had akses kepada data atau perkhidmatan; (e) Kawalan capaian ke atas perkhidmatan rangkaian	ICTSO, Pengurus ICT dan Pentadbir Sistem

dalaman dan luaran; (f) Pengasingan peranan kawalan capaian; (g) Kebenaran rasmi permintaan akses; (h) Keperluan semakan hak akses berkala; (i) Pembatalan hak akses; (j) Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan (k) Akses *privilege.*	
050102 Capaian Kepada Rangkaian Dan Perkhidmatan Rangkaian	
Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari ICTSO. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian JKSM, rangkaian agensi lain dan rangkaian awam; (b) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO, Pengurus ICT dan Pentadbir Rangkaian dan Keselamatan

0502 Pengurusan Capaian Pengguna	
Objektif: Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	
050201 Pendaftaran Pengguna dan Pembatalan Pengguna	
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan capaian dan pembatalan hak capaian Perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan oleh JKSM/JKSN/MSN sahaja boleh digunakan; (b) Akaun pengguna mestilah unik; (c) Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada JKSM/JKSN/MSN terlebih dahulu; (d) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan (e) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan JKSM/JKSN/MSN.	Pengguna JKSM/JKSN/ MSN, Pentadbir Sistem Aplikasi, ICTSO, Pengurus ICT

050202 Penyediaan Akses Pengguna (*Provisioning*)	
Satu proses penyediaan akses pengguna untuk kebenaran dan pembatalan capaian pengguna ke atas semua aplikasi dan perkhidmatan ICT.	Pentadbir Sistem Aplikasi, ICTSO, Pengurus ICT
050203 Pengurusan Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem Aplikasi
050204 Pembatalan atau Pelarasan Hak Akses	
Hak capaian kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian, atau diselaraskan apabila berlaku perubahan dalam JKSM/JKSN/MSN. Pengurusan capaian ini hendaklah dilaksanakan sekurang-kurangnya sebulan sekali atau setiap kali adanya perubahan maklumat.	Pentadbir Sistem Aplikasi, Pentadbir E-mel, ICTSO, Pengurus ICT
0503 Tanggungjawab Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JKSM/JKSN/MSN yang berkuatkuasa; (b) Mengetahui dan memahami implikasi keselamatan ICT	Pengguna, Pentadbir Sistem Aplikasi, ICTSO, Pengurus ICT

serta kesan daripada tindakannya; (c) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT JKSM/JKSN/MSN dan menjaga kerahsiaan maklumat JKSM/JKSN/MSN; (d) Melaksanakan langkah-langkah perlindungan seperti berikut: • Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; • Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; • Menentukan maklumat sedia digunakan; • Menjaga kerahsiaan kata laluan; • Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; • Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, Pertukaran dan pemusnahan; dan • Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum. (e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; dan (f) Menghadiri program-program kesedaran mengenai keselamatan ICT.	

050301 Penggunaan Kata Laluan	
Pengguna perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahihan identiti.	Pengguna, Pentadbir Sistem Aplikasi, ICTSO, Pengurus ICT
0504 Kawalan Capaian Sistem dan Aplikasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi.	
050401 Had Kawalan Capaian Maklumat	
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.	Pengguna, Pentadbir Sistem Aplikasi, ICTSO, Pengurus ICT
050402 Capaian Jarak Jauh	
Kemudahan capaian ke dalam rangkaian dalaman JKSM/JKSN/MSN sama ada dari rangkaian dalam atau luar JKSM/JKSN/MSN. (a) Kemudahan ini mestilah menggunakan kaedah pengesahan ID pengguna dan kata laluan atau kaedah	Pentadbir Sistem, Pembekal

lain yang selamat dan dipercayai (*secure and trusted*). (b) Capaian jarak jauh daripada luar rangkaian JKSM/JKSN/MSN hendaklah menggunakan mekanisme perhubungan rangkaian Internet yang disediakan oleh JKSM/JKSN/MSN. (c) Penggunaan perkhidmatan capaian jarak jauh selain daripada yang disediakan oleh JKSM hendaklah mendapat kebenaran CIO atau ICTSO JKSM/JKSN/MSN. (d) Penggunaan perkhidmatan ini hendaklah dimohon dan mendapat kebenaran bertulis daripada CIO atau ICTSO JKSM/JKSN/MSN. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	
050403 Prosedur *Log-on*	
Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan *log-on* yang bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kaedah-kaedah yang digunakan adalah seperti berikut: (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Jabatan; (b) Menjana amaran (*alert*) sekiranya berlaku pelanggaran semasa proses *log-on* terhadap aplikasi sistem;	Pentadbir Sistem, ICTSO, Pengurus ICT

(c) Mengawal capaian ke atas aplikasi sistem menggunakan prosedur *log-on* yang terjamin; (d) Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna; (e) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; dan (f) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	
050404 Sistem Pengurusan Kata Laluan	
Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh JKSM seperti berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Pengguna hendaklah menukar kata laluan dengan segera apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Panjang kata laluan mestilah sekurang kurangnya dua belas (12) aksara dengan gabungan antara huruf, aksara khas dan nombor (alphanumerik); (d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun;	Pengguna, Pentadbir Sistem Aplikasi, ICTSO, Pengurus ICT

(e) Kata laluan komputer hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam aturcara; (g) Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (i) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; dan (j) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	
050405 Penggunaan Utiliti Sistem	
Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding* sistem.	Pentadbir Sistem Aplikasi, ICTSO, Pengurus ICT

050406 Kawalan Akses Kepada *Source Code Program*	
Pembangunan sistem secara sumber luaran perlu diselia dan dipantau oleh JKSM. (a) Log audit perlu dikekalkan kepada semua akses kepada kod sumber; (b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan (c) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hakmilik JKSM.	Pentadbir Sistem, ICTSO, Pengurus ICT

BIDANG 06 **KRIPTOGRAFI**	
0601 Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
060101 Kawalan Penggunaan Kriptografi	
Melindungi kerahsiaan, integriti dan kesahihan maklumat yang merangkumi data di dalam sistem rangkaian, sistem aplikasi dan pangkalan data. Kunci enkripsi mestilah dilindungi dengan menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut. Kriptografi turut merangkumi kaedah-kaedah seperti berikut: (a) **Enkripsi** Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (*encryption*). (b) **Tandatangan Digital** Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan.	Pentadbir Sistem

(c) **Pengurusan Infrastruktur Kunci Awam/Public Key Infrastructure (PKI)** Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	
060102 Penggunaan Kriptografi Terpercaya (*Trusted Cryptography*)	
(a) Penggunaan mekanisme Kriptografi Terpercaya adalah mandatori bagi pengendalian Maklumat Rahsia Rasmi. (b) Untuk mengendalikan Maklumat Rasmi, penggunaan mekanisme Kriptografi Terpercaya adalah digalakkan. Mekanisme kriptografi lain yang digunapakai oleh pihak industri juga boleh digunakan untuk mengendalikan Maklumat Rasmi.	Pentadbir Sistem

BIDANG 07 **KESELAMATAN FIZIKAL DAN PERSEKITARAN**	
0701 Keselamatan Kawasan	
Objektif: Mencegah akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat JKSM/JKSN/MSN.	
070101 Kawalan Kawasan	
Ini bertujuan menghalang capaian, kerosakan dan gangguan secara perolehan fizikal terhadap premis dan maklumat agensi. Jabatan hendaklah mengenal pasti Kawasan Terperingkat. Peranti milik persendirian adalah DILARANG penggunaannya di Kawasan Terperingkat. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan	CGSO, CIO

kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (c) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (d) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana disebabkan oleh kuasa Tuhan atau perbuatan manusia; (e) Melaksana perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; (f) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan (g) Memasang alat penggera atau kamera pengawasan. Jabatan hendaklah merujuk kepada CGSO untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.	
070102 Kawalan Masuk Fizikal	
Kawalan masuk fizikal bertujuan untuk mewujudkan kawalan keluar masuk ke premis JKSM. Perkara yang perlu dipatuhi adalah seperti berikut:	Semua

(a) Setiap pegawai dan kakitangan JKSM hendaklah mempamerkan Pas Keselamatan sepanjang waktu bertugas. Semua Pas Keselamatan hendaklah dikembalikan kepada JKSM apabila bertukar, tamat perkhidmatan atau bersara; (b) Setiap Pelawat hendaklah mendaftar dan mendapatkan Pas Keselamatan Pelawat di Kaunter Keselamatan dan hendaklah dikembalikan selepas tamat urusan/lawatan pada hari yang sama. Kegagalan Pelawat mengembalikan Pas Keselamatan Pelawat adalah satu kesalahan dan boleh diambil tindakan; (c) Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT JKSM; dan (d) Kehilangan Pas Keselamatan Pelawat hendaklah dilaporkan segera kepada Pihak Berkuasa.	
070103 Kawalan Pejabat, Bilik dan Tempat Operasi	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawasan tempat bekerja, bilik dan tempat operasi ICT perlu dihadkan daripada akses oleh pihak luar; (b) Penunjuk arah ke lokasi bilik operasi dan tempat larangan tidak harus menonjol dan hanya memberi petunjuk minimum.	Semua

070104 Perlindungan Terhadap Ancaman Luaran dan Dalaman	
JKSM perlu merekabentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	Semua
070105 Kawalan Tempat Larangan (*Working In Secure Area*)	
Kawasan larangan lokasi ICT bagi JKSM ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga JKSM yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis tersebut. Kawasan larangan lokasi ICT JKSM adalah Pusat Data JKSM. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas premis tersebut adalah seperti berikut: (a) Sumber data atau *server*, peralatan komunikasi dan storan perlu ditempatkan di Pusat Data, Bilik Server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran; (b) Akses adalah terhad kepada warga JKSM yang telah diberi kuasa sahaja dan dipantau pada setiap masa; (c) Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) atau lain-lain peralatan yang sesuai; (d) Peralatan keselamatan (CCTV, log akses) perlu	Pentadbir Pusat Data, Pentadbir Keselamatan dan Rangkaian

diperiksa secara berjadual; (e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; (f) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab sepanjang tempoh di lokasi berkaitan; (g) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; (h) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; (i) Memperkukuhkan dinding dan siling; dan (j) Menghadkan jalan keluar masuk.	
070106 Kawasan Penghantaran dan Pemunggahan	
JKSM hendaklah memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Semua
0702 Keselamatan Peralatan ICT	
Objektif: Melindungi peralatan ICT JKSM dari kehilangan, kerosakan, kecurian dan disalahgunakan.	

070201 Keselamatan Peralatan/Peralatan ICT	
Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: (a) Penggunaan kata laluan untuk akses kepada sistem komputer adalah diwajibkan; (b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; (d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; (e) Pengguna mesti memastikan perisian antivirus di komputermasing-masing sentiasa aktif dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; (f) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna; (g) Setiap pengguna adalah bertanggungjawab ke atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; (h) Peralatan-peralatan kritikal perlu disokong oleh	Semua

Uninterruptable Power Supply (UPS) dan *Generator Set* (*Gen-Set*); (i) Semua alat sokongan perlu disemak dan dikemaskinikan dari semasa ke semasa (sekurang-kurangnya setahun sekali); (j) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; (k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; (l) Peralatan ICT yang hendak dibawa ke luar dari premis JKSM/JKSN/MSN, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan; (m) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden; (n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa; (o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ianya ditempatkan tanpa kebenaran Pentadbir Sistem;	

(p) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem untuk dibaik pulih; (q) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (r) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal; (s) Pengguna dilarang sama sekali mengubah kata laluan ***administrator*** yang telah ditetapkan oleh Pentadbir Sistem; (t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan digunakan sepenuhnya bagi urusan rasmi Jabatan sahaja; dan (u) Pengguna adalah bertanggungjawab melaporkan kehilangan aset ICT di bawah jagaannya kepada Ketua Jabatan mengikut tatacara yang dinyatakan dalam Tatacara Pengurusan Aset (TPA) yang terkini.	
070202 Keselamatan Kabel	
Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-	Pentadbir Rangkaian

langkah keselaatan yang perlu diambil adalah seperti berikut: (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	
070203 Penyelenggaraan Peralatan	
Peralatan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: (a) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (b) Mematuhi spesifikasi yang ditetapkan oleh	Pegawai Aset, Unit ICT JKSN/MSN

pengeluar bagi semua perkakasan yang diselenggara; (c) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	
070204 Peralatan Dibawa Keluar Premis	
(a) Peralatan ICT yang hendak dibawa keluar dari premis JKSM untuk tujuan rasmi, perlulah mendapat kelulusan CIO atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan (b) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	Pengguna, Pegawai Aset dan Ketua Jabatan
070205 Keselamatan Peralatan di Luar Premis	
Peralatan yang dibawa keluar dari premis JKSM/JKSN/MSN adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut:	Semua

(a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	
070206 Pelupusan Peralatan dan Kitar Semula	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau aset bernilai rendah yang dibekalkan oleh JKSM dan ditempatkan di JKSM sendiri dan Jabatan Kehakiman Syariah Negeri (JKSN/MSN). Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan JKSM/JKSN/MSN. Langkah-langkah seperti berikut hendaklah diambil: (a) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; (b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (c) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan	Pegawai Aset, Unit ICT JKSN/ MSN

peralatan tersebut; (d) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; (e) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speake*r dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di Jabatan; iii. Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab JKSM; v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *thumbdrive*, *flash drive*, *external drive* atau apa-apa bentuk peranti storan sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	

(f) Data dan maklumat dalam aset ICT yang akan dipinda milik atau dilupuskan hendaklah dihapuskan secara kekal; (g) Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan; (h) Maklumat lanjut berhubung pelupusan bolehlah merujuk kepada Pekeliling Perbendaharaan 5 Tahun 2007: Tatacara Pengurusan Aset Alih Kerajaan (PPP); (i) Maklumat lanjut berhubung pelupusan bolehlah merujuk kepada Tatacara Pengurusan Aset (TPA) terkini; (j) Pegawai Aset bertanggungjawab merekod butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam sistem inventori (Sistem Pengurusan Pemantauan Aset); dan (k) Pegawai Aset bertanggungjawab merekod butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Pemantauan Aset (SPPA).	
070207 Perkakasan Tanpa Penyeliaan (*Unattended User Equipment*)	
Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut:	Semua

(a) Tamatkan sesi aktif apabila selesai tugas; (b) *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; (c) Komputer meja, komputer riba atau pelayan disimpan dengan selamat daripada pengguna yang tidak dibenarkan.	
070208 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk dan Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkah-langkah perlu diambil termasuklah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; (c) Memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat. (d) E-mel masuk dan keluar hendaklah dikawal; dan	Semua

(e) Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	
0703 *Bring Your Own Device* (BYOD)	
Bring Your Own Device atau BYOD adalah kemudahan yang diberikan kepada kakitangan untuk membawa dan menggunakan peralatan mudah alih persendirian di persekitaran kerja Jabatan untuk tujuan rasmi. Peralatan mudah alih terdiri daripada telefon pintar, tablet dan laptop. Garis panduan yang menjelaskan polisi dan peraturan berkaitan BYOD adalah seperti dalam Tatacara Keselamatan ICT JKSN/JKSN/MSN.	Semua

BIDANG 08 **PENGURUSAN OPERASI**	
0801 Pengurusan Prosedur Operasi	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan ke atas kemudahan pemprosesan maklumat.	
080101 Pengendalian Prosedur	
(a) Semua prosedur keselamatan ICT yang diwujud, dikenalpasti dan masih digunapakai hendaklah didokumenkan, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua
080102 Kawalan Perubahan	
(a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;	Pentadbir Sistem

(b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat pada sistem sama ada secara sengaja atau pun tidak.	
080103 Perancangan Kapasiti	
(a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan (b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem Aplikasi, Pentadbir E-mel, Pentadbir Pusat Data dan Pengurus ICT

080104 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi	
(a) Perkakasan yang digunakan bagi kerja-kerja membangun, mengemaskini, menyelenggara dan menguji aplikasi (*staging/development*) perlu diasingkan daripada perkakasan yang digunakan sebagai *production server*. (b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pentadbir Sistem Aplikasi, Pengurus ICT
0802 Perisian Berbahaya (*Protection from Malware*)	
Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.	
080201 Perlindungan Daripada Perisian Berbahaya	
Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, *Intrusion Detection System* (IDS) an *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa;	Pentadbir Sistem, Pengguna

(c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; (d) Mengemas kini antivirus dengan *pattern* antivirus yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; dan (h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.	
0803 *Backup*	
Objektif: Memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.	
080301 *Backup* Maklumat (*Information Backup*)	
Memastikan sistem dapat dibangunkan semula dan digunakan setelah berlakunya bencana. *Backup* hendaklah dilakukan setiap kali berlakunya sebarang perubahan ke atas fail sistem, kod sistem, data dan fail-fail	Pentadbir Sistem

penting yang lain. *Backup* hendaklah direkodkan dan disimpan di luar kawasan premis (*off site*). (a) Membuat salinan pendua ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaharu; (b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi; (c) Menguji sistem *backup* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan (d) *Backup* hendaklah dilaksanakan secara berkala sama ada secara harian, mingguan, bulanan dan/atau tahunan. Kekerapan *backup* bergantung kepada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi.	
0804 Log dan Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
080401 *Event logging*	
Fail log hendaklah disimpan untuk tempoh sekurang-kurangnya enam (6) bulan. Jenis fail log bagi pelayan dan aplikasi yang perlu diaktifkan adalah seperti berikut:	Pentadbir Sistem

i. Fail log sistem pengoperasian; ii. Fail log servis (contoh: web); iii. Fail log aplikasi (*audit trail*); dan iv. Fail log rangkaian (contoh: *switch*, *firewall*, IPS). Pentadbir Sistem hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem Aplikasi hendaklah melaporkan kepada ICTSO dan CIO.	
080402 Perlindungan Log	
Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan.	Pentadbir Pusat Data, Pentadbir Sistem Aplikasi, ICTSO
080403 Log pentadbir dan Operator	
(a) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya	Pentadbir Sistem, ICTSO

perlu dipantau secara berkala; (b) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu; (c) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; (d) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan (e) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada ICTSO dan CIO.	
080404 *Clock Synchronisation*	
Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam JKSM/JKSN/MSN atau *Network Time Zone* (NTP) perlu diselaraskan kepada satu sumber waktu yang ditetapkan oleh SIRIM.	Pentadbir Pusat Data

0805 Kawalan Perisian Operasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
080501 Pemasangan Perisian Pada Sistem Operasi	
(a) Pengemaskinian perisian operasi, aplikasi dan *library program* hanya boleh dilakukan oleh pentadbir terlatih setelah mendapat kelulusan pengurusan; (b) Sistem operasi hanya boleh memegang "*executable code*"; (c) Penggunaan aplikasi dan sistem operasi hanya boleh dilaksanakan selepas ujian yang terperinci dan diperakui berjaya; (d) Setiap konfigurasi ke atas sistem perlu dikawal dan didokumentasikan melalui satu sistem kawalan konfigurasi. Konfigurasi hanya boleh dilaksanakan selepas mendapat persetujuan daripada pihak berkaitan; (e) Satu "*rollback*" strategi harus diadakan sebelum perubahan dilaksanakan; dan (f) Versi lama perisian perlu diarkibkan selaras dengan Dasar Pengurusan Rekod dan Arkib Elektronik, Jabatan Arkib Negara.	Pentadbir Sistem Aplikasi dan Pengurus ICT

0806 Kawalan Teknikal Keterdedahan (*Vulnerability*)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.	
080601 Kawalan Daripada Ancaman Teknikal	
Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memperoleh maklumat keterdedahan teknikal sistem maklumat yang digunakan; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT
080602 Kawalan Pemasangan Perisian	
(a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan pengguna di JKSM; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; dan (c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.	Pengguna, Pentadbir Sistem Aplikasi, ICTSO

0807 Pertimbangan Audit Sistem Maklumat	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
080701 Pematuhan Keperluan Audit/Kawalan Audit Sistem Maklumat	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.	Semua

BIDANG 09 **PENGURUSAN KOMUNIKASI**	
0901 Pengurusan Keselamatan Rangkaian	
Objektif: Memastikan perlindungan pemprosesan maklumat dalam rangkaian.	
090101 Kawalan Infrastruktur Rangkaian	
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas daripada risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (*FAC*) semasa pemasangan dan konfigurasi; (e) *Firewall* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian; (f) Semua trafik keluar dan masuk rangkaian hendaklah	Pengguna, Pentadbir Rangkaian dan ICTSO

melalui *firewall* di bawah kawalan BTMK, JKSM; (g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran daripada ICTSO; (h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat JKSM; (i) Memasang *Web Content Filtering* pada Internet Gateway untuk menyekat aktiviti yang dilarang; (j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan BTMK, JKSM adalah tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di JKSM sahaja dan penggunaan modem peribadi adalah dilarang sama sekali; (l) Kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya; (m) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan; (n) Menempatkan atau memasang antara muka (*interfaces*) yang bersesuaian di antara rangkaian JKSM, rangkaian agensi lain dan rangkaian awam; (o) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; (p) Memantau dan menguatkuasakan kawalan capaian	

pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; (q) Mengawal capaian fizikal dan logikal ke atas kemudahan *port* diagnostik dan konfigurasi jarak jauh; (r) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan JKSM; dan (s) Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan JKSM.	
090102 Keselamatan Perkhidmatan Rangkaian	
Pengurusan bagi semua perkhidmatan rangkaian dalaman atau sumber luaran yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenalpasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian.	Pentadbir Rangkaian, Pengurus ICT dan ICTSO
090103 Pengasingan Rangkaian	
Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian JKSM.	Pentadbir Rangkaian, Pengurus ICT dan ICTSO

0902 Pemindahan Maklumat	
Objektif: Memastikan keselamatan perpindahan/pertukaran maklumat dan perisian antara JKSM dan pihak luar terjamin.	
090201 Dasar dan Prosedur Pemindahan Maklumat	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar, prosedur dan kawalan pemindahan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan maklumat melalui sebarang jenis kemudahan komunikasi; (b) Terma pemindahan maklumat dan perisian di antara JKSM dengan pihak luar hendaklah dimasukkan di dalam Perjanjian; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan maklumat; dan (d) Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.	Pengguna, Pentadbir Rangkaian, Pentadbir E-mel dan ICTSO
090202 Perjanjian Mengenai Pemindahan Maklumat	
JKSM perlu mengambil kira keselamatan maklumat organisasi atau menandatangani perjanjian bertulis apabila berlaku pemindahan maklumat organisasi antara JKSM dengan pihak luar. Perkara yang perlu dipertimbangkan adalah:	CIO, ICTSO Pengurus ICT

(a) Tanggungjawab pengurusan bagi mengawal penghantaran dan penerimaan maklumat organisasi. (b) Prosedur bagi pengesanan maklumat organisasi semasa pemindahan maklumat. (c) Menggunapakai prinsip dan tatacara *escrow*. (d) Tanggungjawab dan liabiliti sekiranya berlaku insiden keselamatan maklumat seperti kehilangan data.	
090203 Pengurusan Mel Elektronik (E-mel)	
Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003 dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik (e-mel) adalah seperti berikut: (a) Menggunakan akaun e-mel Jabatan bagi urusan rasmi. Penggunaan akaun e-mel milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh JKSM; (c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; (d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel	Semua

penerima adalah betul; (e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10MB) semasa penghantaran. Kaedah pemampatan (*compress*) untuk mengurangkan saiz adalah disarankan; (f) Pengguna dilarang membuka e-mel daripada penghantar yang tidak diketahui atau diragui; (g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; (h) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; (i) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; (j) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; (k) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti *yahoo.com*, *gmail.com*, *streamyx.com.my* dan sebagainya) tidak digunakan untuk tujuan rasmi; dan (l) Pengguna hendaklah bertanggungjawab ke atas penyelenggaraan *mailbox* masing-masing.	

090204 Kerahsiaan dan *Non-Disclosure Agreement*	
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan dari semasa ke semasa.	CIO, ICTSO, Semua

BIDANG 10 **PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM**	
1001 Keperluan Keselamatan Sistem Maklumat	
Objektif: Memastikan keselamatan maklumat adalah merupakan sebahagian daripada proses pembangunan sistem. Ini merangkumi keperluan keselamatan maklumat apabila menggunakan rangkaian luar.	
100101 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat	
Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem sedia ada hendaklah mematuhi perkara-perkara berikut: (a) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Dasar Keselamatan ICT JKSM/JKSN/MSN; (b) Penyediaan rekabentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan (c) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data.	Pentadbir Sistem

100102 Keselamatan Perkhidmatan Aplikasi di Rangkaian Umum	
Maklumat aplikasi yang melalui rangkaian umum (*public networks*) hendaklah dilindungi daripada aktiviti penipuan dan pendedahan maklumat yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti berikut: (a) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*); (b) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; (c) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan (d) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	Pentadbir Rangkaian dan Pentadbir Sistem Aplikasi
100103 Melindungi Perkhidmatan Transaksi Aplikasi	
Maklumat yang terlibat dalam perkhidmatan transaksi hendaklah dilindungi daripada penghantaran yang tidak lengkap, *mis-routing*, pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan dan duplikasi mesej. Perkara yang perlu dipertimbangkan adalah seperti berikut:	ICTSO, Pentadbir Rangkaian dan Keselamatan, Pentadbir Sistem Aplikasi

(a) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi; (b) Memastikan semua aspek transaksi dipatuhi: i. Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan. ii. Mengekalkan kerahsiaan maklumat. iii. Mengekalkan privasi pihak yang terlibat. iv. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi. (c) Pihak yang mengeluarkan tandatangan digital adalah dilantik oleh Kerajaan.	
1002 Keselamatan Dalam Pembangunan Sistem	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.	
100201 Dasar Keselamatan Dalam Pembangunan Sistem	
Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan untuk perkembangan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti berikut: (a) Keselamatan persekitaran pembangunan; (b) Keselamatan pangkalan data; (c) Keselamatan dalam kawalan versi; dan (d) Bagi pembangunan secara sumber luaran, kebolehan	Pentadbir Sistem, ICTSO

pembekal untuk mengenalpasti kelemahan dan mencadangkan penambahbaikan dalam pembangunan sistem (sebelum penentuan pembekal).	
100202 Prosedur Kawalan Perubahan Sistem	
Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau sesebuah unit tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal; (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; dan (d) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.	Pentadbir Sistem Aplikasi, Pengurus ICT

100203 Kajian Teknikal Selepas Permohonan Perubahan Platform	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; (b) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan (c) Memastikan perubahan yang sesuai dibuat kepada Pelan Kesinambungan Perkhidmatan (PKP).	Pentadbir Sistem
100204 Sekatan Perubahan Pakej Perisian (*Software Packages*)	
Perubahan kepada pakej perisian adalah tidak digalakkan tetapi terhad kepada perubahan yang diperlukan dan semua perubahan hendaklah dikawal.	Pentadbir Sistem Aplikasi, Pengurus ICT
100205 Prinsip Kejuruteraan Keselamatan Sistem (S*ecure System Engineering Principles)*	
Prinsip-prinsip kejuruteraan keselamatan sistem hendaklah diwujudkan, didokumentasi, diselenggara dan digunapakai dalam pelaksanaan sistem. Keselamatan perlu diambilkira dalam semua peringkat pembangunan sistem termasuk pengkonsepan perisian, pengumpulan keperluan, reka bentuk, pelaksanaan, ujian,	Pentadbir Sistem, Pengurus ICT

penerimaan, pasang atur, penyelenggaraan dan pelupusan. Prinsip dan prosedur hendaklah sentiasa dikaji dari semasa ke semasa bagi memastikan keberkesanan kepada keselamatan maklumat.	
100206 Keselamatan Persekitaran Pembangunan Sistem	
Persekitaran pembangunan sistem hendaklah selamat bagi melindungi keseluruhan kitaran pembangunan sistem (*development lifecycle*).	Pentadbir Sistem, Pengurus ICT
100207 Pembangunan Sistem Secara Sumber Luaran	
Pembangunan perisian aplikasi secara sumber luaran perlu dipantau oleh BTMK, JKSM dan ICT JKSN/MSN. *Source code* adalah menjadi hak milik JKSM/JKSN/MSN.	Pentadbir Sistem Aplikasi, Pengurus ICT, ICTSO
100208 Pengujian Keselamatan Sistem	
(a) Pengujian keselamatan sistem hendaklah dijalankan semasa pembangunan; (b) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; (c) Membuat semakan pengesahan di dalam aplikasi untuk mengenalpasti kesilapan maklumat; dan (d) Menjalankan proses semak ke atas output data daripada setiap proses aplikasi untuk menjamin	Pentadbir Sistem, ICTSO

ketepatan.	
100209 Pengujian Penerimaan Sistem	
Pengujian penerimaan semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai.	Pengguna, Pentadbir Sistem, ICTSO
1003 Data Ujian	
100301 Perlindungan Data Ujian	
(a) Data dan aturcara yang hendak diuji perlu dipilih, dilindungi dan dikawal. (b) Pengujian hendaklah dibuat ke atas aturcara yang terkini. (c) Mengaktifkan audit log bagi merekodkan aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	

BIDANG 11 **HUBUNGAN DENGAN PEMBEKAL**	
1101 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal	
Objektif: Memastikan aset ICT JKSM/JKSN/MSN yang boleh dicapai oleh pembekal dilindungi.	
110101 Dasar Keselamatan Maklumat Untuk Pembekal	
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan bersama pihak pembekal bagi mengurangkan risiko kepada aset JKSM/JKSN/MSN. Perkara yang perlu dipertimbangkan adalah seperti berikut: (a) Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori; (b) Proses kitaran (*lifecycle*) yang seragam untuk menguruskan pembekal; (c) Mengawal dan memantau akses pembekal; (d) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian/kontrak; (e) Jenis-jenis obligasi kepada pembekal; (f) Pelan kontigensi (*contigency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; dan (g) Latihan Kesedaran Keselamatan kepada pembekal.	ICTSO, Pembekal

110102 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal	
Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan JKSM/JKSN/MSN.	Pembekal
110103 Kawalan Rantaian Bekalan Maklumat dan Komunikasi	
Perjanjian dengan pembekal hendaklah mengambilkira keperluan keselamatan maklumat rantaian pembekal (*Supply Chain*) bagi menangani risiko. Perkara-perkara yang perlu diambilkira adalah seperti berikut: (a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; (b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberi perkhidmatan atau pembekalan produk; dan (c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	ICTSO, Pembekal

1102 Pengurusan Penyampaian Perkhidmatan Pembekal	
110201 Pemantauan dan Kajian Perkhidmatan Pembekal	
JKSM/JKSN/MSN hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal. Perkara-perkara yang perlu diambil kira adalah seperti berikut: (a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; (b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan (c) Memaklumkan mengenai insiden keselamatan kepada pembekal dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	ICTSO, Pembekal
110202 Pengurusan Perubahan Perkhidmatan Pembekal	
Perkara yang perlu diambilkira adalah seperti berikut: (a) Perubahan dalam perjanjian dengan pembekal; (b) Perubahan yang dilakukan oleh JKSM/JKSN/MSN bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; (c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu,	ICTSO, Pembekal

	perubahan lokasi, pertukaran pembekal dan sub-kontraktor.	

BIDANG 12 **PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN**	
1201 Pengurusan dan Penambahbaikan Insiden Keselamatan Maklumat	
Objektif: Memastikan insiden keselamatan maklumat dikendalikan dengan cepat, teratur dan berkesan bagi meminimumkan kesan insiden dan mengenal pasti komunikasi serta kelemahan apabila berlaku insiden.	
120101 Tanggungjawab dan Prosedur	
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat.	ICTSO, Pengurus ICT dan JKSMCERT
120102 Mekanisme Pelaporan Insiden	
Insiden keselamatan ICT atau ancaman yang mungkin berlaku ke atas aset ICT yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada ICTSO. Selepas itu, ICTSO hendaklah melaporkan kepada pihak NACSA dengan kadar segera melalui e-mel aduan@nacsa.gov.my atau telefon 03-8064 4829. Perkara yang perlu dipertimbangkan adalah seperti berikut: (a) Maklumat didapati hilang, didedahkan kepada pihak-	ICTSO, Pengurus ICT dan JKSMCERT

pihak yang tidak diberi kuasa; (b) Maklumat disyaki hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa; (c) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (d) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; (e) Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan; (f) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (g) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka; dan (h) Carta Alir Pelaporan Insiden keselamatan ICT di JKSM seperti di **LAMPIRAN 3.** Prosedur pelaporan insiden keselamatan ICT berdasarkan: (a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam; dan (c) Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency	

Response Team (GCERT) oleh NACSA bertarikh 28 Januari 2019.	
120103 Melaporkan Kelemahan Keselamatan ICT	
Kakitangan dan pembekal yang menggunakan sistem dan perkhidmatan maklumat JKSM dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT	Semua
120104 Penilaian dan Keputusan Mengenai Aktiviti Keselamatan Maklumat	
Aktiviti keselamatan maklumat hendaklah dinilai dan diputuskan sama ada untuk diklasifikasikan sebagai insiden keselamatan maklumat.	ICTSO
120105 Pengurusan Maklumat Insiden Keselamatan ICT	
Insiden keselamatan maklumat hendaklah dikendalikan mengikut prosedur yang telah ditetapkan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; (b) Menjalankan kajian forensik sekiranya perlu; (c) Menghubungi pihak yang berkenaan dengan secepat mungkin; (d) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;	ICTSO, JKSMCERT

(e) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (f) Menyediakan pelan kontigensi dan mengaktifkan Pelan Kesinambungan Perkhidmatan; (g) Menyediakan tindakan pemulihan segera; dan (h) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	
120106 Pengalaman Dari Insiden Keselamatan Maklumat	
Pengetahuan dan pengalaman yang diperolehi daripada menganalisis dan menyelesaikan kes-kes insiden keselamatan maklumat perlu digunakan untuk mengurangkan kemungkinan dan kesan kejadian pada masa hadapan.	ICTSO, JKSMCERT
120107 Pengumpulan Bahan Bukti	
JKSM hendaklah menentukan prosedur untuk mengenalpasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti.	ICTSO, JKSMCERT

BIDANG 13 **ASPEK KESELAMATAN MAKLUMAT DALAM PENGURUSAN KESINAMBUNGAN PERKHIDMATAN**	
1301 Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
Objektif: Keselamatan maklumat hendaklah diberi penekanan dalam sistem pengurusan kesinambungan organisasi	
130101 Rancangan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
JKSM hendaklah membangunkan Pelan Kesinambungan Perkhidmatan (PKP) dan mengenal pasti aspek keselamatan maklumat. Ini bertujuan memastikan tiada gangguan kepada proses dalam penyediaan perkhidmatan organisasi dan mengenal pasti keselamatan maklumat pada lokasi kesinambungan perkhidmatan. Pelan ini mestilah diluluskan oleh CIO.	CIO, ICTSO

130102 Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan (PKP)	
Pengurusan Kesinambungan Perkhidmatan (PKP) adalah mekanisme bagi mengurus dan memastikan pihak berkepentingan (*stakeholder)* terhadap sistem penyampaian perkhidmatan dilindungi dan imej JKSM/JKSN/MSN terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan JKSM/JKSN/MSN di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan. Ketua Pengarah/Ketua Hakim Syarie adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT JKSM/JKSN/MSN. PKP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai keperluan keselamatan maklumat dalam membangunkan kesinambungan perkhidmatan; (b) Senarai aktiviti teras dan aset yang dianggap kritikal mengikut susunan keutamaan;	CIO, ICTSO

(c) Senarai personel JKSM dan pembekal berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai personel gantian juga hendaklah dikenalpasti bagi menggantikan personel yang tidak dapat hadir untuk menangani insiden; (d) Senarai lengkap maklumat yang perlu disalin pendua (*backup*) dan lokasi sebenar penyimpanannya; (e) Menetapkan arahan pemulihan maklumat dan kemudahan yang berkaitan; (f) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah terancam; (g) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan penyambungan semula perkhidmatan mengikut keutamaan; dan (h) Menguji tahap keselamatan kesinambungan perkhidmatan. Salinan dokumen PKP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan PKP hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.	

Ujian PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan pegawai yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. JKSM hendaklah memastikan salinan dokumen PKP sentiasa dikemas kini dan dilindungi seperti di lokasi utama. JKSM hendaklah mewujud, mendokumentasi, melaksana dan mengekalkan proses, prosedur serta kawalan untuk memastikan tahap keselamatan maklumat bagi kesinambungan perkhidmatan dalam situasi yang terancam. Perkara berikut perlu diberi perhatian: (a) Mengenalpasti aspek keselamatan dalam membangunkan pelan kesinambungan keselamatan; (b) Mengenalpasti semua aset, tanggungjawab, struktur organisasi dan menetapkan prosedur kecemasan atau pemulihan amalan terbaik; (c) Mengenalpasti peristiwa atau ancaman yang boleh mengakibatkan gangguan terhadap proses organisasi; (d) Mengenalpasti kemungkinan dan impak gangguan tersebut serta akibatnya terhadap keselamatan ICT; (e) Menjalankan analisis impak organisasi; (f) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat	

mungkin atau dalam jangka masa yang telah ditetapkan; (g) Mendokumentasikan proses dan prosedur yang telah ditetapkan; (h) Mengadakan program latihan secara berkala kepada warga JKSM mengenai prosedur kecemasan; (i) Membuat *backup* mengikut prosedur yang ditetapkan; dan (j) Menguji, menyelenggara dan mengemaskini pelan keselamatan ICT sekurang-kurangnya setahun sekali. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.	
130103 Mengkaji, Mengesah dan Menilai Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
JKSM hendaklah mengkaji, mengesah dan menilai tahap keselamatan maklumat yang diwujudkan dan disimpan di lokasi kesinambungan perkhidmatan keselamatan.	CIO, ICTSO
1302 *Redundancy*	
130201 Ketersediaan Kemudahan Pemprosesan Maklumat	
Kemudahan pemprosesan maklumat JKSM perlu mempunyai *redundancy* yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan *redundancy* perlu diuji (*failover*	ICTSO, BTMK

test) keberkesanannya dari masa ke semasa. Kemudahan pemprosesan maklumat JKSM perlu mempunyai *redundancy* yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan *redundancy* perlu diuji (*failover test*) keberkesanannya dari masa ke semasa.	

BIDANG 14 **PEMATUHAN**	
1401 Pematuhan Terhadap Keperluan Perundangan dan Perjanjian Kontrak	
Objektif: Meningkat dan memantapkan tahap keselamatan ICT bagi mengesan amalan ketidakpatuhan dan mengelak daripada pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	
140101 Mengenalpasti Undang-Undang dan Perjanjian Kontrak	
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenalpasti dan dipatuhi oleh kakitangan JKSM/JKSN/MSN dan pembekal. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di JKSM/JKSN/MSN dan pembekal: (1) Arahan Keselamatan; (2) Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan; (3) *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS); (4) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);	Semua

(5) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan; (6) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; (7) Surat Pekeliling Am Bil. 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; (8) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama) - Tatacara Penyediaan, Penilaian dan PenerimaanTender; (9) Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan; (10) Akta Tandatangan Digital 1997; (11) Akta Rahsia Rasmi 1972; (12) Akta Jenayah Komputer 1997; (13) Akta Hak Cipta (Pindaan) Tahun 1997; (14) Akta Komunikasi dan Multimedia 1998; (15) Perintah-Perintah Am; (16) Arahan Perbendaharaan; (17) Arahan Teknologi Maklumat 2007; (18) *Standard Operating Procedure* (SOP) ICT JKSM; (19) Etika Penggunaan E-mel dan Internet JKSM/JKSN/MSN; (20) Perintah-Perintah Am;	

(21) Arahan Perbendaharaan; (22) Surat Aku Janji; (23) Manual Prosedur Kerja (MPK) Jabatan; (24) MyPortfolio Pegawai; (25) Pelan Kesinambungan Perkhidmatan (PKP); (26) Surat Arahan MAMPU.702-1/1/7 Jld. 3 (48) bertarikh 23 Mac 2009 - Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan; (27) Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 - Penggunaan Media Jaringan Sosial di Sektor Awam; (28) Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk Tatacara Pengurusan Aset Alih Kerajaan (1PP); (29) Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2013 Dalam Sektor Awam; (30) Pekeliling Perkhidmatan Bil 5 2007 bertajuk Panduan Pengurusan Pejabat bertarikh 30 April 2007; (31) Prosedur Pengurusan Pelaporan Dan Pengendalian Insiden Keselamatan ICT JKSM/JKSN/MSN; dan (32) Rangka Kerja Keselamatan Siber Sektor Awam (RAKSSA).	

140102 Hak Harta Intelek (*Intellectual Property Rights* - IPR)	
Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan perlesenan di mana mematuhi had pengguna yang telah ditetapkan atau dibenarkan dan hanya menggunakan perisian yang mempunyai lesen yang sah.	Semua
140103 Perlindungan Rekod	
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.	Semua
140104 Privasi dan Perlindungan Maklumat Peribadi	
JKSM/JKSN/MSN hendaklah memberi jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.	Semua
140105 Kawalan Kriptografi	
Kawalan kriptografi hendaklah dilaksanakan mengikut perundangan, peraturan dan perjanjian kontrak.	Semua

1402 Kajian Keselamatan Maklumat	
Objektif: Untuk memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur JKSM/JKSN/MSN.	
140201 Kajian Bebas/Pihak Ketiga Terhadap Keselamatan Maklumat	
Penilaian keselamatan maklumat oleh pihak pembekal hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	CIO
140202 Pematuhan Dasar dan Standard/Piawaian	
JKSM/JKSN/MSN hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti di dalam polisi, piawaian dan keperluan teknikal.	CIO

GLOSARI

Antivirus	Perisian yang berupaya mengimbas dan menyekat malware jenis virus daripada merosakkan perkakasan komputer atau sistem aplikasi.
Arahan Keselamatan	Panduan mengenai peraturan-peraturan keselamatan yang perlu dipatuhi semua kakitangan Kerajaan.
Aset Alih	Aset yang boleh dipindahkan dari satu tempat ke tempat yang lain merangkumi Harta Modal dan Aset Bernilai Rendah.
Aset ICT	Peralatan ICT yang terdiri daripada perkakasan, perisian, perkhidmatan, data atau manusia.
Aset ICT Sewaan	Peralatan ICT yang diperoleh secara sewaan di bawah kontrak sewaan yang berkuat kuasa.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Juga dikenali sebagai jalur lebar yang merupakan ukuran atau jumlah data yang boleh dipindahkan melalui kawalan Komunikasi (contoh di antar cakera keras dan komputer dalam jangka masa yang ditetapkan.
***Chief Information Officer* (CIO)**	Pegawai yang dilantik dan bertanggungjawab ke atas pengurusan maklumat organisasi.
Clear Desk and Clear Screen	Tidak meninggalkan dokumen, data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skirn komputer apabila pengguna tidak berada di tempatnya.

***Closed-circuit Television System* (CCTV)**	Sistem televisyen yang digunakan secara komersil di mana satu sistem TV kamera video yang dipasang di dalam atau sekitar premis/pejabat bagi tujuan membantu pemantauan fizikal.
***Confidentiality, Integrity and Availability* (CIA)**	Terma yang merujuk kepada model asas kepada reka bentuk polisi keselamatan maklumat dalam satu-satu organisasi. *Confidentiality* bermaksud peraturan yang menghadkan capaian kepada maklumat, *integrity* bermaksud memastikan maklumat adalah tepat dan sahih dan *availability* pula ialah jaminan capaian maklumat oleh pihak yang dibenarkan sahaja.
Denial of Service	Insiden di mana berlaku halangan ke atas capaian kepada sesuatu perkhidmatan.
Downloading	Aktiviti memuat-turun fail, data, maklumat dan seumpamanya.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh pihak lain kecuali penerima yang sah.
Escrow	Satu pelan mitigasi memindahkan risiko keselamatan data/maklumat kepada pihak ketiga melalui terma dan perjanjian bagi mengurangkan risiko ancaman keselamatan ICT.
Firewall	Sistem yang direkabentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.

Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantara mesej melalui e-mel termasuk penyalahgunaan dan pencurian identity, pencurian maklumat (*information theft / espionage*) dan penipuan (*hoaxes*).
Hard Disk	Cakera keras yang digunakan untuk menyimpan data.
Hub	
ICT *Security Officer* (ICTSO)	Pegawai yang bertanggungjawab untuk menjaga keselamatan ICT.
Insiden Keselamatan	Musibah yang berlaku ke atas aset ICT merangkumi sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Internet	Sistem rangkaian seluruh dunia di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
Intranet	Rangkaian dalaman yang dimilik oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitanan dan mereka yang diberi kebenaran sahaja.
***Intrusion Detection System* (IDS)**	Sistem Pengesanan Pencerobohan yang berupaya mengesan aktiviti tidak berkaitan, tidak dikenali, kesilapan atau yang berbahaya kepada rangkaian.
***Intrusion Prevention System* (IPS)**	Sistem Pencegahan Pencerobohan yang merupakan teknologi keselamatan rangkaian sebagai perlindungan ke atas ancaman dengan memeriksa aliran trafik untuk mengesan dan menghalang *vulnerabitlity.*

Jawatankuasa Pemandu ICT (JPICT) JKSM/JKSN/MSN	Jawatankuasa yang melulus dan memantau pelaksanaan projek-projek ICT di JKSM/JKSN/MSN.
Jawatankuasa Keselamatan ICT JKSM/JKSN/MSN	Jawatankuasa yang melulus peraturan dan program keselamatan ICT yang dirancang untuk dilaksanakan di JKSM/JKSN/MSN.
JKSM	JKSM merangkumi Pejabat/Bahagian/Unit seperti berikut: 1. Pejabat Ketua Pengarah/Ketua Hakim Syarie JKSM 2. Pejabat Hakim Mahkaman Rayuan Syariah 3. Pejabat Ketua Pendaftar 4. Pejabat Pakar Rujuk 5. Bahagian Pendaftaran, Keurusetiaan dan Rekod 6. Bahagian Dasar dan Penyelidikan 7. Bahagian Pusat Sumber Maklumat dan Penerbitan 8. Bahagian Latihan 9. Bahagian Sokongan Keluarga 10. Bahagian Khidmat Pengurusan dan Sumber Manusia 11. Bahagian Teknologi Maklumat dan Komunikasi 12. Unit Integriti 13. Unit Komunikasi Korporat

JKSMCERT	Organisasi yang ditubuhkan untuk membantu agensi menguruskan pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Kakitangan JKSM/JKSN/MSN	Semua pegawai dan kakitangan JKSM/JKSN/MSN yang menggunakan Aset ICT yang disediakan oleh JKSM.
Kawasan Terperingkat	Meliputi kawasan premis atau sebahagian daripada premis di mana Rahsia Rasmi disimpan atau diuruskan atau di mana kerja terperingkat dijalankan.
Kriptografi	Kaedah penyulitan yang menukar data dan maklumat biasa kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
***Local Area Network* (LAN)**	Rangkaian Kawasan Setempat yang merujuk kepada rangkaian komputer dalaman JKSM/JKSN/MSN.
Lock	Aktiviti mengunci komputer bagi mengelakkan pihak lain menggunakan komputer tanpa kebenaran.
Log Out	Keluar daripada satu-satu sistem atau aplikasi komputer.
Malicious Code	Kod program yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan menyebabkan kerosakan dan/ atau pelanggaran polisi keselamatan seterusnya menjadi ancaman kepada komputer atau sistem. Ia melibatkan serangan virus, *trojan horse*, *worm*, *spyware* dan seumpamanya.

Pas Keselamatan	Pas keselamatan yang mengandungi maklumat pengenalan Pegawai yang dikeluarkan oleh pihak berwajib ke atas JKSM/JKSN/MSN.
Pas Keselamatan Pelawat	Pas kebenaran masuk premis yang diberikan kepada Pelawat selepas berdaftar di Kaunter Pertanyaan/Keselamatan JKSM/JKSN/MSN.
Pasukan CERT JKSM (JKSMCERT)	Jawatankuasa yang mengendalikan insiden keselamatan ICT sebagai *first level support* di peringkat Jabatan.
Pegawai Aset	Pegawai yang dilantik oleh Jabatan dan dipertanggungjawabkan untuk mengendalikan pengurusan aset JKSM/JKSN/MSN.
Pelan Kesinambungan Perkhidmatan (PKP)	Pelan atau perancangan pengurusan kesinambungan perkhidmatan yang meliputi segala sumber, proses, peranan dan tanggungjawab semua pihak terlibat yang diperlukan sebelum, semasa dan selepas sesuatu gangguan kepada sistem penyampaian perkhidmatan JKSM/JKSN/MSN.
Pelawat	Individu atau syarikat yang berurusan dengan JKSM/JKSN/MSN.
Pembekal	Individu atau syarikat yang memberi perkhidmatan ICT kepada JKSM/JKSN/MSN.
Perisian Aplikasi	Perisian atau pakej yang selalu digunakan seperti spreadsheet dan word processing atau sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.

Pihak Ketiga	Individu atau syarikat yang menyediakan perkhidmatan kepada JKSM/JKSN/MSN.
***Public-Key Infrastructure* (PKI)**	Kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan JKSM melindungi keselamatan komunikasi dan transaksi melalui Internet.
Router	Peralatan rangkaian yang berfungsi menghubungkan komputer daripada satu rangkaian ke satu rangkaian lain.
Sanitasi Data	Proses memadam atau menghapus data secara terancang, kekal dan menyeluruh sehingga tidak dapat dipulihkan walaupun menggunakan perisian pemulihan data.
Screen Saver	Animasi atau gambar yang diaktifkan selepas komputer tidak digunakan dalam satu jangka masa tertentu.
Server	Perkakasan atau perisian yang menyediakan dan mengurus pelbagai perkhidmatan seperti pangkalan data, aplikasi, storan, memori, integrasi dan sebagainya.
Sumber Luaran (*Outsource*)	Perkhidmatan luar untuk melaksanakan fungsi-fungsi ICT tertentu bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Telecommuting	Satu proses kerja yang membolehkan Pegawai ICT melaksanakan tugasan di mana sahaja dan dalam masa yang sama berhubung terus dengan sistem ICT JKSM/JKSN/MSN.

Threat	Gangguan atau ancaman daripada pelbagai sumber dan mekanisme yang mungkin atau tidak mungkin berlaku tetapi berupaya menyebabkan kerosakan kepada sistem komputer dan juga rangkaian.
***Uninterruptable Power Supply* (UPS)**	Peralatan yang terdiri daripada bateri yang menyimpan kuasa elektrik bagi mengambil alih penyambungan kuasa elektrik ketika berlaku gangguan bekalan kuasa elektrik utama.
Video Conference	Persidangan video yang membolehkan seorang atau lebih dari lokasi yang berbeza berkomunikasi dalam bentuk visual dan audio secara langsung.
Video Streaming	Aktiviti melayari video secara langsung dan berterusan di atas talian (*online*) tanpa perlu memuat-turun fail atau data video ke dalam peralatan komputer.
Virus	Kod aturcara yang bertujuan untuk merosakkan data atau sistem aplikasi.
***Wide Area Network* (WAN)**	Rangkaian Kawasan Luas yang merujuk kepada rangkaian komputer luar JKSM/JKSN/MSN.
Wireless LAN	Jaringan komputer LAN yang dihubungkan tanpa melalui kabel fizikal Internet.

RUJUKAN

1. Arahan Teknologi Maklumat 2007
2. Garis Panduan Permohonan Perkhidmatan EG-Net (v1)
3. Garis Panduan IT Outsourcing
4. The Malaysian Government Interoperability Framework For Open Source Software (MyGIFOSS)
5. Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia (MyMIS)
6. Pekeliling Am Bil. 1/2015 - Pelaksanaan Data Terbuka Sektor Awam
7. Pekeliling Kemajuan Perkhidmatan Awam Bil. 1/2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan
8. Pekeliling Kemajuan Perkhidmatan Awam Bil. 1/2015 - Pelaksanaan Data Terbuka Sektor Awam
9. Pekeliling Kemajuan Perkhidmatan Awam Bil. 2/2015 - Pengurusan Laman Web Agensi Sektor Awam
10. Pekeliling Kemajuan Perkhidmatan Awam Bil.3/2015 - Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan (Government Public Key Infrastructure - GPKI)
11. Surat Pekeliling Am Bil. 6/2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam
12. Surat Pekeliling Am Bil. 4/2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat (ICT) Sektor Awam
13. Surat Pekeliling Am Bil. 3/2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam

14. Surat Pekeliling Am Bil. 3/2015 – Garis Panduan Permohonan Kelulusan Teknikal Dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Agensi Sektor Awam

15. Pekeliling Transformasi Pentadbiran Awam Bil. 2/2017 - Pengurusan Perkhidmatan Rangkaian Telekomunikasi Bersepadu Kerajaan (1GovNet)

16. Pekeliling Transformasi Pentadbiran Awam Bil. 3/2017 - Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan (1GovUC)

17. Pekeliling Transformasi Pentadbiran Awam Bil. 2/2018 - Panduan Pengurusan Projek ICT Sektor Awam (PPrISA)

18. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan

19. Surat Arahan Ketua Pengarah MAMPU bertarikh 23 November 2007 - Langkah-langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan

20. Surat Arahan Ketua Pengarah MAMPU bertarikh 23 Mac 2009 - Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT Di Agensi-Agensi Kerajaan

21. Surat Arahan Ketua Pengarah MAMPU bertarikh 19 November 2009 - Penggunaan Media Jaringan Sosial Di Sektor Awam

22. Surat Arahan Ketua Pengarah MAMPU bertarikh 24 November 2010 - Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 270012007 dalam Sektor Awam

23. Surat Arahan Ketua Pengarah MAMPU bertarikh 24 November 2010 - Garis Panduan Penggunaan ICT Ke Arah ICT Hijau Dalam Perkhidmatan Awam

24. Surat Arahan Ketua Pengarah MAMPU bertarikh 5 Mac 2010 – Panduan Pelaksanaan Pengurusan Projek ICT Sektor Awam

25. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Julai 2010 – Pemantapan Penggunaan Dan Pengurusan E-Mel Di Agensi-Agensi Kerajaan

26. Surat Arahan Ketua Pengarah MAMPU bertarikh 22 Januari 2010 – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam

27. Surat Arahan Ketua Pengarah MAMPU bertarikh 8 April 2011 – Amalan Terbaik Penggunaan Media Jaringan Sosial

28. Surat Arahan Ketua Pengarah MAMPU bertarikh 26 Mei 2015 – Pelaksanaan Rasionalisasi Laman Web Sektor Awam

29. Surat Arahan Ketua Pengarah MAMPU bertarikh 12 Ogos 2015 – Pelaksanaan Penilaian Risiko Keselamatan Maklumat Menggunakan MyRAM App. 2.0 Di Agensi Sektor Awam

30. Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) oleh NACSA bertarikh 28 Januari 2019

31. Dasar Keselamatan ICT JKSM/JKSN/MSN Versi 3.0

Lampiran 1

Surat Akuan Pematuhan

Dasar Keselamatan ICT JKSM/JKSN/MSN

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT JKSM/JKSN/MSN

Nama : ……..

No. Kad Pengenalan : …….....

Jawatan : ……..

Jabatan : ……..

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT;

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

……

( )

Tarikh :

Pengesahan Pegawai Keselamatan ICT

……

( )

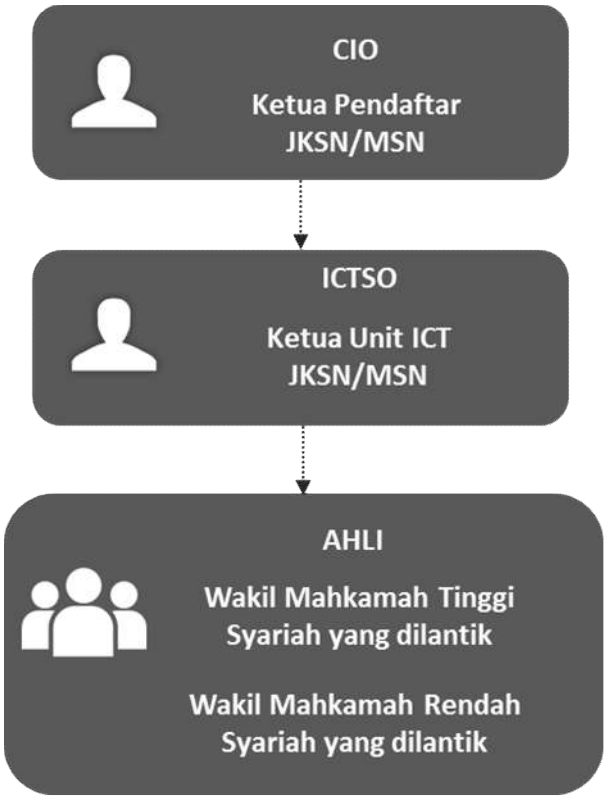
b.p : Ketua Pengarah / Ketua Hakim Syarie

Tarikh :

LAMPIRAN 2

Struktur Organisasi Jawatankuasa Keselamatan ICT JKSM

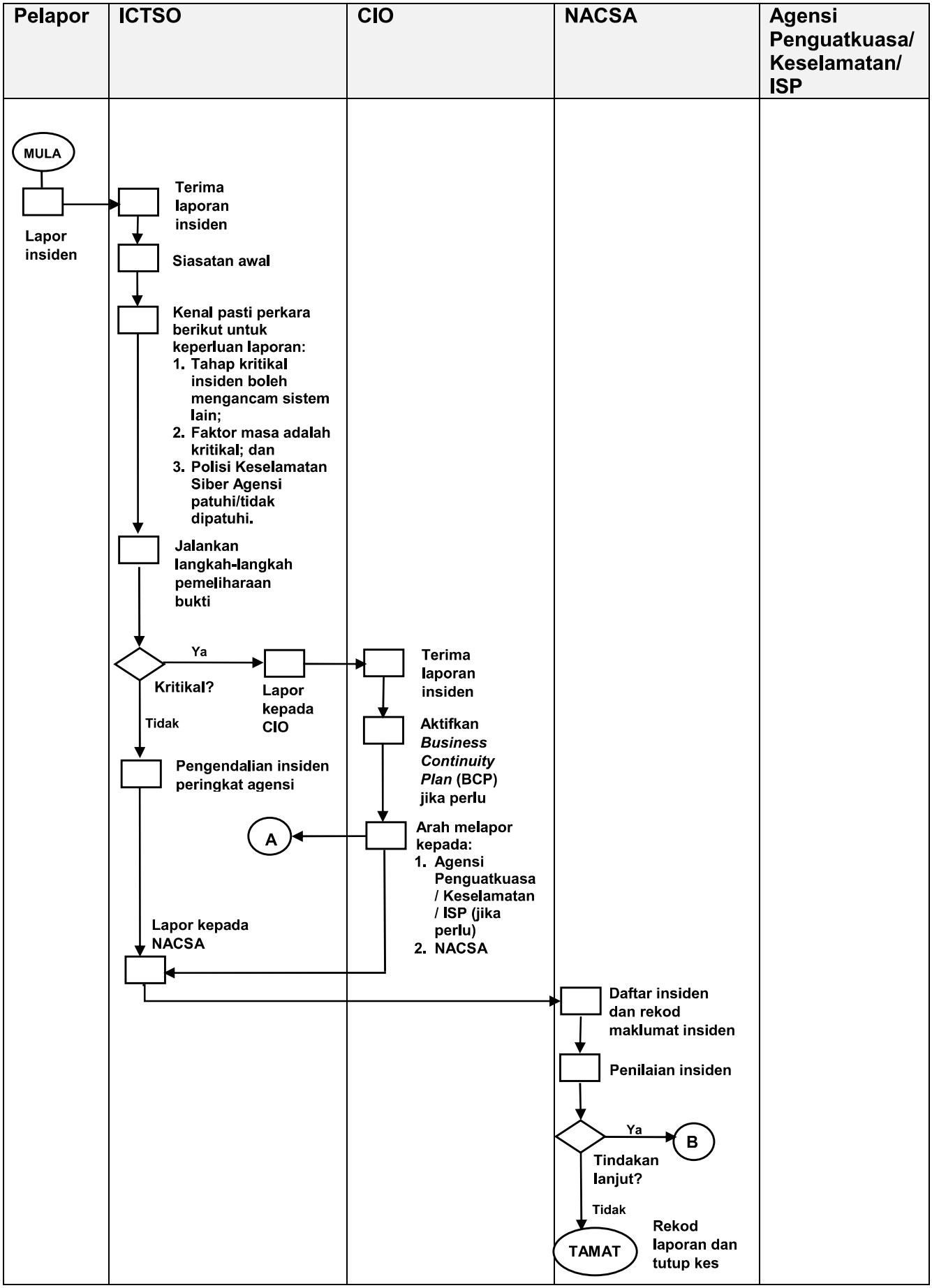
Struktur Organisasi Jawatankuasa Keselamatan ICT JKSN/ MSN



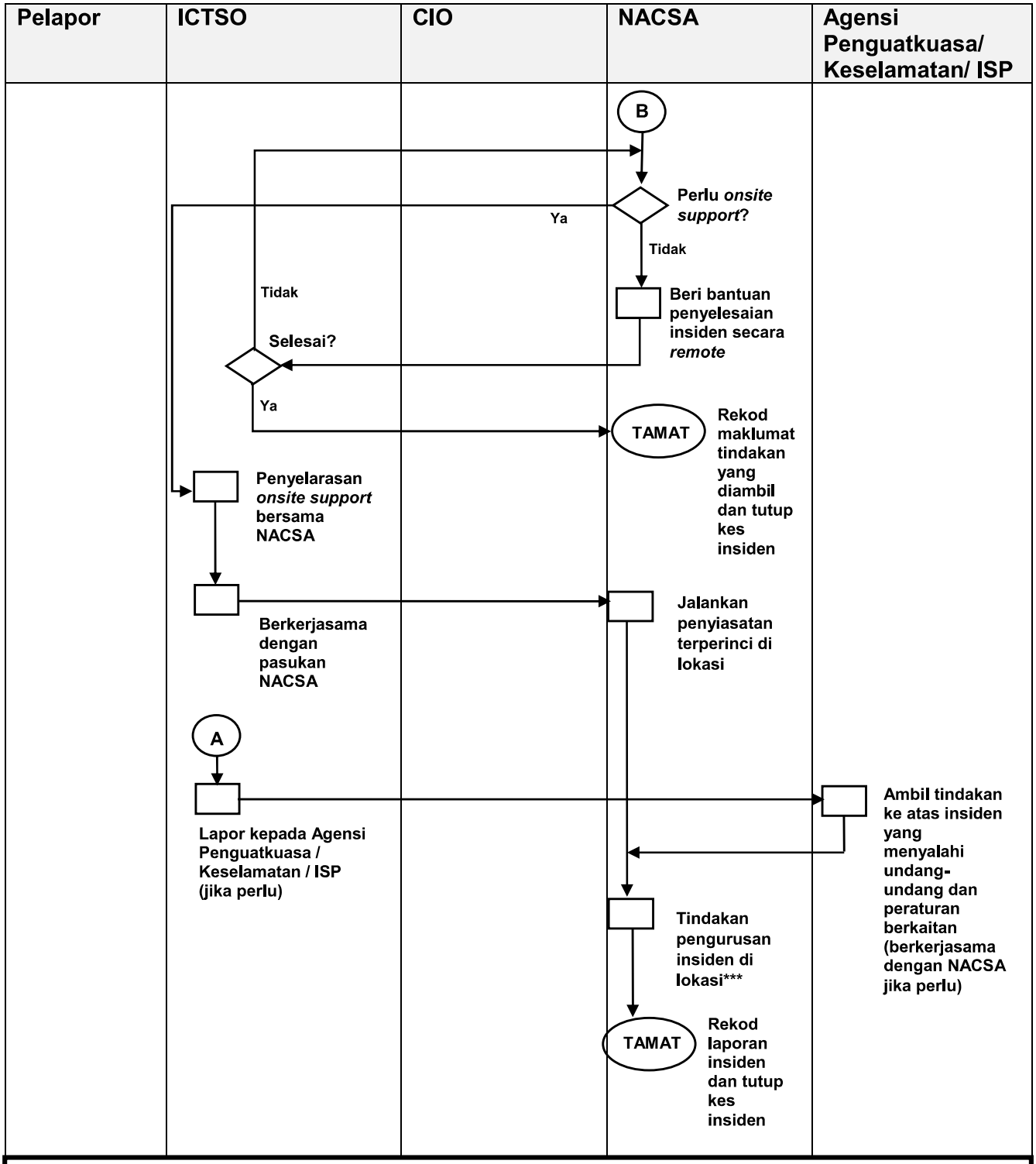
LAMPIRAN 3

Carta Alir Pelaporan Insiden Keselamatan ICT JKSM/JKSN/MSN

Carta Alir Proses Kerja Pelaporan Insiden Keselamatan Siber



Carta Alir Proses Kerja Pelaporan Insiden Keselamatan Siber



***** Tindakan pengurusan insiden di lokasi:**

1. Kawal kerosakan;
2. Baik pulih minima dengan segera;
3. Siasat insiden dengan terperinci;
4. Analisis impak (Business Impact Analysis);
5. Hasilkan laporan insiden;
6. Bentang dan kemukakan laporan kepada agensi; dan
7. Selaraskan tindakan di antara agensi dan Agensi Penguatkuasa/Keselamatan/ISP (jika berkenaan).