POLISI KESELAMATAN SIBER 1.0

JABATAN KEHAKIMAN SYARIAH MALAYSIA

POLISI KESELAMATAN SIBER

JABATAN KEHAKIMAN SYARIAH MALAYSIA

TUJUAN

1. Dokumen ini bertujuan untuk menjelaskan Polisi Keselamatan Siber (PKS) Jabatan Kehakiman Syariah Malaysia (JKSM) serta perkara-perkara yang berkaitan yang perlu difahami dan dipatuhi warga JKSM, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT JKSM.

LATAR BELAKANG

2. Berpandukan kepada dokumen Rangka Kerja Keselamatan Siber Sektor Awam (RAKSSA) yang berkuat kuasa pada 1 April 2016, JKSM telah telah mengambil inisiatif terhadap keselamatan siber yang merangkumi aset ICT bagi meminimumkan kesan gangguan ke atas sistem penyampaian perkhidmatan JKSM secara khususnya.

3. PKS ini dibangunkan selaras dengan perkembangan garis panduan keselamatan siber khususnya maklumat dan data yang semakin berkembang di Malaysia seterusnya menggantikan Dasar Keselamatan ICT JKSM sedia ada.

BIDANG KAWALAN

4. Terdapat 14 bidang kawalan keselamatan yang terkandung di dalam PKS JKSM versi 1.0 ini.

Kawalan	Tajuk
01	Polisi Keselamatan
02	Organisasi Keselamatan Maklumat
03	Keselamatan Sumber Manusia
04	Pengurusan Aset
05	Kawalan Capaian
06	Kawalan Kriptografi
07	Keselamatan Fizikal dan Persekitaran
08	Keselamatan Operasi
09	Keselamatan Komunikasi
10	Perolehan, Pembangunan dan Penyelenggaraan Sistem
11	Hubungan Dengan Pembekal
12	Risiko dan Pengurusan Pengendalian Insiden Keselamatan
13	Keselamatan Maklumat bagi Pengurusan Kesinambungan Perkhidmatan
14	Pematuhan

TANGGUNJAWAB DAN PERANAN

5. KP/KHS / CDO / ICTSO hendaklah bertanggungjawab sepenuhnya dalam melaksanakan kesemua bidang kawalan yang digariskan di dalam PKS JKSM dan memastikan polisi ini dipatuhi semua warga JKSM, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT JKSM.

6. Polisi ini hendaklah disemak dan dipinda pada masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan dan polisi Kerajaan bagi memastikan dokumen sentiasa relevan. Peranan dan tanggungjawab setiap individu yang terlibat dalam mencapai objektif polisi diterangkan dengan lebih jelas di dalam Kawalan 02 - Organisasi Keselamatan Maklumat.

PEMAKAIAN

7. Polisi ini terpakai kepada semua warga JKSM, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT JKSM.

TARIKH BERKUAT KUASA

8. Polisi ini berkuat kuasa mulai tarikh dikeluarkan dan terpakai selama 2 tahun melainkan jika terdapat arahan terkini atau perkembangan baharu yang memerlukannya dikaji semula dan dikemas.

PERTANYAAN

9. Sebarang pertanyaan mengenai polisi ini boleh dikemukakan kepada:

Pengarah
Bahagian Teknologi Maklumat dan Komunikasi
Jabatan Kehakiman Syariah Malaysia
Blok C, Kompleks Islam Putrajaya
No. 20, Jalan Tunku Abdul Rahman, Presint 3
62100 Putrajaya
No Telefon: 03-88709222
Faks: ukde@esyariah.gov.my

PENGUATKUASAAN

10. **PKS JKSM** ini berkuat kuasa mulai tarikh dokumen ini dikeluarkan. Dengan berkuat kuasanya PKS 1.0 ini, maka DKICT versi 4.0 bertarikh 1 November 2019 terbatal.

JKSM.100-12/1/2 JLD 2 ( )

Dikeluarkan pada 21 Julai 2023

POLISI KESELAMATAN SIBER 1.0

JABATAN KEHAKIMAN SYARIAH MALAYSIA

KANDUNGAN

KELULUSAN DOKUMEN

Disediakan oleh	..... **(EFFAH BINTI ABU BAKAR)** **Penolong Pengarah Kanan** Tarikh: 04.07.2023
Disemak dan disahkan oleh	..... **(MOHD RAZALAN BIN KAMAL)** **Pengarah Bahagian Teknologi Maklumat dan Komunikasi** Tarikh: 04.07.2023
Diluluskan oleh	..... **(HAJI NASSIR BIN ABDUL AZIZ)** **Ketua Pendaftar JKSM** Tarikh: 07.07.2023

SEJARAH DOKUMEN

Versi	Perkara	Tarikh Diluluskan	Pihak Meluluskan
1.0	Polisi Keselamatan Siber JKSM versi 1.0	18 Mei 2023	Jawatankuasa Keselamatan ICT JKSM

PENGENALAN

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

OBJEKTIF

PKS JKSM diwujudkan untuk menjamin kesinambungan urusan JKSM dengan meminimumkan kesan insiden keselamatan ICT. Polisi ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi Jabatan.

Objektif utama PKS JKSM diwujudkan adalah seperti berikut:

1. Memastikan kelancaran operasi JKSM/JKSN/MSN dan meminimumkan kerosakan atau kemusnahan.
2. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan daripada segi kerahsiaan, integriti, tidak boleh disangkal, keboleh sediaan dan kesahihan (CIA).
3. Mencegah atau salah guna aset JKSM.
4. Memperkemas pengurusan risiko keselamatan ICT.
5. Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal.

TADBIR URUS PKS JKSM

Bagi memastikan keberkesanan dan kejayaan pelaksanaan polisi, satu struktur tadbir urus telah diwujudkan seperti berikut:

ASET ICT JKSM

Aset ICT JKSM merangkumi aspek Maklumat, Aliran Data, Platform Aplikasi dan Perisian, Peranti Fizikal dan Sistem, Sistem Luaran dan Sumber Luaran. Perincian aset seperti berikut:

(a) Maklumat

Semua penyedia perkhidmatan ICT di dalam JKSM hendaklah mengenal pasti kategori maklumat yang dijana atau dikendalikan dan hendaklah mengasingkannya mengikut kategori berikut:

(i) Maklumat Rahsia Rasmi

Maklumat Rahsia Rasmi mempunyai erti yang diberikan kepadanya di bawah Akta Rahsia Rasmi 1972 (Akta 88). Apa-apa suratan yang dinyatakan di dalam Jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain

sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah Seksyen 2B Akta Rahsia Rasmi 1972.

(ii) Maklumat Rasmi

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

(iii) Maklumat Pengenalan Peribadi

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

(iv) Data Terbuka

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

JKSM adalah tidak bertanggungjawab bagi apa-apa kehilangan atau kerugian yang disebabkan oleh penggunaan mana-mana maklumat yang diperoleh daripada Data Terbuka yang dikongsi.

(b) Aliran Data

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

i. Saluran komunikasi dan aliran data antara sistem di JKSM.
ii. Saluran komunikasi dan aliran data ke sistem luar.
iii. Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

(c) Platform Aplikasi dan Perisian

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

(d) Peranti Fizikal dan Sistem

Semua peranti fizikal dan sistem hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala atau mengikut kesesuaian. Senarai adalah termasuk namun tidak terhad kepada:

i. Pelayan
ii. Peranti/Peralatan Rangkaian
iii. Komputer Meja/Komputer Riba
iv. Telefon/ Peranti Pintar
v. Media Storan
vi. Peranti dengan sambungan ke rangkaian. Contohnya: mesin pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV)
vii. Peranti persendirian yang digunakan untuk urusan rasmi Kerajaan
viii. Peranti pengesahan

(e) Sistem Luaran

Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dinilai secara berkala atau mengikut kesesuaian. Sistem luaran ialah sistem bukan milik JKSM yang dihubungkan dengan sistem JKSM.

(f) Sumber Luaran

Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkod dan dinilai secara berkala atau mengikut kesesuaian. Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi JKSM. Contoh perkhidmatan sumber luaran adalah seperti berikut:

(i) Perisian sebagai Satu Perkhidmatan (*Software as a Service* - SaaS)
(ii) Platform sebagai Satu Perkhidmatan (*Platform as a Service* - Paas)
(iii) Infrastruktur sebagai satu Perkhidmatan (*Infrastructure as a Service* - IaaS)
(iv) Storan Pengkomputeran Awan (*Cloud Computing*)
(v) Pemantauan Keselamatan (*Security Monitoring*)

RISIKO

JKSM hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat daripada ancaman dan kerentanan yang semakin meningkat. JKSM 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 hendaklah dilaksanakan secara berkala ke atas sistem maklumat JKSM 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

termasuk pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

(a) Kerentanan

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

(b) Ancaman

JKSM hendaklah mengenal pasti kedua-dua ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

(c) Impak

JKSN hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan sebagai impak teknikal dan impak berkaitan dengan fungsi Jabatan.

(d) Tahap Risiko

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

(e) Pengolahan Risiko

Pengolahan risiko hendaklah dikenal pasti untuk menentukan sama ada perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya.

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

(i) Teknologi

Teknologi hendaklah dikenal pasti untuk mengelak atau mengurangkan risiko. Contohnya *firewall* digunakan untuk mengehadkan capaian logikal kepada sistem tertentu.

(ii) Proses

JKSM hendaklah sekiranya perlu untuk pengolahan risiko, membangunkan atau mengemas kini Perekayasaan Proses (*Process Engineering*), Prosedur Operasi Standard (*Standard Operating Procedure*) dan polisi.

(iii) Manusia

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

(f) Pengurusan Risiko

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

(i) Mengenal pasti kerentanan
(ii) Mengenal pasti ancaman
(iii) Menilai risiko
(iv) Menentukan pengolahan risiko

(v) Memantau keberkesanan pengolahan risiko

(vi) Memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima

Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya **sekali setahun** dalam Mesyuarat Jawatankuasa Keselamatan ICT JKSM.

PRINSIP KESELAMATAN

PKS JKSM merangkumi perlindungan ke atas semua bentuk maklumat elektronik dan bukan elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan keboleh sediaan kepada semua pengguna yang dibenarkan.

Objektif utama keselamatan maklumat adalah seperti berikut:

(i) Kerahsiaan (*Confidentiality*)

(ii) Integriti (*Integrity*)

(iii) Tanpa Sangkalan (*Non-Repudiation*)

(iv) Kesahihan (*Authenticity*)

(v) Ketersediaan (*Availability*)

Bagi mencapai objektif tersebut, JKSM hendaklah melaksanakan prinsip keselamatan seperti berikut:

(a) Prinsip “Perlu Tahu”

JKSM hendaklah melaksanakan mekanisme bagi memberi kebenaran capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah berdasarkan prinsip “Perlu-Tahu” yang memberikan capaian maklumat yang diperlukan untuk melaksanakan tugasnya sahaja.

(b) Hak Keistimewaan Minimum

Hak keistimewaan kepada pengguna hanya diberi pada tahap yang paling minimum untuk menjalankan tugasnya.

(c) Pengasingan Tugas

JKSM hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

(d) Kawalan Capaian Berdasarkan Peranan Pengauditan

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

(e) Peminimuman Data

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

TEKNOLOGI

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

(a) Peringkat Pemprosesan Data

(i) Data-dalam-simpanan

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

(ii) Data-dalam-pergerakan

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

(iii) Data-dalam-penggunaan

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

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

(iv) Perlindungan Ketirisan Data

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

(b) Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, JKSM hendaklah menggunakan teknologi dan kawalan keselamatan yang dapat melindungi data di semua peringkat saluran pemprosesan dan bagi semua elemen dalam persekitaran pengkomputeran.

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

PROSES

Warga JKSM hendaklah melindungi keselamatan siber dengan melaksanakan perkara-perkara berikut:

(a) Konfigurasi Asas

Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem. Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

(b) Kawalan Perubahan Konfigurasi

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

Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.
Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

(c) Sandaran

Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan.

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

(d) Kitaran Pengurusan Aset

(i) Pindah

Pemindahan hak milik aset berlaku dalam keadaan berikut:

- Warga JKSM meninggalkan agensi disebabkan oleh persaraan, peletakan jawatan atau penugasan semula;
- Aset yang dikongsi untuk kegunaan sementara;
- Pemberian aset kepada agensi lain; dan

- Aset dikembalikan setelah tamat tempoh sewaan.

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

(ii) Pelupusan

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

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

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

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

(iii) Kitaran Hayat

Kitaran hayat data hendaklah diuruskan mengikut Akta 629. Akta 629 memberikan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

MANUSIA

Warga JKSM, pembekal dan pihak-pihak yang berkepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

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

(a) Kompetensi Pengguna

Kompetensi pengguna termasuk:

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

(ii) Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga JKSM berhubung alat-alat keselamatan berkaitan untuk memastikan warga JKSM untuk melaksanakan tugas harian mereka.

Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian mendalam.

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

(b) Kompetensi Pelaksana

(i) Warga JKSM yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

(ii) Pegawai Keselamatan ICT hendaklah memenuhi syarat-syarat berikut:

- Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.
- Memenuhi keperluan pembelajaran berterusan.
- Menimba pengalaman yang mencukupi dalam bidang keselamatan siber.
- Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.

Pegawai Keselamatan ICT yang dilantik oleh JKSM hendaklah memenuhi keperluan kompetensi di atas. Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan ICT di JKSM.

(c) Peranan

(i) Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.

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

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

(iv) Warga JKSM yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Jabatan dikembalikan sekiranya berlaku perubahan peranan.

(v) Warga JKSM yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan yang berkaitan seperti tersenarai dalam senarai aset dalam Nota Serah Tugas.

(vi) Warga JKSM lain yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Jabatan.

PENYATAAN POLISI KESELAMATAN SIBER JKSM

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

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

(i) Kerahsiaan

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

(ii) Integriti

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

(iii) Tidak Boleh Disangkal

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

(iv) Kesahihan

Data dan maklumat hendaklah dipastikan kesahihannya.

(v) Ketersediaan

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

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

PELAN PENGURUSAN KESELAMATAN MAKLUMAT

Setiap projek ICT di JKSM hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain.

Pelan ini hendaklah dibangunkan berpandukan kepada dokumen Rangka Kerja Keselamatan Siber Sektor Awam (RAKSSA), Polisi Keselamatan Siber JKSM (PKS JKSM) dan juga surat pekeliling/arahan terkini untuk menangani isu-isu operasi projek.

Pelan ini hendaklah mengenal pasti perlindungan data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data.

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

(a) Peranti Pengkomputeran Peribadi

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

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

(b) Peranti Rangkaian

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

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

(c) Aplikasi

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

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

(d) Pelayan

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

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

(e) Persekitaran Fizikal

Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan aset ICT.

JKSM hendaklah merujuk ke CGSO untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

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

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

[Halaman ini sengaja dibiarkan kosong]

0101 Hala Tuju Pengurusan Keselamatan Maklumat

KAWALAN

01

POLISI KESELAMATAN

KAWALAN 01

POLISI KESELAMATAN MAKLUMAT

Sub-Kawalan	Tanggungjawab
0101 Hala Tuju Pengurusan Keselamatan Maklumat	
Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan JKSM dan perundangan yang berkaitan.	
010101 Polisi Keselamatan Maklumat	
Satu set dasar untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan JKSM kepada warga Jabatan, pengguna dan pembekal. Pelaksanaan polisi ini akan dijalankan oleh Ketua Pengarah JKSM dibantu oleh Jawatankuasa Keselamatan ICT JKSM. Jawatankuasa Keselamatan ICT JKSN terdiri daripada Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO) dan ahli-ahli yang dilantik oleh Ketua Pengarah/Ketua Hakim Syarie.	Ketua Pengarah/ Ketua Hakim Syarie
010102 Semakan Polisi Keselamatan	
PKS JKSM mestilah disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan, dan polisi Kerajaan. Berikut adalah prosedur semakan semula PKS JKSM: a) Mengenal pasti dan menentukan perubahan yang diperlukan. b) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan Jawatankuasa Keselamatan ICT (JKICT) JKSM. c) Memaklumkan cadangan pindaan telah dipersetujui oleh JKICT kepada JPICT bagi tujuan pengesahan,	ICTSO, JKICT

Sub-Kawalan	Tanggungjawab
d) Memaklumkan pindaan yang telah disahkan oleh JPICT kepada semua kakitangan JKSM/JKSN/MSN, pengguna dan pembekal. Polisi ini hendaklah disemak semula secara berkala sekurang-kurangnya **dua tahun sekali** atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	
010103 Pelaksanaan dan Pematuhan Polisi	
Polisi ini hendaklah dihebahkan kepada warga JKSM, pengguna dan pembekal. Polisi mestilah dibaca, difahami dan dipatuhi oleh semua warga JKSM, pengguna dan pembekal. Akuan pematuhan hendaklah dilaksanakan sekali setiap tahun bagi memastikan semua warga JKSM, pengguna dan pembekal memahami dan mematuhi polisi yang digariskan.	Warga JKSM, Pengguna, Pembekal

KAWALAN

02

ORGANISASI KESELAMATAN MAKLUMAT

KAWALAN 02

ORGANISASI KESELAMATAN MAKLUMAT

Sub-Kawalan	Tanggungjawab
0201 Struktur Organisasi Dalaman	
Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber JKSM.	
020101 Peranan dan Tanggungjawab	
(A) Ketua Pengarah Peranan dan tanggungjawab Ketua Pengarah / Ketua Hakim Syarie adalah seperti berikut: 1. Membaca, memahami dan mematuhi PKS JKSM. 2. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah PKS JKSM. 3. Memastikan semua pengguna mematuhi PKS JKSM. 4. Memastikan semua keperluan organisasi seperti sumber kewangan, sumber manusia dan perlindungan keselamatan adalah mencukupi. 5. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam PKS JKSM.	Ketua Pengarah/ Ketua Hakim Syarie
(B) Ketua Pegawai Digital Jawatan Ketua Pegawai Digital (*Chief Digital Officer* - CDO) JKSM disandang oleh Ketua Pendaftar JKSM dan dilantik secara rasmi oleh Ketua Pengarah/Ketua Hakim Syarie JKSM. Peranan dan tanggungjawab CDO adalah seperti berikut:	CDO

Sub-Kawalan	Tanggungjawab
1. Membaca, memahami dan mematuhi PKS JKSM. 2. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT JKSM. 3. Memastikan kawalan keselamatan maklumat dalam organisasi diseragamkan dan diselaraskan dengan sebaiknya. 4. Menentukan keperluan keselamatan ICT. 5. Mempengerusikan Jawatankuasa Keselamatan ICT (JKICT). 6. Memastikan program-program kesedaran mengenai keselamatan ICT dilaksanakan.	
(C) Pegawai Keselamatan ICT (ICTSO) Jawatan ICTSO JKSM disandang oleh Pengarah Bahagian Teknologi Maklumat dan Komunikasi (BTMK) dan dilantik secara rasmi oleh Ketua Pengarah/Ketua Hakim Syarie JKSM. Peranan dan tanggungjawab ICTSO adalah seperti berikut: 1. Membaca, memahami dan mematuhi PKS JKSM. 2. Mengurus keseluruhan program keselamatan ICT JKSM. 3. Menguatkuasakan pelaksanaan PKS JKSM. 4. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS JKSM. 5. Menjalankan pengurusan risiko dan audit keselamatan ICT berpandukan *Malaysian Public Sector Management of Information and Communication* (MyMIS) untuk mengenal pasti ketidakpatuhan kepada PKS JKSM.	ICTSO

Sub-Kawalan	Tanggungjawab
6. Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlaku ancaman keselamatan ICT dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian. 7. Melaporkan insiden keselamatan ICT kepada pihak NACSA dan seterusnya membantu dalam penyiasatan atau pemulihan. 8. Melaporkan insiden keselamatan ICT kepada CDO bagi insiden yang memerlukan Pelan Kesinambungan Perkhidmatan (PKP). 9. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera. 10. Memastikan pematuhan PKS JKSM oleh pihak luar seperti pembekal dan kontraktor yang mencapai dan menggunakan aset ICT JKSM untuk tujuan penyelenggaraan dan sebagainya. 11. Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan. 12. Memastikan Pelan Strategik Pendigitalan JKSM mengandungi aspek keselamatan.	
(D) Pengurus ICT Pengurus ICT JKSM/JKSN/MSN ialah Pengarah Bahagian Teknologi Maklumat dan Komunikasi (BTMK), JKSM. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: 1. Membaca, memahami dan mematuhi PKS JKSM.	Pengurus ICT

Sub-Kawalan	Tanggungjawab
2. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan JKSM. 3. Menentukan kawalan akses pengguna terhadap aset ICT JKSM. 4. Melaporkan sebarang penemuan mengenai keselamatan ICT kepada JKICT JKSM. 5. Menyimpan rekod atau laporan terkini tentang ancaman keselamatan ICT JKSM. 6. Memastikan semua warga JKSM, pengguna dan pembekal yang terlibat dengan aset ICT JKSM mematuhi dasar, piawaian dan garis panduan keselamatan ICT.	
(E) Pengarah Bahagian Pengarah Bahagian ialah pegawai yang memegang jawatan sebagai Pengarah Bahagian dan Ketua Unit di JKSM. Peranan dan tanggungjawab Pengarah Bahagian ialah melaksanakan keperluan PKS JKSM dalam operasi semasa seperti berikut: 1. Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu. 2. Pembelian atau peningkatan perisian dan sistem komputer. 3. Perolehan teknologi dan perkhidmatan komunikasi baharu. 4. Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan.	Pengarah Bahagian

Sub-Kawalan	Tanggungjawab
5. Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan dan pelan pengurusan keselamatan maklumat Kerajaan yang berkuat kuasa.	
(F) Pentadbir Sistem Pentadbir Sistem di JKSM ialah Pegawai Teknologi Maklumat di JKSM. Pentadbir Sistem terdiri seperti berikut: 1. Pentadbir Rangkaian dan Keselamatan. 2. Pentadbir Pangkalan Data. 3. Pentadbir Portal/ Laman Web Rasmi (*Webmaster*). 4. Pentadbir Pusat Data. 5. Pentadbir Sistem Aplikasi. 6. Pentadbir E-mel. 7. Pentadbir Aset ICT. 8. Pentadbir Media Sosial. Pentadbir Sistem hendaklah menjadi Ahli Jawatankuasa Keselamatan ICT (JKICT) JKSM. Pentadbir Sistem juga bertanggungjawab melaporkan sebarang insiden pelanggaran polisi berkaitan kepada ICTSO.	Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
Pentadbir Rangkaian dan Keselamatan	
Peranan dan tanggungjawab Pentadbir Rangkaian dan Keselamatan adalah seperti berikut: 1. Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di JKSM beroperasi sepanjang masa. 2. Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna. 3. Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada. 4. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil. 5. Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian. 6. 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*. 7. Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian. 8. Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT (*Security Posture Assessment* - SPA) serta penilaian risiko keselamatan maklumat.	Pentadbir Rangkaian dan Keselamatan
Pentadbir Pangkalan Data	
Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut:	Pentadbir Pangkalan Data

Sub-Kawalan	Tanggungjawab
1. Melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data. 2. Memastikan pangkalan data boleh digunakan pada setiap masa. 3. Melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data. 4. Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur. 5. Melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip PKS. 6. Melaksanakan proses pembersihan data (*housekeeping*) di dalam pangkalan data. 7. Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.	
Pentadbir Portal/Laman Web Rasmi	
Peranan dan tanggungjawab Pentadbir Portal/Laman Web Rasmi adalah seperti berikut: 1. Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah. 2. Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar. 3. Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan	Pentadbir Portal/Laman Web Rasmi

Sub-Kawalan	Tanggungjawab
menggodam, menceroboh dan mengubahsuai muka laman. 4. Mengehadkan capaian Pentadbir Portal/Laman Web server. 5. Mengasingkan kandungan dan aplikasi atas talian untuk capaian secara Intranet dan Internet ke portal JKSM. 6. Memastikan data-data SULIT tidak boleh disalin atau dicetak oleh orang yang tidak berhak. 7. Memastikan reka bentuk laman web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi. 8. Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di pelayan web. 9. Melaksanakan proses *backup* dan *restore* secara berkala.	
Pentadbir Pusat Data	
Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut: 1. Memastikan persekitaran fizikal dan keselamatan Pusat Data berada dalam keadaan baik dan selamat. 2. Memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data. 3. Menjadualkan dan melaksanakan proses salinan (*backup and restore*) ke atas pangkalan data secara berkala.	Pentadbir Pusat Data

Sub-Kawalan	Tanggungjawab
4. Menyediakan perancangan pemulihan bencana mengikut prinsip Pengurusan Kesinambungan Perkhidmatan (PKP) dalam PKS JKSM. 5. Melaksanakan prinsip-prinsip PKS. 6. Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan.	
Pentadbir Sistem Aplikasi	
Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut: 1. Mengkaji cadangan pembangunan/ penyelarasan sistem/ modul di JKSM. 2. Membuat kajian semula serta memperbaiki sistem/ modul sedia ada di JKSM. 3. Membuat pertimbangan dan mengusulkan cadangan pelaksanaan sistem/ modul di JKSM. 4. Membuat pemantauan dan penyelenggaraan terhadap sistem /modul dari semasa ke semasa. 5. Bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem/ modul. 6. Menyediakan dokumentasi sistem/ modul dan manual pengguna. 7. Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas. 8. Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya. 9. Memastikan virus *pattern*, *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemas kini	Pentadbir Sistem Aplikasi

Sub-Kawalan	Tanggungjawab
supaya terhindar daripada ancaman virus dan penggodam. 10. Mematuhi dan melaksanakan prinsip-prinsip PKS dalam mewujudkan akaun pengguna ke atas setiap sistem aplikasi. 11. Melaksanakan sandaran (*backup*) sistem aplikasi pangkalan data yang berkaitan dengannya dibuat secara berjadual. 12. Mengehadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan daripada penyalahgunaannya.	
Pentadbir E-mel	
Peranan dan tanggungjawab Pentadbir E-mel adalah seperti berikut: 1. 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. 2. Membekukan akaun pengguna jika perlu bagi pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib. 3. Memastikan akaun e-mel pengguna sentiasa dalam keadaan baik dan berfungsi. 4. Memastikan pengguna e-mel JKSM berkemahiran menggunakan e-mel melalui penyediaan dokumen panduan penggunaan e-mel dan kursus pembudayaan penggunaan e-mel secara berterusan.	Pentadbir E-mel

Sub-Kawalan	Tanggungjawab
Pentadbir Aset ICT	
Pentadbir Aset ICT dilantik oleh Ketua Pengawal JKS. Peranan dan tanggungjawab Pentadbir Aset ICT adalah seperti berikut: 1. Memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan. 2. Memastikan penerimaan aset ICT Kerajaan dilaksanakan oleh pegawai yang dilantik oleh Ketua Jabatan/ Bahagian. 3. Memastikan semua aset ICT Kerajaan yang diterima didaftarkan menggunakan Sistem Pemantauan Pengurusan Aset (SPA) dalam tempoh dua minggu dari tarikh pengesahan penerimaan aset. 4. Memastikan semua aset ICT Kerajaan yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan secara bertulis daripada Ketua Jabatan/ Pegawai Aset/ Pegawai pegawai lain yang diberi kuasa oleh Ketua Jabatan. 5. Memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/ penggantian/ naik-taraf aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira. 6. Memastikan semua aset ICT Kerajaan diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia dan nama JKSM/ Bahagian/ Agensi berkenaan di tempat yang mudah dilihat dan sesuai pada aset berkenaan.	Pentadbir Aset ICT

Sub-Kawalan	Tanggungjawab
7. Memastikan semua aset ICT Kerajaan ditandakan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan. 8. Memastikan senarai daftar induk aset ICT Kerajaan disediakan. 9. Memastikan senarai aset ICT Kerajaan disediakan mengikut lokasi dan format Senarai Aset ICT Kerajaan dalam dua (2) buah salinan. Satu (1) senarai berkenaan perlu disimpan oleh Pegawai Aset ICT/ Pembantu Pegawai Aset ICT dan satu (1) buah salinan perlu dipaparkan oleh pegawai yang bertanggungjawab di lokasi. 10. Memastikan setiap kerosakan aset ICT Kerajaan dilaporkan untuk tujuan penyelenggaraan. 11. Bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT Kerajaan. 12. Merancang, memantau dan memastikan pemeriksaan aset ICT Kerajaan dilaksanakan ke atas keseluruhan aset ICT Kerajaan sekurang-kurangnya sekali setahun. 13. Memastikan setiap kes kehilangan aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur.	
Pentadbir Media Sosial	
Peranan dan tanggungjawab Pentadbir Media Sosial JKSM adalah seperti berikut: 1. Mematuhi segala peraturan atau syarat-syarat yang digariskan oleh penyedia platform media sosial.	Pentadbir Media Sosial

Sub-Kawalan	Tanggungjawab
2. Mentadbir dan menyemak ketepatan serta sensitiviti maklumat dalam pengurusan kandungan (video, audio, gambar dan dokumen) dan komen mengikut etika media sosial semasa. 3. Melaporkan sebarang pelanggaran polisi atau etika penggunaan media sosial yang sedang berkuat kuasa kepada Ketua Unit Komunikasi Korporat JKSM.	
(G) Pengguna Peranan dan tanggungjawab pengguna adalah seperti berikut: 1. Membaca, memahami dan mematuhi Polisi Keselamatan Siber JKSM. 2. Mengetahui dan memahami implikasi keselamatan ICT daripada tindakannya. 3. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat. 4. Melaksanakan prinsip-prinsip PKS JKSM dan menjaga kerahsiaan maklumat JKSM. 5. Melaksanakan langkah-langkah perlindungan seperti berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. (b) Memeriksa maklumat dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa. (c) Menentukan maklumat sedia untuk digunakan.	Pengguna

Sub-Kawalan	Tanggungjawab
(d) Menjaga kerahsiaan kata laluan. (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. 6. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan. 7. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum. 8. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera. 9. Menghadiri program-program kesedaran mengenai keselamatan ICT. 10. Mengawal aktiviti penggunaan media sosial. 11. Menandatangani "Surat Akuan Pematuhan" (LAMPIRAN 1) bagi mematuhi Polisi Keselamatan Siber JKSM.	
(H) Jawatankuasa Pemandu ICT (JPICT) Keanggotaan JKICT JKSM adalah seperti berikut: **<u>Pengerusi</u>** Ketua Pengarah/ Ketua Hakim Syarie **<u>Ahli:</u>** 1. Ketua Pendaftar 2. Pengarah Kanan (Kehakiman) 3. Pengarah Kanan (Pengurusan)	Ketua Pengarah/ Ketua Hakim Syarie

Sub-Kawalan	Tanggungjawab
4. Pengarah-pengarah Bahagian 5. Ketua Penolong Pengarah BTMK **<u>Urus Setia:</u>** BTMK, JKSM **<u>Bidang Kuasa:</u>** 1. Menetapkan arah tuju dan strategi ICT untuk pelaksanaan ICT JKSM. 2. Merancang, menyelaras dan memantau pelaksanaan program atau projek ICT JKSM. 3. Menyelaras dan menyeragamkan pelaksanaan ICT agar selari dengan Pelan Strategik Pendigitalan (PSP) JKSM PSP Sektor Awam; 4. Meluluskan projek-projek ICT. 5. Mengikuti dan memantau perkembangan program ICT serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT. 6. Merancang dan menentukan langkah-langkah keselamatan ICT. 7. Mengemukakan perolehan ICT yang telah diluluskan di peringkat JPICT JKSM kepada Jawatankuasa Teknikal ICT Sektor Awam (JTISA) MAMPU untuk kelulusan. 8. Mengemukakan laporan kemajuan projek ICT yang diluluskan kepada JTISA MAMPU. 9. Menetapkan dasar dan prosedur pengurusan portal JKSM. 10. Meluluskan dokumen PKS JKSM.	

Sub-Kawalan	Tanggungjawab
(I) Jawatankuasa Keselamatan ICT (JKICT) Keanggotaan JKICT JKSM adalah seperti berikut: **<u>Pengerusi</u>** CDO **<u>Ahli:</u>** 1. ICTSO 2. Pengarah Kanan (Kehakiman) 3. Pengarah Kanan (Pengurusan) 4. Pengarah-pengarah Bahagian 5. Pegawai Teknologi Maklumat **<u>Urus Setia:</u>** BTMK, JKSM **<u>Bidang Kuasa:</u>** 1. Menyelenggara dokumen PKS JKSM. 2. Memantau tahap pematuhan PKS JKSM. 3. Menilai aspek teknikal keselamatan projek-projek ICT. 4. Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam jabatan yang mematuhi keperluan PKS JKSM. 5. Menyemak semula sistem ICT supaya sentiasa mematuhi keperluan keselamatan dari semasa ke semasa.	CDO

Sub-Kawalan	Tanggungjawab
6. Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT. 7. Memastikan PKS JKSM selaras dengan dasar-dasar ICT Kerajaan semasa. 8. Bekerjasama dengan JKSMCERT untuk mendapatkan maklum balas dan insiden untuk tindakan pengemaskinian PKS JKSM. 9. Membincang tindakan yang melibatkan pelanggaran PKS JKSM.	
(J) Pasukan Tindak Balas Insiden Keselamatan ICT (JKSMCERT) Keanggotaan JKSMCERT adalah seperti berikut: **<u>Pengerusi</u>** ICTSO **<u>Ahli:</u>** 1. Pegawai Teknologi Maklumat 2. Penolong Pegawai Teknologi Maklumat 3. Juruteknik ICT **<u>Urus Setia:</u>** BTMK, JKSM **<u>Bidang Kuasa:</u>** 1. Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden. 2. Merekodkan dan menjalankan siasatan awal insiden yang diterima.	ICTSO

Sub-Kawalan	Tanggungjawab
3. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum. 4. Menghubungi dan melaporkan insiden yang berlaku kepada ICTSO dan NACSA sama ada sebagai input atau untuk tindakan seterusnya. 5. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baharu dapat dielakkan. 6. Mengguna pakai *Standard Operating Procedure* (SOP) bagi pengurusan pengendalian insiden keselamatan. 7. Melaporkan sebarang maklum balas dan insiden keselamatan ICT kepada ICTSO. 8. Merujuk insiden keselamatan siber yang melibatkan Maklumat Rahsia Rasmi kepada pihak CGSO.	
020102 Pengasingan Tugas	
Tugas dan tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT. 2. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT	Pengarah Bahagian

Sub-Kawalan	Tanggungjawab
daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. 3. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. 4. Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.	
020103 Hubungan Dengan Pihak Berkuasa	
Hubungan baik dengan pihak berkuasa hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab JKSM. 2. Mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis DiRaja Malaysia (PDRM) dan Suruhanjaya Komunikasi dan Multimedia (SKMM). 3. Insiden keselamatan maklumat harus dilaporkan dengan segera bagi mengurangkan impak insiden.	CDO, BKPSM, Pasukan ERT

Sub-Kawalan	Tanggungjawab
020104 Hubungan Dengan Pihak Berkepentingan	
Hubungan baik dengan pihak berkepentingan atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan.	Warga JKSM
020105 Keselamatan Maklumat Dalam Pengurusan Projek	
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek JKSM. 2. Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek. 3. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan semasa awal projek untuk mengenal pasti kawalan yang diperlukan. 4. Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti mana yang terkandung di dalam PKS JKSM. 5. Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai persijilan keselamatan maklumat.	Pengurus Projek
0202 Peranti Mudah Alih dan *Teleworking*	
Memastikan keselamatan *teleworking* dan penggunaan peranti mudah alih.	

Sub-Kawalan	Tanggungjawab
020201 Polisi Peranti Mudah Alih	
Pembangunan dasar, arahan, peraturan dan langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada warga JKSM. Bahagian Teknologi Maklumat dan Komunikasi berperanan membangun serta menyebarkan dasar dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih. Jawatankuasa Keselamatan ICT JKSM berperanan meluluskan dasar, arahan, peraturan dan langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada warga JKSM. Perkara-perkara yang perlu dipatuhi oleh Warga JKSM adalah seperti berikut: 1. Pendaftaran ke atas peralatan mudah alih. 2. Keperluan perlindungan secara fizikal. 3. Kawalan ke atas pemasangan perisian peralatan mudah alih. 4. Kawalan ke atas versi dan *patches* perisian. 5. Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi. 6. Keperluan penyimpanan peralatan mudah alih di tempat yang selamat.	JKICT, Pengguna
020202 *Teleworking*	
Dasar dan langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi *teleworking*.	JKICT dan Warga JKSM

[Halaman ini sengaja dibiarkan kosong]

0301 Sebelum Perkhidmatan

0302 Dalam Perkhidmatan

0303 Bertukar atau Tamat Perkhidmatan

KAWALAN

03

KESELAMATAN SUMBER MANUSIA

KAWALAN 03

KESELAMATAN SUMBER MANUSIA

Sub-Kawalan	Tanggungjawab
0301 Sebelum Perkhidmatan	
Memastikan semua pengguna yang terdiri daripada warga JKSM, pembekal, pakar runding dan pihak yang mempunyai urusan perkhidmatan ICT JKSM memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.	
030101 Tapisan Keselamatan	
Menjalankan tapisan keselamatan terhadap kakitangan JKSM, pembekal dan pihak-pihak lain yang terlibat selaras dengan keperluan perkhidmatan.	Ketua Pengarah/ Ketua Hakim Syarie
030102 Terma dan Syarat	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: 1. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga JKSM, pembekal, dan pihak-pihak lain yang terlibat dalam menjamin keselamatan aset ICT. 2. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Ketua Pengarah/ Ketua Hakim Syarie
0302 Dalam Perkhidmatan	
Memastikan semua pengguna yang terdiri daripada warga JKSM, pembekal, pakar runding dan pihak yang mempunyai urusan perkhidmatan ICT JKSM memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan	

Sub-Kawalan	Tanggungjawab
aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.	
030201 Tanggungjawab Pengurusan	
1. Memastikan warga JKSM, pengguna dan pembekal mematuhi PKS JKSM. 2. Memastikan warga JKSM, pengguna dan pembekal mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh JKSM.	CDO
030202 Latihan, Pendidikan dan Kesedaran Keselamatan Maklumat	
Warga JKSM dan pihak pembekal perlu diberikan taklimat kesedaran mengenai keselamatan ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka.	ICTSO
030203 Tindakan Tatatertib	
1. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga JKSM sekiranya berlaku pelanggaran dengan perundangan dan peraturan yang ditetapkan oleh JKSM. 2. Pengguna yang melanggar PKS JKSM akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT JKSM.	Ketua Pengarah/ Ketua Hakim Syarie dan CDO

Sub-Kawalan	Tanggungjawab
0303 Bertukar atau Tamat Perkhidmatan	
Memastikan pertukaran, tamat perkhidmatan atau pertukaran bidang tugas warga JKSM diuruskan dengan teratur.	
030301 Penamatan atau Pertukaran Tanggungjawab Perkhidmatan	
Warga JKSM yang telah tamat perkhidmatan hendaklah mematuhi perkara berikut: 1. Memastikan semua aset ICT dikembalikan kepada JKSM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan. 2. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan JKSM dan terma perkhidmatan yang ditetapkan.	Pentadbir Sistem, Pentadbir Aset ICT dan Warga JKSM

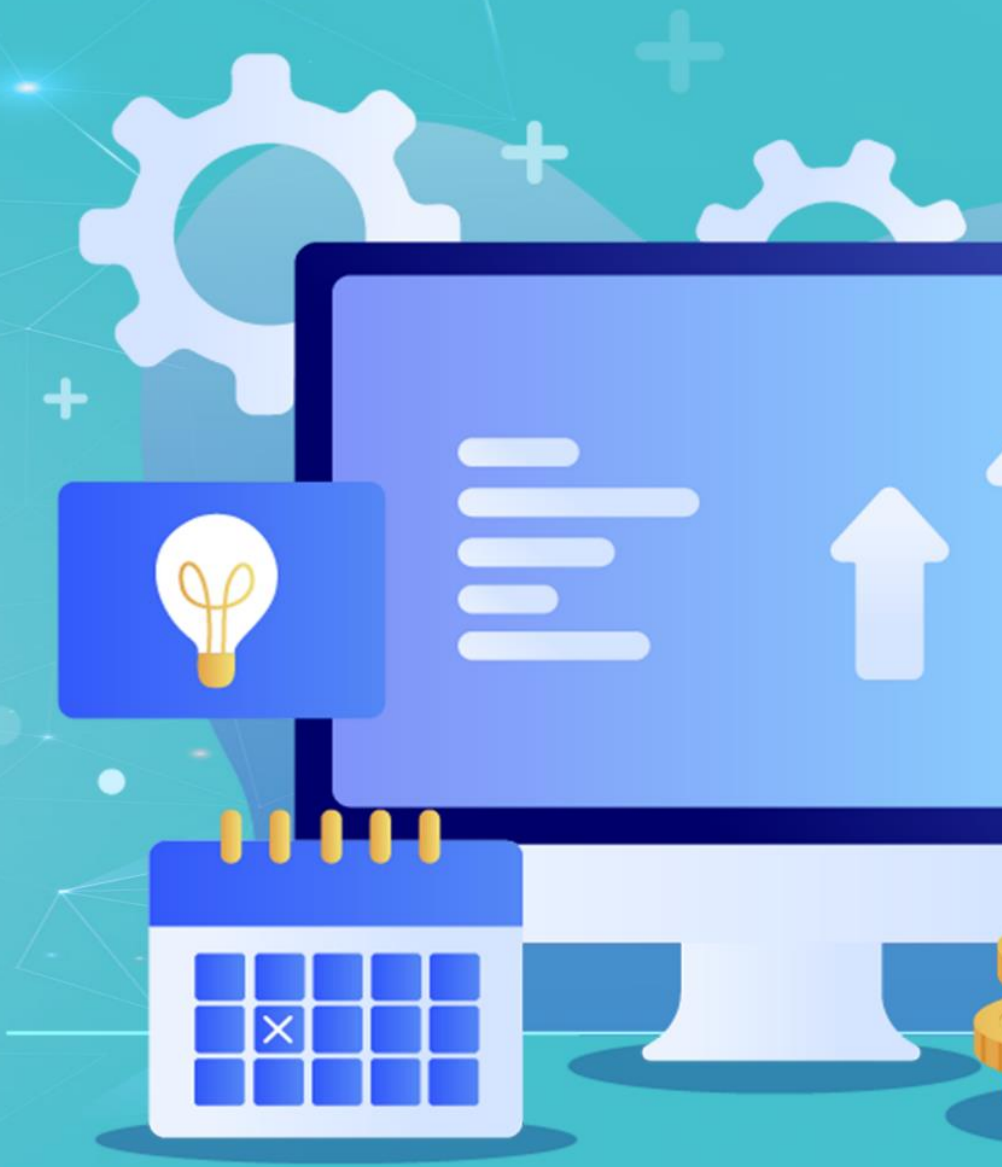
[Halaman ini sengaja dibiarkan kosong]

0401 Tanggungjawab Terhadap Aset

0402 Klasifikasi Maklumat

0403 Pengurusan Ketirisan Maklumat Elektronik

0404 Pengendalian Media



KAWALAN

04

PENGURUSAN ASET

KAWALAN 04
PENGURUSAN ASET

Sub-Kawalan	Tanggungjawab
0401 Tanggungjawab Terhadap Aset	
Mengenal pasti aset Jabatan bagi memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT JKSM.	
040101 Inventori Aset	
Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT JKSM. Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi: 1. Mengenal pasti Pegawai Penerima Aset setiap Bahagian untuk menguruskan penerimaan aset ICT bagi projek ICT. 2. Memastikan semua aset ICT dikenal pasti, dikelaskan, didokumenkan, diselenggarakan dan dilupuskan. Maklumat aset direkodkan dan dikemas kini dalam Sistem Pengurusan Aset (SPA), Kad Daftar Harta Modal dan Aset Alih Bernilai Rendah sebagaimana mengikut Pekeliling Perbendaharaan AM 2 Tahun 2018:Tatacara Pengurusan Aset Alih Kerajaan atau senarai aset yang berkaitan. 3. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja. 4. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di JKSM. 5. Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.	Pegawai Aset, Pegawai Penerima aset, Warga JKSM

Sub-Kawalan	Tanggungjawab
040102 Pemilikan Aset	
Aset yang diselenggarakan hendaklah milik JKSM. Tanggungjawab yang perlu dipatuhi termasuk perkara-perkara berikut: 1. Memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset. 2. Memastikan aset telah dikelaskan dan dilindungi. 3. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja. 4. Pegawai Aset hendaklah mengesahkan penempatan aset ICT.	Pegawai Aset dan Warga JKSM
040103 Penggunaan Aset Yang Dibenarkan	
Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.	Warga JKSM
040104 Pemulangan Aset	
Warga JKSM hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar Jabatan dan penamatan perkhidmatan atau kontrak.	Warga JKSM
0402 Klasifikasi Maklumat	
Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
040201 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan	Pegawai Pengelas

Sub-Kawalan	Tanggungjawab
sebagai mana yang ditetapkan di dalam Arahan Keselamatan. Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap Pegawai Pengelas kritikal kepada JKSM. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan dan dilabel sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: 1. Rahsia Rasmi a. Rahsia Besar b. Rahsia c. Sulit d. Terhad 2. Rasmi 3. Data Terbuka	
040202 Pelabelan Maklumat	
Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.	Warga JKSM
040203 Pengendalian Maklumat	
Prosedur mengendalikan aset hendaklah dibangunkan dan dilaksanakan mengikut skim klasifikasi maklumat yang diguna pakai oleh JKSM. Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai,	Pegawai Aset Warga JKSM

Sub-Kawalan	Tanggungjawab
menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut: 1. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. 2. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa. 3. Menentukan maklumat sedia untuk digunakan. 4. Menjaga kerahsiaan kata laluan. 5. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. 6. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan. 7. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.	
040204 Pengendalian Data Terbuka	
Data Terbuka ialah data yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi Kerajaan dan organisasi swasta untuk pelbagai tujuan. Jabatan akan menyediakan set data terbuka berdasarkan bidang atau sektor atau kluster. Kategori set data ini tidak terhad dan boleh berubah mengikut fungsi teras dan keperluan semasa Jabatan. Data terbuka yang telah diperakukan oleh Jabatan akan dikemukakan kepada JKSM untuk kelulusan dan seterusnya diterbitkan ke Portal Data Terbuka Sektor Awam (DTSA) di bawah pengurusan MAMPU.	Pemilik Data

Sub-Kawalan	Tanggungjawab
0403 Pengurusan Ketirisan Maklumat Elektronik	
Melindungi keselamatan maklumat elektronik daripada kebocoran dan disalah guna oleh pihak yang tidak dibenarkan.	
040301 Pengurusan Ketirisan Maklumat Elektronik	
Ketirisan maklumat terperingkat ialah 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 meja dan komputer riba bagi membolehkan kawalan ke atas perkongsian atau penyebaran maklumat rasmi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Gambar dokumen maklumat Rahsia Rasmi/ Rasmi TIDAK BOLEH diambil menggunakan telefon bimbit atau pelbagai peranti elektronik milik peribadi. 2. Akaun e-mel peribadi TIDAK BOLEH digunakan dalam urusan rasmi Kerajaan. 3. Maklumat rasmi TIDAK BOLEH dimuat naik dalam media sosial dan storan awan awam (seperti *dropbox*). 4. Maklumat log masuk dan kata laluan komputer/sistem ICT TIDAK BOLEH ditulis dan ditampal di skrin komputer atau mana-mana ruang kerja. 5. Penghantaran e-mel maklumat terperingkat haruslah menggunakan kaedah penyulitan (*encryption*).	CDO dan ICTSO

Sub-Kawalan	Tanggungjawab
0404 Pengendalian Media	
Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
040401 Pengurusan Media Boleh Alih (*Removal Media*)	
Prosedur pengurusan media mudah alih hendaklah dibangunkan dan dilaksanakan mengikut skim pengelasan yang diguna pakai oleh JKSM. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: 1. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat. 2. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja. 3. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja. 4. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan. 5. Menyimpan semua media di tempat yang selamat.	ICTSO Pentadbir Sistem, Pengguna
040402 Pelupusan Media	
1. Pelupusan media perlu mendapat kelulusan daripada pihak pengurusan ICT dan mengikut prosedur pelupusan aset ICT yang ditetapkan oleh Kerajaan. 2. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang	ICTSO

Sub-Kawalan	Tanggungjawab
betul serta selamat dan dengan kebenaran JKSM/JKSN/MSN. 3. Pelupusan media storan perlu dirujuk kepada CGSO dan Jabatan Arkib Negara bagi menentukan sama ada ia mengandungi maklumat terperingkat dan/atau mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara. 4. Pelupusan maklumat/data boleh dilaksanakan dalam bentuk pemusnahan fizikal dan/atau sanitasi data. Sanitasi data hendaklah mengikut garis panduan yang dikeluarkan oleh Kerajaan.	
040403 Pemindahan Media Fizikal	
JKSM hendaklah memastikan media yang mengandungi maklumat dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan.	Pengguna

[Halaman ini sengaja dibiarkan kosong]

0501 Keperluan Kawalan Capaian

0502 Pengurusan Capaian Pengguna

0503 Tanggungjawab Pengguna

0504 Kawalan Capaian Sistem dan Aplikasi

KAWALAN

05

KAWALAN CAPAIAN

KAWALAN 05
KAWALAN CAPAIAN

Sub-Kawalan	Tanggungjawab
0501 Keperluan Kawalan Capaian	
Mengehadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.	
050101 Polisi Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong kawalan capaian pengguna sedia ada. 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: 1. Keperluan keselamatan aplikasi JKSM. 2. Kebenaran untuk menyebarkan maklumat. 3. Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian. 4. Undang-undang Malaysia/ Persekutuan yang berkaitan dan obligasi kontrak mengenai had akses kepada data atau perkhidmatan. 5. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran. 6. Pengasingan peranan kawalan capaian.	Pentadbir Sistem Pengguna

Sub-Kawalan	Tanggungjawab
7. Kebenaran rasmi permohonan akses. 8. Keperluan semakan hak akses berkala. 9. Pembatalan hak akses. 10. Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat. 11. Akses *privilege*.	
050102 Capaian Kepada Rangkaian dan Perkhidmatan Rangkaian	
Pengguna hanya boleh mendapat capaian kepada rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran daripada JKSM. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: 1. Menempatkan atau memasang perkakasan ICT yang bersesuaian antara rangkaian JKSM, rangkaian agensi lain dan rangkaian awam. 2. Mewujud dan menguatkuasakan mekanisme kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT. 3. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO, Pentadbir Rangkaian
050103 Capaian Jarak Jauh	
JKSM hendaklah menyediakan kemudahan capaian ke dalam rangkaian dalaman JKSM dari rangkaian luar JKSM. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Kemudahan ini mestilah menggunakan kaedah pengesahan ID pengguna dan kata laluan atau	ICTSO, Pentadbir Sistem, Pengguna

Sub-Kawalan	Tanggungjawab
kaedah lain yang selamat dan dipercayai (*secure and trusted*). 2. Capaian jarak jauh dari luar rangkaian JKSM hendaklah menggunakan mekanisme perhubungan rangkaian Internet yang disediakan oleh JKSM. 3. Penggunaan perkhidmatan capaian jarak jauh selain daripada yang disediakan oleh JKSM hendaklah mendapat kebenaran CDO atau ICTSO JKSM. 4. Penggunaan perkhidmatan ini hendaklah dimohon dan mendapat kebenaran bertulis daripada CDO atau ICTSO JKSM. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	
0502 Pengurusan Capaian Pengguna	
Memastikan capaian pengguna yang dibenarkan sahaja dan menghalang capaian yang tidak dibenarkan kepada sistem dan perkhidmatan.	
050201 Pendaftaran dan Pembatalan Pengguna	
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. Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan capaian dan pembatalan hak capaian. Perkara-perkara berikut hendaklah dipatuhi: 1. Akaun yang diperuntukkan oleh JKSM sahaja boleh digunakan.	Pentadbir Sistem, Pengguna

Sub-Kawalan	Tanggungjawab
2. Akaun pengguna mestilah unik. 3. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada JKSM terlebih dahulu. 4. Penggunaan ID milik orang lain atau berkongsi ID adalah dilarang. 5. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan JKSM.	
050202 Penyediaan Akses Pengguna	
Satu proses penyediaan akses pengguna untuk kebenaran dan pembatalan capaian pengguna ke atas semua aplikasi dan perkhidmatan ICT.	Pentadbir Sistem
050203 Pengurusan Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem
050204 Pengurusan Maklumat Pengesahan Rahsia Pengguna	
Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.	Pentadbir Sistem
050205 Kajian Semula Hak Capaian Pengguna	
Pemilik aset hendaklah menyemak hak capaian pengguna pada sela masa yang ditetapkan. Pentadbir Sistem perlu mewujudkan Pendaftaran dan Penamatan Pengguna Sistem masing-masing sebagai rujukan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan.	ICTSO, Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
050206 Pembatalan atau Pelarasan Hak Capaian	
Hak capaian kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan perkhidmatan, kontrak atau perjanjian, atau diselaraskan apabila berlaku perubahan dalam JKSM. Pengurusan capaian ini hendaklah dilaksanakan sekurang-kurangnya sebulan sekali atau setiap kali adanya perubahan maklumat.	Pentadbir Sistem
0503 Tanggungjawab Pengguna	
Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.	
050301 Penggunaan Maklumat Pengesahan Rahsia	
Peranan dan tanggungjawab pengguna dalam melindungi maklumat pengesahan adalah seperti berikut: 1. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. 2. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa. 3. Menentukan maklumat sedia digunakan. 4. Menjaga kerahsiaan kata laluan. 5. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. 6. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, Pertukaran dan pemusnahan.	Pengguna

Sub-Kawalan	Tanggungjawab
7. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.	
0504 Kawalan Capaian Sistem dan Aplikasi	
Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas maklumat yang terdapat dalam sistem dan aplikasi.	
050401 Had Kawalan Capaian Maklumat	
Capaian kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.	ICTSO, Pentadbir Sistem
050402 Prosedur Log Masuk Yang Selamat	
Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk (*log-on*) yang bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kaedah-kaedah yang digunakan adalah seperti berikut: 1. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Jabatan. 2. Menjana amaran (*alert*) sekiranya berlaku pelanggaran semasa proses *log-on* terhadap aplikasi sistem. 3. Mengawal capaian ke atas aplikasi sistem menggunakan prosedur *log-on* yang terjamin. 4. Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna. 5. Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti.	ICTSO, Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
6. Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	
050403 Pengurusan Kata Laluan	
Pengguna perlu mengikut amalan keselamatan yang baik dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti. Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh JKSM seperti berikut: 1. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun. 2. Pengguna hendaklah menukar kata laluan dengan segera apabila disyaki berlakunya kebocoran kata laluan atau dikompromi. 3. Panjang kata laluan mestilah sekurang kurangnya 12 aksara dengan gabungan antara huruf, aksara khas dan nombor (alfa numerik) **kecuali** bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad. 4. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun. 5. Kata laluan hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama. 6. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara. 7. Kuat kuasakan pertukaran kata laluan semasa log masuk kali pertama atau selepas log masuk kali pertama atau selepas kata laluan diset semula.	ICTSO, Pentadbir Sistem, Pengguna

Sub-Kawalan	Tanggungjawab
8. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna. 9. Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum tiga sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga ID capaian diaktifkan semula. 10. Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	
050404 Penggunaan Utiliti Sistem	
Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *overriding* sistem.	Pentadbir Sistem
050405 Kawalan Akses Kepada Kod Sumber Program	
Pembangunan sistem secara sumber luaran perlu diselia dan dipantau oleh JKSM: 1. Log audit perlu dikekalkan kepada semua akses kepada kod sumber. 2. Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan. 3. Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik JKSM.	Pentadbir Sistem
050406 Token/ Sijil Digital	
Pembangunan sistem secara sumber luaran perlu diselia dan dipantau oleh JKSM: 1. Penggunaan token Kerajaan Elektronik (Token EG) atau sijil digital hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan.	Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
2. Perkongsian penggunaan token adalah tidak dibenarkan sama sekali. 3. Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pihak yang mengeluarkan token.	
0505 *Bring Your Own Device* (BYOD)	
Melindungi keselamatan maklumat melalui penggunaan peralatan persendirian seperti telefon pintar, tablet, komputer riba dan seumpamanya.	
050101 Pengurusan BYOD	
Garis panduan yang menjelaskan polisi dan peraturan berkaitan adalah seperti dalam Tatacara Keselamatan ICT JKSN/JKSN/MSN – *Bring Your Own Device* (BYOD). Borang Pendaftaran Bring Your Own Device (BYOD) seperti di **LAMPIRAN B**.	ICTSO, Pentadbir Sistem

[Halaman ini sengaja dibiarkan kosong]

0601 Kawalan Kriptografi

KAWALAN

06

KRIPTOGRAFI

KAWALAN 06
KRIPTOGRAFI

Sub-Kawalan	Tanggungjawab
0601 Kawalan Kriptografi	
Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, integriti dan kesahihan maklumat.	
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: 1. Enkripsi Sistem Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (*encryption*). 2. Tandatangan Digital Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan.	Pengarah Projek
060102 Pengurusan Kunci Awam (*Public Key*)	
Pengurusan ke atas Infrastruktur Kunci Awam (*Public Key Infrastructure* – PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan	Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
dari diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.	

0701 Keselamatan Kawasan

0702 Keselamatan Peralatan ICT

KAWALAN

07

KESELAMATAN FIZIKAL DAN PERSEKITARAN

KAWALAN 07
KESELAMATAN FIZIKAL DAN PERSEKITARAN

Sub-Kawalan	Tanggungjawab
0701 Keselamatan Kawasan	
Menghalang akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat JKSM.	
070101 Keselamatan Fizikal	
Jabatan hendaklah mengenal pasti Kawasan Terperingkat. Peranti milik persendirian DILARANG penggunaannya di Kawasan Terperingkat. Ini bertujuan menghalang capaian, kerosakan dan gangguan secara perolehan fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk: 1. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat. 2. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini. 3. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan. 4. Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana disebabkan oleh kuasa Tuhan atau perbuatan manusia.	CDO, BKPSM

5. Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad. 6. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya. 7. 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: 1. 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. 2. 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 merupakan satu kesalahan dan boleh diambil tindakan. 3. Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT JKSM. 4. Kehilangan Pas Keselamatan Pelawat hendaklah dilaporkan segera kepada JKSM.	Pengguna

070103 Kawalan Pejabat, Bilik dan Kemudahan	
Perkara yang perlu dipatuhi adalah seperti berikut: 1. Kawasan tempat bekerja, bilik dan tempat operasi ICT perlu dihadkan daripada akses oleh pihak luar. 2. Penunjuk arah ke lokasi bilik operasi dan tempat larangan tidak harus menonjol dan hanya memberi petunjuk minimum.	Pengguna
070104 Perlindungan Terhadap Ancaman Luaran dan Persekitaran	
Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. JKSM perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	BKPSM, Pentadbir Pusat Data
070105 Bekerja di Kawasan Selamat	
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: 1. 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. 2. Akses adalah terhad kepada warga JKSM yang telah diberi kuasa sahaja dan dipantau pada setiap masa.	BKPSM , Pentadbir Pusat Data

3. Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) atau lain-lain peralatan yang sesuai. 4. Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual. 5. Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan. 6. Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab sepanjang tempoh di lokasi berkaitan. 7. Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam. 8. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan. 9. Memperkukuhkan dinding dan siling. 10. Mengehadkan jalan keluar masuk.	
070106 Kawasan Penghantaran dan Pemunggahan	
Titik kemasukan (*access point*) seperti kawasan penghantaran dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan. JKSM hendaklah memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki pihak yang tidak diberi kebenaran.	Warga JKSM, Pembekal
0702 Keselamatan Peralatan ICT	
Melindungi peralatan ICT JKSM daripada kehilangan, kerosakan, kecurian dan disalahgunakan.	

070201 Penempatan dan Perlindungan Peralatan ICT	
Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran serta peluang kemasukan yang tidak dibenarkan. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: 1. Penggunaan kata laluan untuk akses pada sistem komputer diwajibkan. 2. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan. 3. Pengguna dilarang sama sekali menambah, menanggalkan atau mengganti sebarang perkakasan ICT yang telah ditetapkan. 4. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem. 5. Hanya perisian rasmi yang dibenarkan bagi kegunaan Jabatan. Dilarang pemasangan perisian tidak sah tanpa kebenaran ICTSO. 6. Pengguna mesti memastikan perisian antivirus di komputer masing-masing sentiasa aktif dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan. 7. Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna. 8. Setiap pengguna adalah bertanggungjawab ke atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya.	Pengguna

9. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Gen-Set). 10. Semua alat sokongan perlu disemak dan dikemaskinikan dari semasa ke semasa (sekurang-kurangnya setahun sekali). 11. 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. 12. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai aliran pengudaraan (*air ventilation*) yang sesuai. 13. Peralatan ICT yang hendak dibawa ke luar dari premis JKSM, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan. 14. Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikuti prosedur pelaporan insiden. 15. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa. 16. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ianya ditempatkan tanpa kebenaran Pentadbir Sistem; 17. Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem untuk dibaik pulih. 18. 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. 19. Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal. 20. Pengguna dilarang sama sekali mengubah kata laluan *administrator* yang telah ditetapkan oleh Pentadbir Sistem. 21. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan digunakan sepenuhnya bagi urusan rasmi Jabatan sahaja. 22. 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 Utiliti Sokongan	
Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu diselenggarakan dari semasa ke semasa **sekurang-kurangnya setahun sekali**.	BKPSM
070203 Keselamatan Kabel	
Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: 1. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan.	Pentadbir Sistem

2. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan. 3. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*. 4. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	
070204 Penyelenggaraan Peralatan	
Peralatan ICT hendaklah diselenggarakan dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan dan juga memastikan keboleh sediaan, kerahsiaan dan integriti (CIA). Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: 1. Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan. 2. Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggarakan. 3. Memastikan perkakasan hanya diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja. 4. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan. 5. Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	ICTSO, Pentadbir Sistem dan Pentadbir Aset ICT

070205 Pengalihan Aset	
Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: 1. Peralatan ICT yang hendak dibawa keluar dari premis JKSM untuk tujuan rasmi perlulah mendapat kelulusan CDO atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan. 2. Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	Pentadbir Aset ICT dan Pengguna
070206 Keselamatan Peralatan dan Aset di Luar Premis	
Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis JKSM. Peralatan yang dibawa keluar dari premis JKSM adalah terdedah kepada pelbagai risiko. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: 1. Peralatan perlu dilindungi dan dikawal sepanjang masa. 2. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian. 3. Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	Warga JKSM
070207 Pelupusan atau Penggunaan Semula Peralatan	
Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data sensitif dan perisian	Pegawai Aset, Pentadbir Sistem dan Warga JKSM

berlesen dikeluarkan atau ditulis ganti (*overwrite*) sebelum dilupuskan atau diguna semula.

Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh JKSM dan ditempatkan di JKSM.

Peralatan yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan JKSM.

Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:

1. Bagi peralatan yang akan dilupuskan sebelum dipindah milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara selamat.

2. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya.

3. Peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut.

4. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa.

5. Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:

    a. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk dijadikan milik peribadi.

    b. Mencabut, menanggalkan dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya.

c. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ek mana-mana bahagian JKSM.

d. Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan.

e. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab JKSM.

6. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *thumbdrive* atau *external hardisk* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.

7. Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal. Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan.

8. Maklumat lanjut berhubung pelupusan boleh dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa.

9. Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara.

10. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem SPPA.

070208 Peralatan Tanpa Penyeliaan	
Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara-perkara berikut: 1. Tamatkan sesi aktif apabila selesai tugas. 2. *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai. 3. Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.	Warga JKSM
070209 *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 dan mendedahkan bahan-bahan yang sensitif sama ada di atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: 1. Menggunakan kemudahan *password screensaver* atau log-off apabila meninggalkan komputer. 2. Menyimpan bahan-bahan sensitif terutama dokumen terperingkat di dalam laci atau kabinet fail yang berkunci. 3. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat yang digunakan secara bersama. 4. E-mel masuk dan keluar hendaklah dikawal.	Warga JKSM

5. Menghalang penggunaan tanpa kebenaran mesin fotostat dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	
070210 Kawalan Peralatan Sewaan/Pinjaman/Uji Cuba (*Proof of Concepts* – POC)	
Peralatan ICT secara sewaan/pinjaman/POC adalah berdasarkan kepada persetujuan secara bertulis sama ada melalui kontrak perjanjian atau dokumen rasmi yang menyatakan tujuan. Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: 1. Penerimaan Peralatan 2. Penyelenggaraan Peralatan 3. Pemulangan Peralatan	ICTSO dan Pengarah Projek

[Halaman ini sengaja dibiarkan kosong]

0801 Prosedur dan Tanggungjawab Operasi

0802 Perlindungan daripada Perisian Hasad (Malware)

0803 Sandaran (Backup)

0804 Log dan Pemantauan

0805 Kawalan Perisian Operasi

0806 Pengurusan Kerentanan Teknikal

0807 Pertimbangan Audit Sistem Maklumat

KAWALAN

08

KAWALAN OPERASI

KAWALAN 08
KESELAMATAN OPERASI

Sub-Kawalan	Tanggungjawab
0801 Prosedur dan Tanggungjawab Operasi	
Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan ke atas kemudahan pemprosesan maklumat.	
080101 Dokumen Prosedur Operasi	
Penyedia dokumen perlu memastikan prosedur operasi dan tanggungjawab didokumenkan untuk mereka yang memerlukan. Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: 1. Semua prosedur keselamatan ICT yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; 2. 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. 3. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pengarah Bahagian dan Pentadbir Sistem
080102 Pengurusan Perubahan	
Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan ang didokumenkan mematuhi perkara-perkara berikut:	CDO dan Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
1. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu. 2. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini 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. 3. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. 4. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.	
08103 Pengurusan Kapasiti	
Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. 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. 2. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko	Pengurus ICT dan Pentabir Sistem

Sub-Kawalan	Tanggungjawab
seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	
08104 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi	
Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan daripada perkakasan yang digunakan sebagai pengeluaran (*production*). 2. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian 3. Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.	Pentadbir Sistem
0802 Perlindungan Daripada Perisian Hasad (*Malware*)	
Memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.	
080201 Kawalan ke atas Perisian Hasad (*Malware*)	
Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada serangan *malware* hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut.	Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut: 4. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat. 5. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa. 6. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya. 7. Mengemas kini antivirus dengan *pattern* antivirus yang terkini. 8. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat. 9. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya. 10. 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. 11. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.	

Sub-Kawalan	Tanggungjawab
0803 Sandaran (*Backup*)	
Memastikan segala data diselenggarakan agar penyimpanan data diuruskan dengan sempurna.	
080301 Sandaran Maklumat (*Information Backup*)	
Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di *off-site*. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaharu. 2. Membuat sandaran ke atas semua data dan maklumat dan maklumat mengikut keperluan operasi. 3. Menguji sistem sandaran sedia ada bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana. 4. Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan. Kekerapan sandaran bergantung pada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya **TIGA GENERASI**.	Pentadbir Sistem
0804 Log dan Pemantauan	
Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	

Sub-Kawalan	Tanggungjawab
080401 *Event Logging*	
Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan. Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis faillog bagi server dan aplikasi yang perlu diaktifkan adalah seperti yang berikut: 1. Fail log sistem pengoperasian. 2. Fail log servis. 3. Fail log aplikasi. 4. Fail log rangkaian. Pentadbir Sistem hendaklah melaksanakan perkara berikut: 1. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna. 2. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera. 3. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan,	Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
Pentadbir Sistem Aplikasi hendaklah melaporkan kepada ICTSO dan CDO.	
080402 Perlindungan Log	
Kemudahan merekodkan dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan.	Pentadbir Sistem
080403 Log Pentadbir dan Pengendali	
Aktiviti Pentadbir Sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap. 1. Memantau penggunaan kemudahan memproses maklumat secara berkala. 2. 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. 3. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya. 4. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian. 5. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada pasukan JKSMCERT.	Pentadbir Sistem dan JKSMCERT
080404 *Clock Synchronization*	
Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain	Pentadbir Pusat Data

Sub-Kawalan	Tanggungjawab
keselamatan hendaklah diseragamkan mengikut sumber rujukan tunggal. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam JKSM atau *Network Time Zone* (NTP) perlu diselaraskan kepada sumber waktu yang ditetapkan oleh SIRIM.	
0805 Kawalan Perisian Operasi	
Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
080501 Pemasangan Perisian Pada Sistem Operasi	
Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Perkara-perkara yang perlu dipatuhi setelah mendapat kelulusan ICTSO adalah seperti berikut: 1. Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian. 2. Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya. 3. Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.	Pentadbir Sistem
0806 Pengurusan Kerentanan Teknikal	
Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya	

Sub-Kawalan	Tanggungjawab
080601 Pengurusan Kerentanan Teknikal	
Maklumat kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem aplikasi dan operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: 1. Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi. 2. Menganalisis tahap risiko kerentanan. 3. Mengambil tindakan pengolahan dan kawalan risiko.	Pentadbir Sistem
080602 Sekatan ke atas Pemasangan Perisian	
Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti berikut: 1. Hanya perisian yang diperakukan sahaja dibenarkan bagi kegunaan warga JKSM, pembekal, pakar runding dan pihak yang berurusan dengan perkhidmatan ICT JKSM. 2. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa. 3. Memastikan antivirus berupaya mengimbas semua perisian atau sistem sebelum digunakan.	Semua Pengguna

Sub-Kawalan	Tanggungjawab
0807 Pertimbangan Audit Sistem Maklumat	
Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
080701 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.	ICTSO dan Pentadbir Sistem
080702 Pemantauan dan Forensik ICT	
Pemantauan ke atas aktiviti pemprosesan maklumat dan bertanggungjawab merekodkan dan menganalisis aktiviti seperti berikut: 1. Sebarang percubaan pencerobohan kepada sistem ICT JKSM. 2. Serangan kod perosak seperti DOS, DDOS, *spam, forgery, intrusions, threats dan physical loss*. 3. Pengubahsuaian ciri peralatan, perisian atau mana-mana komponen sistem tanpa kebenaran. 4. Aktiviti melayari laman web yang tidak produktif dan membebankan *bandwidth* rangkaian. 5. Aktiviti instalasi dan penggunaan perisian yang berbahaya dan menjejaskan prestasi komputer pengguna.	ICTSO dan Pentadbir Sistem

0901 Pengurusan Keselamatan Rangkaian

0902 Pemindahan Data dan Maklumat

KAWALAN

09

KESELAMATAN KOMUNIKASI

KAWALAN 09
KESELAMATAN KOMUNIKASI

Sub-Kawalan	Tanggungjawab
0901 Pengurusan Keselamatan Rangkaian	
Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.	
090101 Kawalan Rangkaian	
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti berikut: 1. Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan. 2. Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas daripada risiko seperti banjir, gegaran dan habuk. 3. Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. 4. Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi. 5. *Firewall* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian. 6. Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan BTMK, JKSM.	Pengarah Bahagian dan Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
7. Semua perisian *sniffer* atau *network analyser* **dilarang** dipasang pada komputer pengguna kecuali mendapat kebenaran daripada ICTSO. 8. Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat JKSM. 9. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang. 10. Sebarang penyambungan rangkaian yang bukan di bawah kawalan BTMK, JKSM adalah tidak dibenarkan. 11. Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di JKSM dan penggunaan modem peribadi adalah tidak dibenarkan. 12. Kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya. 13. Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan. 14. Menempatkan atau memasang antara muka (*interfaces*) yang bersesuaian antara rangkaian JKSM, rangkaian agensi lain dan rangkaian awam. 15. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya. 16. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja.	

Sub-Kawalan	Tanggungjawab
17. Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh. 18. Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan JKSM. 19. Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan JKSM.	
090102 Keselamatan Pekhidmatan Rangkaian	
Pengurusan bagi semua perkhidmatan rangkaian dalaman atau sumber luaran yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan dalam perjanjian perkhidmatan rangkaian.	CDO, Pentadbir Sistem dan Pengarah Bahagian
09103 Pengasingan Dalam Rangkaian	
Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian JKSM.	ICTSO, Pengarah Bahagian dan Pentadbir Sistem
0902 Pemindahan Data dan Maklumat	
Memastikan keselamatan perpindahan/pertukaran data, maklumat dan perisian antara JKSM dan pihak luar.	
090201 Polisi dan Prosedur Pemindahan Data dan Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Dasar, prosedur dan kawalan pemindahan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan maklumat melalui sebarang jenis kemudahan komunikasi.	Pengguna, Warga JKSM dan Pembekal

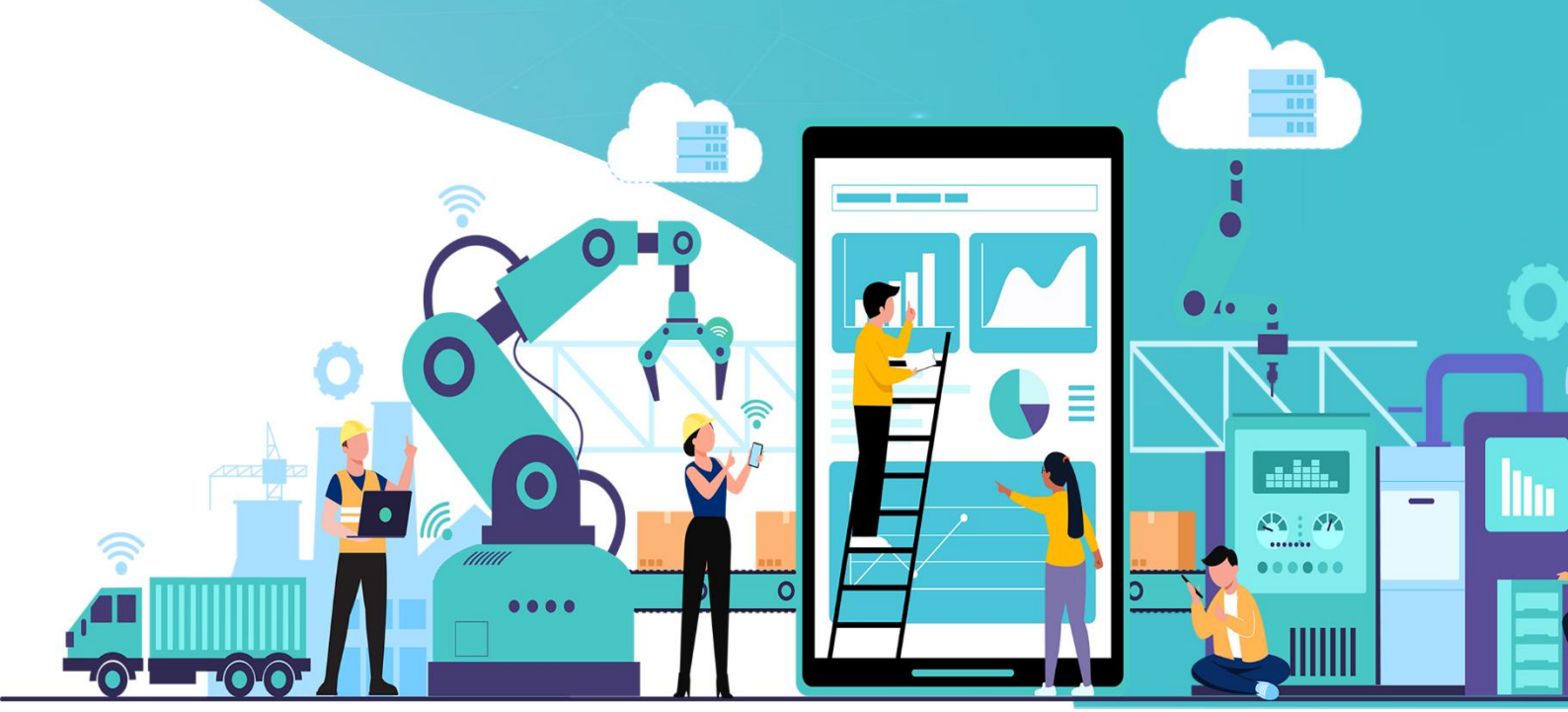
Sub-Kawalan	Tanggungjawab
2. Terma pemindahan maklumat dan perisian di antara JKSM dengan pihak luar hendaklah dimasukkan di dalam Perjanjian. 3. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan maklumat. 4. Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.	
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: 1. Pemilik Data hendaklah mengawal penghantaran dan penerimaan maklumat JKSM. 2. Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat JKSM. 3. Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat. 4. JKSM hendaklah mengenal pasti perlindungan data dalam penggunaan data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data.	CDO dan Pengarah Bahagian

Sub-Kawalan	Tanggungjawab
090203 Pengurusan Mel Elektronik	
Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Menggunakan akaun e-mel Jabatan bagi urusan rasmi. Dilarang penggunaan akaun e-mel milik pegawai lain. 2. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi. Dilarang penghantaran e-mel rasmi menggunakan akaun e-mel peribadi. 3. Sebarang e-mel rasmi hendaklah direkodkan ke dalam Sistem DDMS 2.0 untuk tujuan rekod. 4. Mengamalkan tatacara dan amalan terbaik penggunaan e-mel rasmi Jabatan. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik dan undang-undang bertulis lain yang berkuat kuasa adalah seperti di bahagian **RUJUKAN:** 1. Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003. 2. Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 – Pematuhan Tatacara Penggunaan E-mel dan Internet. 3. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2017 – Langkah-langkah Mengenai Penggunaan Mel Elektronik Agensi-agensi Kerajaan. 4. Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan (*Government Unified*	Warga JKSM

Sub-Kawalan	Tanggungjawab
Communication – MyGovUC) dan mana-mana undang-undang bertulis yang berkuat kuasa.	
090204 Perjanjian Kerahsiaan dan Ketidakdedahan (*Non-disclosure*)	
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan dari semasa ke semasa. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	ICTSO, Pentadbir Sistem dan Pembekal

1001 Keperluan Keselamatan Sistem Maklumat

1002 Keselamatan dalam Proses Pembangunan dan Perkhidmatan Sokongan



KAWALAN

10

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

KAWALAN 10
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Sub-Kawalan	Tanggungjawab
1001 Keperluan Keselamatan Sistem Maklumat	
Memastikan keselamatan maklumat dijadikan bahagian penting dalam sistem maklumat.	
100101 Analisis dan Spesifikasi Keperluan Keselamatan Maklumat	
Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada. Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut: 1. Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem. 2. Semua sistem yang dibangunkan sama ada dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan PKS JKSM. 3. Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi polisi keselamatan yang telah ditetapkan. 4. Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bai memastikan kesahihan dan integriti data. 5. Semua trafik keluar dan masuk rangkaian hendaklah melalui firewall di bawah kawalan BTMK, JKSM.	Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
100102 Melindungi Perkhidmatan Aplikasi Dalam Rangkaian Awam	
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: 1. Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi JKSM. 2. Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. 3. Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*). 4. Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; 5. Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT. 6. Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	Pentadbir Sistem
100103 Melindungi Transaksi Perkhidmatan Aplikasi	
Maklumat yang terlibat dalam perkhidmatan transaksi hendaklah dilindungi daripada penghantaran yang tidak lengkap, *mis-routing*, pengubahan mesej yang tidak	ICTSO, Pengarah Bahagian dan Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
dibenarkan, pendedahan yang tidak dibenarkan dan duplikasi mesej. Perkara yang perlu dipertimbangkan adalah seperti berikut: 1. Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi. 2. 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. 3. Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan.	
1002 Keselamatan Dalam Proses Pembangunan dan Perkhidmatan Sokongan	
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 Pembangunan Selamat	
Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan untuk perkembangan dalam organisasi. Perkara yang perlu dipertimbangkan dalam organisasi: 1. Keselamatan persekitaran pembangunan. 2. Keselamatan pangkalan data.	ICTSO, Pengarah Bahagian dan Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
3. Keselamatan dalam fasa reka bentuk. 4. Keperluan *check-point* keselamatan dalam carta perbatuan projek. 5. Keperluan pengetahuan ke atas keselamatan aplikasi. 6. Keselamatan dalam kawalan versi. 7. Bagi pembangunan secara luaran (*oursource*), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambahbaik kelemahan dalam pembangunan sistem.	
100202 Prosedur Kawalan Perubahan Sistem	
Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut: 1. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai. 2. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem operasi 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. 3. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja.	Pengarah Bahagian dan Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
4. Capaian kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.	
100203 Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi	
Apabila platform operasi berubah, aplikasi penting perniagaan hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi. Perkara yang perlu dipatuhi adalah seperti yang berikut: 1. Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform. 2. Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan. 3. Memastikan perubahan yang sesuai dibuat kepada Pelan Kesinambungan Perkhidmatan (PKP) JKSM dan Pelan Pemulihan Bencana sistem yang berkaitan berdasarkan Pelan Pengurusan Keselamatan Maklumat (ISMP) sistem tersebut.	Pentadbir Sistem
100204 Sekatan ke atas Perubahan Dalam Pakej Perisian	
Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan. Ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.	Pentadbir Sistem
100205 Prinsip Kejuruteraan Sistem Yang Selamat	
Prinsip-prinsip kejuruteraan keselamatan sistem hendaklah diwujudkan, didokumentasikan, diselenggarakan dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem	Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
bagi memastikan keberkesanan kepada keselamatan maklumat.	
100206 Persekitaran Pembangunan Selamat	
JKSM hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem (*development life-cycle*). JKSM juga perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: 1. Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem. 2. Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem. 3. Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem. 4. Pegawai yang bekerja dalam persekitaran pembangunan sistem ialah yang boleh dipercayai. 5. Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	Pentadbir Sistem
100207 Pembangunan Sistem oleh Khidmat Luar (*Outsource*)	
JKSM hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Kod sumber (*source code*) menjadi **HAK MILIK** JKSM Perkara yang perlu dipatuhi adalah seperti berikut: 1. Perkiraan pelesenan, kod sumber ialah **HAK MILIK** JKSM dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource*.	Pentadbir Sistem, Pengarah Projek

Sub-Kawalan	Tanggungjawab
2. Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori **"Pembekal hendaklah membenarkan Kerajaan hak mencapai kod sumber dan melaksanakan pengolahan risiko".** 3. Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar adalah mengikut amalan terbaik. 4. Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem. 5. Mengguna pakai prinsip dan tatacara *escrow*. 6. Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.	
100208 Pengujian Keselamatan Sistem	
Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti berikut: 1. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat. 2. Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat. 3. Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.	Pentadbir Sistem

Sub-Kawalan	Tanggungjawab
Maklumat lanjut berkaitan pengujian keselamatan sistem boleh merujuk kepada dokumen ***ISO/IEC/IEEE 29119 Software Testing Standard.***	
100209 Pengujian Penerimaan Sistem	
Aktiviti pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti berikut: 1. Pengujian penerimaan sistem hendaklah merangkumi **Keperluan Keselamatan Sistem Maklumat** (Kawalan: 100101 dan 100102) dan juga kepatuhan kepada **Dasar Pembangunan Selamat** (Kawalan: 100201). 2. Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem diguna pakai. 3. Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan (*vulnerability scanner*). Maklumat lanjut berkaitan pengujian keselamatan sistem boleh merujuk kepada dokumen ***ISO/IEC/IEEE 29119 Software Testing Standard.***	Pentadbir Sistem
1003 Data Ujian	
Memastikan perlindungan ke atas data yang digunakan untuk pengujian.	

Sub-Kawalan	Tanggungjawab
100301 Perlindungan Data Ujian	
Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut: 1. Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian. 2. Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian. 3. Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadamkan sebaik sahaja pengujian selesai. 4. Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.	ICTSO, Pentadbir Sistem, Pembekal dan Pengguna

[Halaman ini sengaja dibiarkan kosong]

1101 Keselamatan Maklumat dalam Hubungan Pembekal

1102 Pengurusan Penyampaian Perkhidmatan Pembekal

KAWALAN

11

HUBUNGAN PEMBEKAL

KAWALAN 11
HUBUNGAN PEMBEKAL

Sub-Kawalan	Tanggungjawab
1101 Keselamatan Maklumat Dalam Hubungan Pembekal	
Memastikan aset ICT JKSM yang boleh dicapai oleh pembekal dilindungi.	
110101 Polisi Keselamatan Maklumat Untuk Hubungan Pembekal	
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset MAMPU. Perkara yang perlu dipertimbangkan adalah seperti berikut: 1. Mengenal pasti dan mendokumentasikan jenis pembekal mengikut kategori. 2. Proses kitaran hayat (*life cycle*) yang seragam untuk menguruskan pembekal.. 3. Mengawal dan memantau akses pembekal. 4. Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian. 5. Jenis-jenis obligasi kepada pembekal. 6. Pelan kontigensi (*contigency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat. 7. Melaksanakan taklimat kesedaran terhadap Polisi Keselamatan Siber JKSM kepada pembekal. 8. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber JKSM (Rujuk LAMPIRAN A). 9. Pembekal perlu mematuhi arahan keselamatan yang berkuat kuasa dari semasa ke semasa.	Pengarah Bahagian, Pemilik Projek dan Pembekal

Sub-Kawalan	Tanggungjawab
110102 Menangani Keselamatan Dalam Perjanjian Pembekal	
Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan menyampaikan atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua kakitangan mereka yang terlibat mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak JKSM selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa. Sekiranya pihak syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti berikut: 1. JKSM hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan. 2. Syarikat pembekal yang mempunyai persijilan keselamatan yang berkaitan hendaklah diberi keutamaan. 3. Semua wakil syarikat hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan. 4. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi. 5. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang	Pengarah Bahagian, Pemilik Projek dan Pembekal

Sub-Kawalan	Tanggungjawab
relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan JKSM. 6. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh JKSM.	
110103 Rantaian Bekalan Teknologi Maklumat dan Komunikasi	
Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara yang perlu diambil kira adalah seperti berikut: 1. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan. 2. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberi perkhidmatan atau pembekalan produk. 3. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	Pengarah Bahagian, Pemilik Projek dan Pembekal
1102 Pengurusan Penyampaian Perkhidmatan Pembekal	
Mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.	
110201 Pemantauan dan Kajian Perkhidmatan Pembekal	
JKSM hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal.	Pengarah Bahagian, Pemilik Projek dan Pembekal

Sub-Kawalan	Tanggungjawab
Perkara-perkara yang perlu diambil kira adalah seperti berikut: 1. Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan. 2. Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan. 3. Memaklumkan mengenai insiden keselamatan kepada pembekal dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	
110202 Pengurusan Perubahan Perkhidmatan Pembekal	
Perubahan kepada peruntukan perkhidmatan oleh pembekal termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan dengan mengambil kira kepentingan maklumat, sistem da proses perniagaan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti berikut: 1. Perubahan dalam perjanjian dengan pembekal. 2. Perubahan yang dilakukan oleh JKSM bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur. 3. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan sub-kontraktor.	Pengarah Bahagian, Pemilik Projek dan Pembekal

1201 Pengurusan dan Penambahbaikan Insiden Keselamatan Maklumat

KAWALAN

12

PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

KAWALAN 12

PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

Sub-Kawalan	Tanggungjawab
1201 Pengurusan dan Penambahbaikan Insiden Keselamatan Maklumat	
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. Pengurusan insiden JKSM adalah berdasarkan kepada Prosedur Operasi Standard Teknikal ICT JKSM: Pengurusan Pengendalian Insiden Keselamatan ICT JKSM yang berkuat kuasa. Perkara yang perlu dipertimbangkan adalah seperti berikut: 1. Memberikan kesedaran berkaitan Prosedur Operasi Standard Teknikal ICT JKSM: Pengurusan Pengendalian Insiden Keselamatan ICT dan hebahan kepada warga JKSM sekiranya ada perubahan. 2. Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.	ICTSO, JKSMCERT dan Pengarah Bahagian
120102 Mekanisme Pelaporan Insiden	
Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada JKSMCERT.	Warga JKSM, Pembekal

Sub-Kawalan	Tanggungjawab
Perkara berkaitan insiden yang perlu dipertimbangkan adalah seperti berikut: 1. Maklumat didapati hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa. 2. Maklumat disyaki hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa. 3. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian. 4. Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan. 5. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar. 6. Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka. Prosedur pelaporan insiden keselamatan siber adalah berdasarkan kepada: 1. Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian *Government Computer Emergency Response Team* (GCERT) oleh NACSA bertarikh 28 Januari 2019 2. Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022	
120103 Pelaporan Kelemahan Keselamatan Maklumat	
Warga JKSM dan pihak-pihak yang menggunakan sistem dan perkhidmatan maklumat JKSM dikehendaki	CDO, ICTSO, Warga JKSM, Pengguna dan Pembekal

Sub-Kawalan	Tanggungjawab
mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT kepada JKSMCERT.	
120104 Penilaian dan Keputusan Mengenai Aktiviti Keselamatan Maklumat	
Insiden keselamatan maklumat hendaklah dinilai dan diputuskan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.	ICTSO
120105 Tindak Balas Terhadap Insiden Keselamatan Maklumat	
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: 1. Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku. 2. Menjalankan kajian forensik sekiranya perlu. 3. Menghubungi pihak yang berkenaan dengan secepat mungkin. 4. Menyimpan jejak audit, semakan fail sandaran dan melindungi integriti semua bahan bukti. 5. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan. 6. Menyediakan pelan kontigensi dan mengaktifkan Pelan Kesinambungan Perkhidmatan. 7. Menyediakan tindakan pemulihan segera. 8. Memaklumkan atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan kepada Prosedur Operasi Standard	ICTSO

Sub-Kawalan	Tanggungjawab
Teknikal ICT JKSM: Pengurusan Pengendalian Insiden Keselamatan ICT.	
120106 Pembelajaran Daripada Insiden Keselamatan Maklumat	
Pengetahuan dan pengalaman yang diperoleh daripada menganalisis dan menyelesaikan kes-kes insiden keselamatan maklumat perlu digunakan untuk mengurangkan kemungkinan dan kesan kejadian pada masa hadapan. Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.	ICTSO dan JKSMCERT
120107 Pengumpulan Bahan Bukti	
JKSM hendaklah menentukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti.	ICTSO dan JKSMCERT

1301 Kesinambungan Keselamatan Maklumat

1302 Lewahan (Redundancy)

KAWALAN

13

ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

KAWALAN 13
ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Sub-Kawalan	Tanggungjawab
1301 Kesinambungan Keselamatan Maklumat	
Memastikan kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem Pengurusan Kesinambungan Perkhidmatan JKSM.	
130101 Perancangan Kesinambungan Keselamatan Maklumat	
JKSM hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan. Ini bertujuan memastikan tiada gangguan kepada proses dalam penyediaan perkhidmatan organisasi dan mengenal pasti keselamatan maklumat pada lokasi kesinambungan perkhidmatan. Dalam merancang kesinambungan keselamatan maklumat, JKSM perlu mengambil kira isu-isu dalaman dan luaran berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi JKSM. Perkara yang perlu dipertimbangkan adalah seperti berikut: 1. Menubuhkan pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) JKSM. 2. Mengenal pasti perkhidmatan kritikal. 3. Menetapkan polisi PKP. 4. Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak Balas Kecemasan dan Pelan Pemulihan Bencana ICT.	Jawatankuasa Pemandu PKP, Kumpulan Tindak Balas Kecemasan (ERT), Kumpulan Komunikasi Krisis (CCT), Kumpulan Pemulihan Bencana (DRT)

Sub-Kawalan	Tanggungjawab
5. Melaksanakan program kesedaran dan latihan kepada warga JKSM. 6. Melaksanakan simulasi ke atas dokumen di perkara 4. 7. Melaksanakan penyelenggaraan dokumen PKP secara berkala.	
130102 Pelaksanaan Kesinambungan Keselamatan Maklumat	
JKSM hendaklah menyedia, mendokumenkan, melaksana dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti berikut: 1. Mengaktifkan dan melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal JKSM yang telah dikenal pasti berdasarkan kepada Pelan Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak Balas Kecemasan dan Pelan Pemulihan Bencana ICT terkini. 2. Melaksanakan *post-mortem* dan mengemas kini pelan di dalam PKP. 3. Mengemas kini pelan PKP jika berlaku perubahan kepada fungsi kritikal JKSM. 4. Mengemas kini struktur tadbir urus PKP JKSM jika berlaku pertukaran pegawai bersara dan bertukar keluar. 5. Memastikan kumpulan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksanakan PKP.	Jawatankuasa Pemandu PKP, Kumpulan Tindak Balas Kecemasan (ERT), Kumpulan Komunikasi Krisis (CCT), Kumpulan Pemulihan Bencana (DRT)

Sub-Kawalan	Tanggungjawab
130103 Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat	
JKSM hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.	Jawatankuasa Pemandu PKP, Kumpulan Tindak Balas Kecemasan (ERT), Kumpulan Komunikasi Krisis (CCT), Kumpulan Pemulihan Bencana (DRT)
1302 Lewahan (*Redundancy*)	
Memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.	
130201 Ketersediaan Kemudahan Pemprosesan Maklumat	
Kemudahan pemprosesan maklumat JKSM yang mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (*failover test*) keberkesanannya dari semasa ke semasa.	Pentadbir Pusat Data, Pentadbir Sistem

[Halaman ini sengaja dibiarkan kosong]

1401 Pematuhan Terhadap Keperluan Perundangan dan Kontrak

1402 Kajian Semula Keselamatan Maklumat

KAWALAN

14

PEMATUHAN

KAWALAN 14

PEMATUHAN

Sub-Kawalan	Tanggungjawab
1401 Pematuhan Terhadap Keperluan Perundangan dan Kontrak	
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 Pengenalpastian Keperluan Undang-undang dan Kontrak yang Terpakai	
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh kakitangan JKSM dan pembekal. Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di JKSM dan pembekal adalah seperti di **LAMPIRAN C**.	Semua Pengguna
140102 Hak Harta Intelek	
Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan pelesenan di mana mematuhi had pengguna yang telah ditetapkan atau dibenarkan dan hanya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Semua Pengguna
140103 Perlindungan Rekod	
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung dalam keperluan perundangan, peraturan dan perjanjian kontrak.	Semua Pengguna

Sub-Kawalan	Tanggungjawab
140104 Privasi dan Perlindungan Maklumat Peribadi	
JKSM hendaklah memberi jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.	Semua Pengguna
140105 Peraturan Kawalan Kriptografi	
Kawalan kriptografi hendaklah dilaksanakan mengikut perundangan, peraturan dan perjanjian kontrak.	Semua Pengguna
1402 Kajian Semula Keselamatan Maklumat	
Untuk memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur JKSM.	
140201 Kajian Semula Keselamatan Maklumat Secara Berkecuali (*Independent Review of Information Security*)	
Penilaian keselamatan maklumat oleh pihak pembekal hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	CDO dan Pemilik Projek
140202 Pematuhan Polisi dan Standard Keselamatan	
JKSM hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti dalam polisi, piawaian dan keperluan teknikal.	CDO dan Pemilik Projek
140203 Kajian Semula Pematuhan Teknikal	
JKSM hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan	CDO dan Pemilik Projek

Sub-Kawalan	Tanggungjawab
prosedur seperti yang terkandung dalam polisi, piawaian dan keperluan komputer.	

[Halaman ini sengaja dibiarkan kosong]

SINGKATAN

TAKRIFAN

GLOSARI

GLOSARI

Singkatan

CGSO	Pejabat Ketua Pegawai Keselamatan Kerajaan
DTSA	Data Terbuka Sektor Awam
ISMS	*Information Security Management System*
JKSM	Jabatan Kehakiman Syariah Pelan
JKSN/MSN	Jabatan Kehakiman Syariah Negeri/ Mahkamah Syariah Negeri
MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Pelan
NACSA	Agensi Keselamatan Siber Negara (*National Cyber Security Agency*)
PDSA	Pusat Data Sektor Awam
PKP	Pelan Kesinambungan Perkhidmatan
SPPA	Sistem Pemantauan Pengurusan Aset

Takrifan

Antivirus	Perisian yang berupaya mengimbas dan menyekat perisian hasad daripada merosakkan perkakasan komputer atau sistem aplikasi.
Arahan Keselamatan	Panduan mengenai peraturan-peraturan yang perlu dipatuhi oleh semua kakitangan Kerajaan. Dokumen ini dikeluarkan oleh CGSO.
Backup	Aktiviti sandaran yang terdiri daripada salin dan muatan semula.
Bandwidth	Jalur lebar

GLOSARI

Closed Circuit Television (CCTV)	Sistem televisyen yang digunakan secara pelan di mana satu sistem TV kamera video yang dipasang di dalam atau sekitar premis/pejabat bagi tujuan membantu pemantauan fizikal.
Data-dalam-simpanan	data-dalam-simpanan (*data-in-rest*) Data yang tidak aktif yang disimpan secara fizikal dalam bentuk digital (contohnya pangkalan data, gudang data, hamparan, arkib dan sebagainya).
Data-dalam-penggunaan	data-dalam-penggunaan (*data-in-use*) Data yang sedang diperbaharui, diproses, dihapus, diakses atau dibaca oleh sistem. Jenis data ini tidak disimpan secara pasif, tetapi bergerak aktif melalui infrastruktur IT.
Data-dalam-pergerakan	data-dalam-pergerakan (*data-in-motion*) Data transit atau maklumat digital yang sedang dalam proses pergerakan di dalam atau antara sistem komputer.
Disaster Recovery Center (DRC)	Pusat Pemulihan Bencana Premis yang dipilih dan dilengkapi infrastruktur komputer dan rangkaian yang menjadi sandaran kepada sistem aplikasi Jabatan apabila berlaku bencana.
Disaster Recovery Pelan (DRP)	Pelan Pemulihan Bencana bagi mengurus proses pemulihan selepas berlaku gangguan terhadap perkhidmatan ICT JKSM.
DOS / DDOS	*Denial-of-Service / Distributed Denial-of-service*

	Jenis serangan siber yang menghalang capaian kepada sistem aplikasi.
Enkripsi	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.
Factory Acceptance Check (FAC)	Pengujian ke atas peralatan atau komponen sebelum penghantaran dibuat.
Firewall	Sistem yang direka untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman/luaran. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Jenayah siber yang menyalin dan menyerupai dokumen asal.
Hardisk	Cakera keras yang digunakan untuk menyimpan data.
Internet	Sistem rangkaian seluruh dunia di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
Internet Gateway	Nod atau titik rangkaian yang bertindak sebagai pintu masuk ke rangkaian lain yang menggunakan protokol yang berbeza untuk berkomunikasi.

GLOSARI

Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
Intrusion Prevention System (IPS)	Sistem keselamatan yang berfungsi mengesan dan menyekat sebarang serangan kod *malware* ke atas sistem rangkaian Jabatan.
Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasi dan mengakibatkan pelanggaran keselamatan.
Kawasan Terperingkat	Ruang atau bilik yang menempatkan operasi berkaitan dokumen terperingkat.
Kriptografi	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
Pasukan Komunikasi Krisis	*Crisis Communication Team* (CCT) Pasukan yang ditubuhkan di dalam PKP bagi mengkoordinasi makluman kepada orang awam, ahli keluarga dan saudara mara warga JKSM mengenai keadaan mereka apabila berlaku gangguan.
Pasukan Tindakan Kecemasan	*Emergency Response Team* (ERT) Pasukan yang ditubuhkan di dalam PKP bagi memastikan tindakan segera dalam mengawal kejadian kecemasan di JKSM.

Patch	Perisian sistem operasi khusus dalam menangani kelemahan atau kerentanan (*vulnerabilities*) dalam satu-satu produk.
Pegawai Keselamatan ICT (ICTSO)	Pegawai ICT yang dilantik dan berperanan mengurus program keselamatan ICT.
Pegawai Pengelas	Pegawai yang dilantik di bawah peruntukan Seksyen 2B Akta Rahsia Rasmi 1972 (Akta 88) dan bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan daripada segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
Pegawai Teknologi Maklumat	Pegawai Teknologi Maklumat Gred F41 dan ke atas lantikan Persekutuan di JKSM.
Pemilik Data	Pihak yang bertanggungjawab mengeluarkan dan mengesahkan kesahihan sesuatu set data atau maklumat yang berada di dalam bidang atau fungsi. Juga bertanggungjawab mengawal keselamatan dan kualiti data tersebut.
Pengarah-pengarah Bahagian	Pengarah Bahagian dan Ketua Unit di JKSM: • Bahagian Pendaftaran, Keurusetiaan dan Rekod (BPKR) • Bahagian Sokongan Keluarga (BSK) • Bahagian Latihan (BL) • Bahagian Dasar dan Penyelidikan (BDP) • Bahagian Pusat Sumber Maklumat dan Penerbitan (BPSMP)

GLOSARI

	• Bahagian Khidmat Pengurusan dan Sumber Manusia (BKPSM) • Bahagian Teknologi Maklumat dan Komunikasi (BTMK) • Unit Komunikasi Korporat (UKK) • Unit Integriti (UI)
Pengolahan Risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dilaksana berdasarkan hasil penilaian risiko.
Physical loss	Jenis kerosakan atau kehilangan data dan fungsi sesuatu sistem komputer.
Readable Access Memory (RAM)	Memori komputer yang hanya boleh membaca (*read*) dan tidak boleh menulis (*write*) data ke atasnya.
Rollback	Pengembalian pangkalan atau program kepada keadaan stabil sebelum sesuatu ralat berlaku.
Router	Peralatan rangkaian yang berupaya menentukan laluan trafik rangkaian berdasarkan polisi yang ditetapkan.
Server	Perkakasan yang mengandungi sistem komputer yang memberi perkhidmatan menghantar atau menerima atau menyimpan data.
Source Code	Kod sumber atau kod program (biasanya dipanggil sumber atau kod) merujuk kepada sebarang penyataan yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia.

Spam	Sebarang bentuk komunikasi digital yang tidak dikehendaki dalam bentuk kiriman pesanan yang banyak.
Switch	Peralatan sebagai komponen rangkaian komputer yang menghubungkan lebih daripada satu buah komputer dalam sebuah jaringan.
Threat	Ancaman serangan siber yang berupaya merosakkan sistem dan rangkaian komputer.
Virtual Private Network (VPN)	Sistem perhubungan rangkaian Internet terenkrip yang membolehkan penghantaran dan penerimaan data sensitif dengan selamat.
Virus	Atur cara komputer yang bertujuan merosakkan data atau sistem aplikasi.
Warga JKSM	Kakitangan Kerajaan yang berkhidmat di JKSM sama ada berjawatan tetap atau kontrak atau sambilan.
Wireless LAN	Jaringan komputer dalaman yang terhubung tanpa kabel. Pengesanan signal adalah melalui *access point*.

[Halaman ini sengaja dibiarkan kosong]

LAMPIRAN A SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER JKSM

LAMPIRAN B CARTA ALIRAN PELAPORAN INSIDEN KESELAMATAN ICT JKSM

LAMPIRAN C UNDANG-UNDANG/PEKELILING/ ARAHAN TERPAKAI

LAMPIRAN

LAMPIRAN A

SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER JKSM

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER JKSM

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 B

BORANG PENDAFTARAN BRING YOUR OWN DEVICE (BYOD)

Tarikh Terima:

PENDAFTARAN *BRING YOUR OWN DEVICE* (BYOD)

Pengguna hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT JKSM/JKSN/MSN dan juga Tatacara Keselamatan ICT JKSM yang sedang berkuatkuasa.

MAKLUMAT PEMOHON	
Nama Pengguna:	**Jawatan & Gred:**
Bahagian/Seksyen/Unit:	

MAKLUMAT PERMOHONAN	
Kategori dan Maklumat Perkakasan	
☐ Komputer Riba	Nama Host : OS : MAC Address : Antivirus : (Pastikan antivirus yang dipasang sentiasa terkemas kini)
☐ Telefon Bimbit / Tablet / iPad	Nama Host : OS : MAC Address :
Tujuan Permohonan	
Perakuan Pemohon	
☐ Saya telah membaca, memahami dan menandatangani Dasar Keselamatan ICT JKSM/JKSN/MSN. ☐ Saya telah membaca dan memahami Tatacara Keselamatan ICT JKSM. ☐ Saya akan patuh dengan dasar dan tatacara yang berkuatkuasa. ☐ Saya juga bersetuju dan bersedia diambil tindakan sekiranya melanggar mana-mana dasar/tatacara yang ditetapkan.	
Tandatangan Pemohon: ..... (Nama dan Jawatan)	**Tandatangan Pengarah Bahagian:** ..... (Nama dan Jawatan)

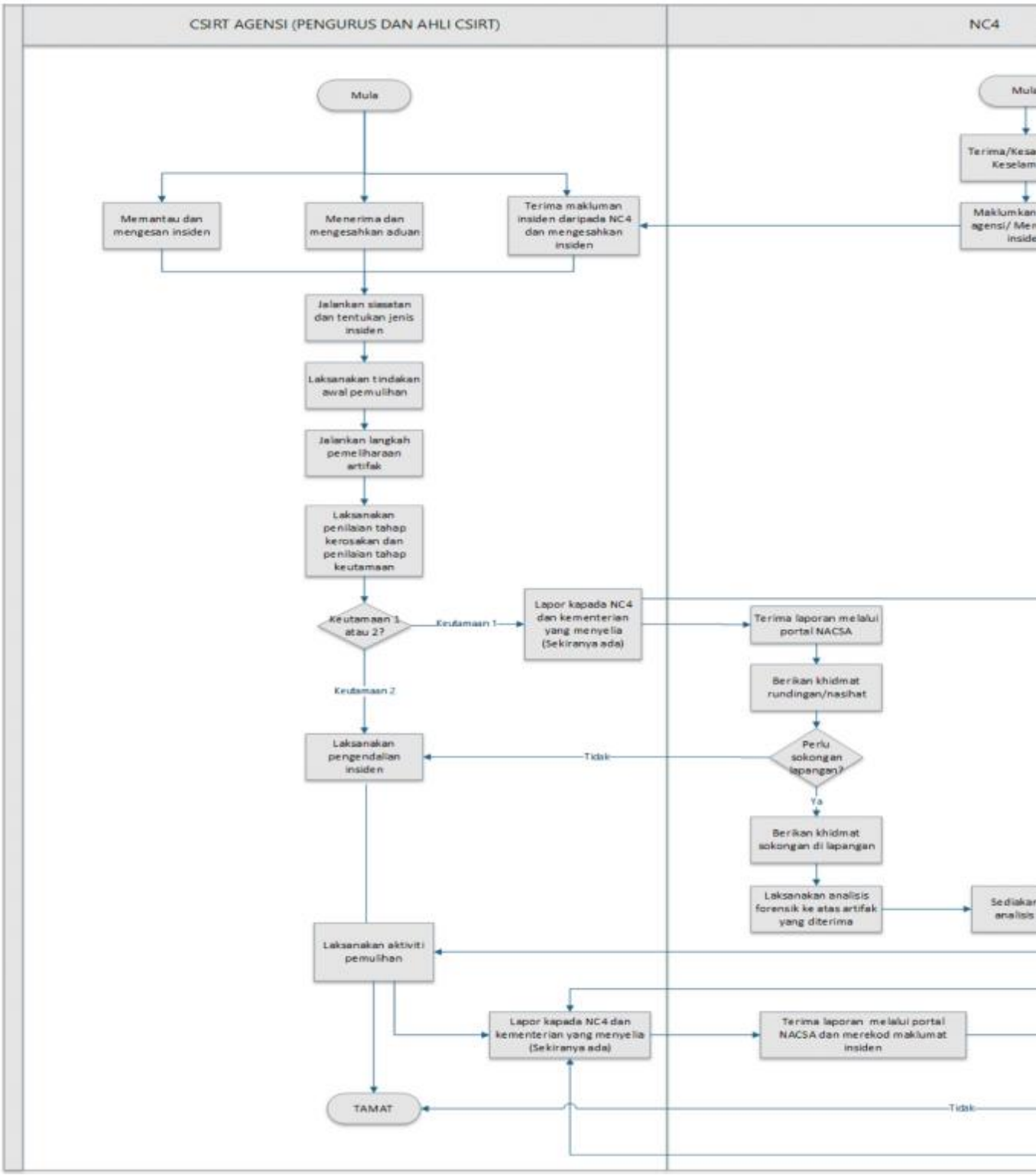
UNTUK KEGUNAAN BAHAGIAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI	
Diluluskan/ Tidak Diluluskan ☐ Lulus ☐ Tidak Diluluskan	**Tarikh:**
Catatan:	

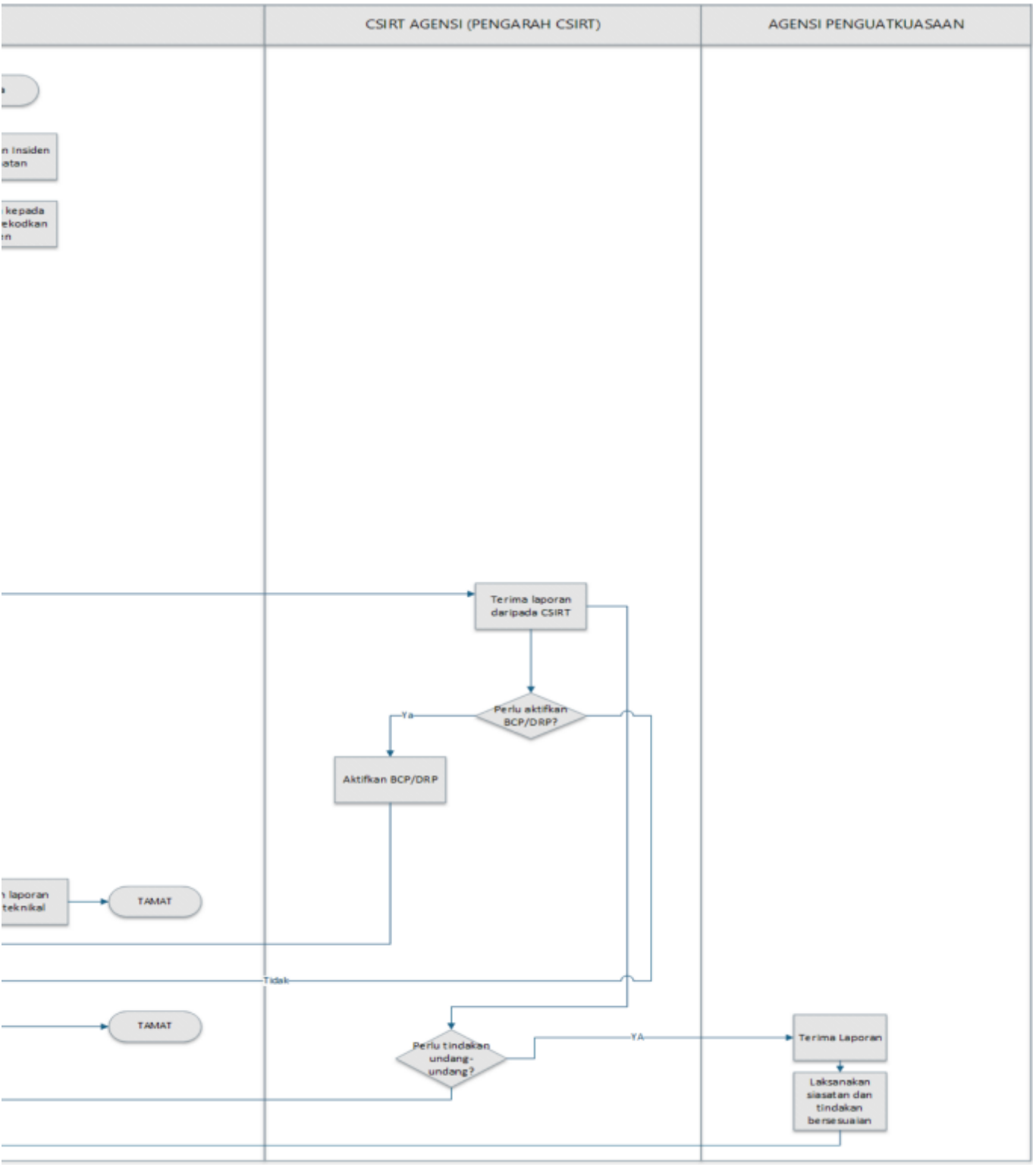
Nota:
Semua pegawai dikehendaki mematuhi garis panduan dan bertanggungjawab ke atas perkara-perkara berikut:

(a) Memastikan dokumen yang dikendalikan bukan dokumen terperingkat;
(b) Memaklumkan kepada Ketua Jabatan masing-masing jika berlaku kehilangan peralatan persendirian; dan
(c) Memastikan maklumat/dokumen rasmi yang disimpan di dalam peranti persendirian dihapuskan terlebih dahulu sebelum peralatan diganti/ dilupus/ ditukar milik.

LAMPIRAN C

CARTA ALIR PELAPORAN INSIDEN KESELAMATAN ICT JKSM




CSIRT AGENSI (PENGARAH CSIRT)
AGENSI PENGUATKUASAAN
Terima laporan daripada CSIRT
Perlu aktifkan BCP/DRP?
Ya
Aktifkan BCP/DRP
TAMAT
Tidak
TAMAT
Perlu tindakan undang-undang?
YA
Terima Laporan
Laksanakan siasatan dan tindakan bersesuaian

LAMPIRAN D

UNDANG-UNDANG / PEKELILING / ARAHAN TERPAKAI

Polisi Keselamatan Siber JKSM ini hendaklah dibaca bersama dengan akta-akta, warta, pekeliling-pekeliling, surat pekeliling dan peraturan dalaman yang berkaitan dan sedang berkuat kuasa antaranya seperti berikut:

1. Arahan Keselamatan
2. Akta Rahsia Rasmi 1972
3. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS)
4. Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan
5. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)
6. Pekeliling Kemajuan Perkhidmatan Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan
7. Pelan Pengurusan Perkhidmatan (PKP) JKSM, 2019
8. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam

JABATAN KEHAKIMAN SYARIAH MALAYSIA

Blok C, Kompleks Islam Putrajaya
No. 20, Jalan Tunku Abdul Rahman, Presint 3
621000 Putrajaya

Tel: 03-8870 9200
Faks: 8870 9500