KEJORA

VERSI 1.1

POLISI KESELAMATAN SIBER (PKS)

BAHAGIAN TEKNOLOGI MAKLUMAT

LEMBAGA KEMAJUAN JOHOR TENGGARA (KEJORA)

KEMENTERIAN PEMBANGUNAN LUAR BANDAR (KPLB)

Sejarah Dokumen

VERSI	TARIKH UBAH	KELULUSAN	TARIKH KUATKUASA
1.0	April 2019	Mesyuarat JPICT KEJORA Bil 1/2019	26 April 2019
1.1	April 2021	Mesyuarat JPICT KEJORA Bil 1/2021	27 April 2021

Rekod Kawalan Pindaan Dokumen

TARIKH	VERSI	BUTIRAN PINDAAN
26 April 2019	1.0	Keluaran Pertama
27 April 2021	1.1	Penambahbaikan A.6.2.2 Telekerja

1 KANDUNGAN

1.0 PENGENALAN

Lembaga Kemajuan Johor Tenggara (KEJORA) adalah salah sebuah agensi badan berkanun di bawah Kementerian Pembangunan Luar Bandar (KPLB) yang berfungsi sebagai agen Pembangunan Wilayah bagi kawasan Tenggara Negeri Johor. Pembahagian wilayah meliputi 16% kawasan Negeri Johor dengan jumlah keluasan 300,111 hektar.

Selaras dengan peranan tersebut KEJORA telah melaksanakan projek pengkomputerannya bagi memastikan penyediaan perkhidmatan kepada pelanggan dapat dilakukan dengan pantas dan berkesan.

Polisi Keselamatan Siber (PKS) menghuraikan pendekatan KEJORA ke atas keselamatan ICT dan ianya menjadi penanda aras komitmen pihak pengurusan. Dokumen ini menjadi dokumen rujukan utama yang menjurus kepada pembinaan dokumen yang berkaitan dengannya (garis panduan, prosedur dan sebagainya).

Kakitangan KEJORA mempunyai tanggungjawab bersama untuk melindungi Aset ICT dan dalam masa yang sama mengawal maklumat dan hak intelek yang dipunyai oleh KEJORA. Segala aset yang kritikal perlulah dikawal untuk mengurangkan sebarang impak yang boleh mengganggu perkhidmatan di KEJORA. Kawalan keselamatan ICT di KEJORA merupakan fungsi kritikal yang perlu diterapkan ke dalam semua operasi dan perkhidmatan KEJORA.

1.1 OBJEKTIF

Dokumen ini menyediakan penyataan PKS yang perlu dipatuhi oleh kakitangan KEJORA. Ianya bertujuan untuk:

a. Menjamin semua aset ICT (termasuk maklumat elektronik dan bukan elektronik, perisian, data, rangkaian data dan peralatan) dan pengguna, peratura, tanggungjawab serta kemudahan ICT yang terdapat di KEJORA adalah dlilindungi sepenuhnya daripada kemusnahan, kehilangan, disalahgunakan atau penyelewengan

b. Membantu membimbing para pegawai dan kekitangan KEJORA menggunakan kaedah yang sistematik dan seragam dalam melaksanakan tugas-tugas dan tanggungjawab yang melibatkan ICT

c. Memastikan segala perkhidmatan akan berjalan dengan lancar dan berterusan

d. Melindungi kepentingan mereka yang bergantung pada teknologi maklumat daripada kesan kegagalan ICT dari segi kerahsiaan, integriti, kebolehsediaan dan ‘tidak boleh disangkal’

e. Mencegah salahguna dan kecurian aset ICT Jabatan

1.2 PERNYATAAN POLISI KESELAMATAN SIBER (PKS)

Polisi Keselamatan Siber adalah satu polisi untuk melindungi aset ICT dengan meminimumkan kesan insiden keselamatan. Ini adalah bertujuan untuk menjamin kesinambungan urusan dengan menekankan aspek kepenggunaan aset ICT serta prosedur keselamatan yang perlu diikuti seperti yang telah ditetapkan

1.3 SKOP

Keselamatan Aset ICT KEJORA merangkumi Kategori Maklumat, Aliran Data, Platform Aplikasi dan Perisian, Peranti Fizikal dan Sistem, Sistem Luaran serta Sumber Luaran seperti berikut:

1.3.1 Kategori Maklumat

Semua penyedia perkhidmatan dalam KEJORA hendaklah mengenal pasti kategori maklumat yang mencukupi dan bersesuaian. Semua maklumat yang dijana atau dikumpul oleh KEJORA hendaklah diasingkan mengikut kategori:

a) Maklumat Rahsia Rasmi

Maklumat Rahsia Rasmi mempunyai erti yang diberikan kepadanya di bawah Akta Rahsia Rasmi 1972 [Akta 88]. Apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 [Akta 88] dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.

b) Maklumat Rasmi

Maklumat Rasmi adalah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh KEJORA semasa menjalankan urusan rasmi. Maklumat Rasmi ini juga adalah merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

c) Maklumat Pengenalan Peribadi

Maklumat Pengenalan Peribadi (PII atau *Personally Identifiable Information*) adalah maklumat yang boleh digunakan secara tersendiri atau digunakan dengan maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu.

Sebaliknya, PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

d) Data Terbuka

Data Terbuka adalah data yang boleh diakses, diguna dan dikongsi oleh sesiapa jua untuk pelbagai tujuan. PII dikecualikan daripada Data Terbuka.

1.3.2 Aliran data

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

e) Saluran komunikasi dan aliran data antara sistem dalam KEJORA;

f) Saluran komunikasi dan aliran data ke sistem luar; dan

g) Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

1.3.3 Platform Aplikasi dan Perisian

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

1.3.4 Peranti Fizikal dan Sistem

Semua peranti fizikal yang digunakan dalam Jabatan hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Peranti fizikal termasuk:

a) Pelayan

b) Peranti/Peralatan Rangkaian

c) Komputer Peribadi

d) Komputer Riba

e) Telefon /peranti pintar

f) Media Storan

g) Peranti dengan sambungan ke rangkaian, contohnya pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV)

h) Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi Kerajaan

i) Peranti pengesahan (*authentication devices*), contohnya token keselamatan, *dongle* dan alat pengimbas *biometric*

1.3.5 Sistem Luaran

Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dipastikan keselamatannya secara berkala. Sistem luaran adalah sistem bukan milik KEJORA yang dihubungkan dengan sistem KEJORA.

1.3.6 Sumber Luaran

Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dipastikan keselamatannya secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi KEJORA. Contoh perkhidmatan sumber luaran ialah:

a) Perisian Sebagai Satu Perkhidmatan
b) Platform Sebagai Satu Perkhidmatan
c) Infrastruktur Sebagai Satu Perkhidmatan
d) Storan Pengkomputeran Awan
e) Pemantauan Keselamatan

Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dan dikaji semula dipastikan keselamatannya secara berkala.

1.4 TERMA DAN DEFINASI

Aset ICT	Sebarang objek ICT yang mempunyai nilai kepada organisasi.
Sandaran	Salinan fail atau program yang dijanakan untuk memudahkan proses pemulihan dijalankan.
Business Impact Analysis	Analisa berkaitan keperluan sistem ICT, proses dan hubungankait antara keduanya yang digunakan untuk menyediakan sistem kontigensi dan keutamaan yang perlu diberikan semasa bencana.
Change Management	Proses yang memastikan semua perubahan ke atas infrastruktur ICT ditaksirkan, ditentusahkan, dilaksanakan dan dikaji semula dalam keadaan terkawal untuk memastikan gangguan tidak berlaku.
Polisi	Pernyataan peringkat tinggi mengenai prinsip, matlamat dan objektif termasuk juga cara-cara untuk mencapainya bagi subjek yang spesifik.
Emel	Mesej yang dihantar secara elektronik.
Impak	Hasil atau lanjutan dari sesuatu kejadian.
Integriti	Keadaan di mana maklumat tersimpan mengikut cara yang dibenarkan dan tiada perubahan dilakukan yang menjadikan maklumat itu berlainan dari asal.
Kawalan	Langkah-langkah penjagaan yang mana bila ia dilakukan dengan betul, akan mengurangkan risiko kemusnahan terhadap aset.

Kerahsiaan	Keadaan di mana maklumat sensitif dikawal dan diberikan kepada pengguna yang sah sahaja.
Keselamatan Fizikal	Prosedur kawalan yang wujud untuk menghalang penceroboh dari memasuki sistem atau prasarana.
Ketersediaan	Keadaan di mana maklumat atau proses sentiasa boleh dicapai dan digunakan oleh pihak yang dibenarkan.
Pengasingan Tugas	Pengasingan tugas dan tanggungjawab supaya tiada individu boleh mengsabotaj sistem kritikal yang dikendalikannya.
Pengguna ICT	Kakitangan KEJORA (tetap, sementara, kontrak) atau pihak ketiga (perunding, kontraktor, pembekal dan pembekal perkhidmatan) yang diberikan hak capaian kepada aset ICT KEJORA.
Pihak Ketiga	Individu yang selain dari kakitangan KEJORA seperti perunding, pembekal, kontraktor, pembekal perkhidmatan dan sebagainya. Kakitangan dari Agensi Kerajaan selain daripada KEJORA juga diklasifikasikan sebagai pihak ketiga.
Risiko	Kemungkinan untuk sesuatu terjadi yang boleh memberikan impak kepada objektifnya.
JPICT	Jawatankuasa Pemandu ICT
Secure Areas *(*Kawasan Terkawal*)*	Kawasan di mana KEJORA menempatkan aset ICT dan maklumat yang sensitif dan kritikal seperti Pusat Data atau bilik pejabat yang mengandungi maklumat yang sulit.

Shred	Cara-cara untuk 'melupuskan media, dengan cara merincih atau menghancurkannya kepada bahagian yang kecil.
Virus	Kod yang dibangunkan untuk merosakkan integriti maklumat dan mengganggu pengoperasian sistem.
Vulnerability (Kerentanan)	Kelemahan dari segi prosedur, senibina, implementasi dan kawalan dalaman yang boleh dieksploitasi hingga mengakibatkan pelanggaran aspek keselamatan atau polisi keselamatan.

1.5 PRINSIP KESELAMATAN

Berikut merupakan prinsip-prinsip asas yang perlu diikuti:

a. Capaian Atas Dasar "Perlu Tahu"

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

b. Capaian yang minimum

Hak capaian kepada pengguna hanya diberi pada tahap aset yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas adalah diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu data atau maklumat.

c. Accountability

Semua kakitangan adalah bertanggungjawab atas segala tindakan mereka terhadap aset ICT di KEJORA.

d. Pembahagian Tugas

Tugas mewujud, memadam, kemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan. Pembahagian tugas juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

e. Audit

Tujuan aktiviti ini ialah untuk mengenal pasti insiden keselamatan atau megenal pasti keadaan yang mengancam keselamatan. Dengan itu, aset ICT seperti komputer, server*, router*, *firewall* dan rangkaian hendaklah menyelenggara akan jejak audit.

f. Pematuhan

Tujuan utama ialah untuk menghindar, mengesan, melengah dan bertindakbalas terhadap sebarang perlanggaran Polisi Keselamatan Siber KEJORA.

g. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objekif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketersediaan. Pemulihan boleh dilakukan melalui sandaran dan peraturan pemulihan atau suatu Pelan Pemulihan Bencana dan Pelan Kesinambungan Perkhidmatan.

h. Saling Bergantung

Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip di atas. Setiap prinsip adalah saling lengkap melengkapi antara satu dengan lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisme keselamatan, dapat menjamin keselamatan yang maksimum.

1.6 PELANGGARAN DAN TINDAKAN DISPLIN

1.6.1 Pelanggaran

Sebarang pelanggaran PKS perlulah dilaporkan pada ICT Security Officer (ICTSO). Insiden perlulah disiasat oleh ICTSO dengan kerjasama penyelia kakitangan terbabit dan pihak berkuasa yang berkaitan.

1.6.2 Tindakan Disiplin

Pelanggaran polisi secara sengaja akan menyebabkan:

a. Kehilangan hak capaian ke atas sumber maklumat;
b. Penilaian prestasi kerja yang buruk;
c. Dikenakan tindakan tatatertib;
d. Digantung kerja atau ditamatkan perkhidmatan;
e. Ditamatkan kontrak;
f. Dikenakan tindakan undang-undang.

1.7 TEKNOLOGI

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

1.7.1 Peringkat Pemprosesan Data

a. Data-dalam-simpanan

i. KEJORA 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. Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII perlu dilindungi daripada segi kerahsiaan dan integriti data. Data Terbuka perlu dilindungi daripada segi integriti data.

b. Data-dalam-pergerakan

i. KEJORA 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.

c. Data-dalam-penggunaan

i. KEJORA 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.

ii. Teknologi untuk memastikan asal data dan data/transaksi tanpa sangkal boleh digunakan oleh KEJORA.

d. Perlindungan Ketirisan Data

i. Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.

ii. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

1.7.2 Elemen Dalam Persekitaran Pengkomputeran

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

b. Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam elemen persekitaran pengkomputeran yang disahkan oleh CGSO.

1.8 RISIKO

KEJORA hendaklah melaksanakan risiko berkaitan dengan aset yang telah dikenal pasti. Risiko yang dikenal pasti adalah kebarangkalian KEJORA tidak dapat menjayakan pelaksanaan fungsinya. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam Aset ICT KEJORA.

Pengurusan risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran.

Pengolahan risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

1.8.1 Kerentanan

a. Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
b. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

1.8.2 Ancaman

a. KEJORA hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

1.8.3 Impak

a. KEJORA hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi KEJORA.

1.8.4 Tahap Risiko

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

1.8.5 Penguraian Risiko

a. Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya.
b. Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

i. Teknologi

Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, tembok api digunakan untuk mengehadkan capaian logikal kepada sistem tertentu.

ii. Proses

Perekayasaan Proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

iii. Manusia

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

1.8.6 Pengurusan Risiko

a. Penyedia perkhidmatan digital di KEJORA 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; dan
   vi. memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

1.9 PELAN PENGURUSAN KESELAMATAN MAKLUMAT

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

Pelan ini hendaklah dibangunkan dengan berpandukan RAKKSSA, Polisi Keselamatan Siber KEJORA dan 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 senibina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

i. Peranti Pengkomputeran Peribadi

a. Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem.
b. Contoh peranti pengkomputeran peribadi adalah komputer riba, stesen kerja, telefon pintar, tablet, dan peranti storan.
c. Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada Bahagian Teknologi Maklumat KEJORA. Walau bagaimanapun, peranti pengkomputeran peribadi milik pensendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

ii. Peranti Rangkaian

a. Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti suis, penghala, tembok api, peranti *Virtual Private Network* (VPN) dan kabel.
b. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

iii. Aplikasi

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

b. 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.

iv. Pelayan

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

b. 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.

v. Persekitaran Fizikal

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

b. KEJORA hendaklah merujuk kepada Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

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

d. 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.

2.0 SEMAKAN DAN PENYELENGGARAAN DOKUMEN

ICT Security Officer (ICTSO) merupakan pemilik dokumen PKS ini. ICTSO bertanggungjawab untuk menyemak dan menyelenggarakan polisi ini.

BAHAGIAN 2: POLISI

2.0 BIDANG A.5 POLISI KESELAMATAN MAKLUMAT
INFORMATION SECURITY POLICY

A.5.1 Hala Tuju Pengurusan Untuk Keselamatan Maklumat ***Management Directions for Information Security***	
Objektif	Menyediakan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan organisasi serta perundangan dan peraturan yang berkaitan.

A.5.1.1 Polisi Keselamatan Maklumat
Policies for Information Security

Polisi untuk keselamatan maklumat perlu dibuat dan diluluskan oleh pihak pengurusan, disebarkan dan dimaklumkan kepada pengguna dan pihak luar yang berkenaan.

Penguatkuasaan polisi ini dijalankan oleh Pengurus Besar KEJORA dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Pengurus Bahagian/Ketua Unit.

Polisi ini perlu disebarkan kepada semua kakitangan dan menjadi tanggungjawab kakitangan untuk membaca dan memahami isi kandungan polisi ini. Polisi Keselamatan Siber KEJORA mestilah dipatuhi oleh semua Kakitangan KEJORA dan pengguna luar.

Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan KEJORA kepada kakitangan KEJORA dan Pengguna Luar.

A.5.1.2 Kajian Semula Polisi untuk Keselamatan Maklumat
Review of Policies for Information Security

PKS adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial untuk memastikan kesesuaian, kemampuan dan keberkesanan PKS. Ianya perlu disemak secara berkala sekurang-kurangnya sekali dalam masa setahun.

Berikut adalah proses kerja untuk semakan semula PKS.

a. Mengenalpasti dan menentukan perubahan yang diperlukan;
b. Mengemukakan cadangan pindaan melalui proses kerja yang sah kepada ICTSO untuk tindakan dan pertimbangan JPICT;
c. JPICT akan mempertimbangkan dan seterusnya mengesahkan sebarang pindaan yang telah dicadangkan;
d. Membuat penyebaran bagi pindaan yang telah disahkan dalam mesyuarat JPICT kepada kakitangan dan pihak luar yang berkenaan.

PKS adalah terpakai kepada semua pengguna ICT KEJORA dan tiada pengecualian diberikan.

3.0 BIDANG A.6 PERANCANGAN BAGI KESELAMATAN ORGANISASI ORGANIZATION OF INFORMATION SECURITY

A.6.1 Perancangan Dalaman ***Internal Organization***	
Objektif	Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber KEJORA.
A.6.1.1 Peranan dan Tanggungjawab Keselamatan Maklumat ***The Role and Responsibility of Information Security***	
Pengurus Besar	
Peranan dan tanggungjawab adalah seperti berikut: a. Memastikan penguatkuasaan pelaksanaan Polisi ini; b. Memastikan Kakitangan dan pengguna luar memahami dan mematuhi peruntukan - peruntukan di bawah Polisi ini; c. Memastikan semua keperluan KEJORA seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi; d. Memastikan pengurusan risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Polisi ini; dan e. Melantik CIO dan ICTSO	
Ketua Pegawai Maklumat (CIO)	
Peranan dan tanggungjawab Ketua Pegawai Maklumat adalah seperti berikut: a. Membantu Pengurus Besar dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT organisasi; b. Menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; c. Menentukan tindakan tatatertib yang perlu diambil ke atas pengguna yang telah dikenalpasti melanggar PKS;	

d. Memastikan kawalan keselamatan maklumat dalam KEJORA diseragam dan diselaraskan dengan sebaiknya; dan
e. Memastikan Pelan Strategik ICT KEJORA mengandungi aspek keselamatan ICT;

Pengurus Bahagian/Ketua Unit

Peranan dan tanggungjawab Pengurus Bahagian/Ketua Unit adalah melaksanakan keperluan Polisi ini dalam operasi semasa seperti berikut:

a. Pelaksanaan sistem atau aplikasi baru sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru;
b. Pembelian atau peningkatan perisian dan sistem komputer;
c. Perolehan teknologi dan perkhidmatan komunikasi baru;
d. Menentukan pembekal dan rakan usahasama menjalani tapisan keselamatan; dan
e. Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat kerajaan yang berkuatkuasa;

Pegawai Keselamatan ICT (ICTSO)

Pegawai Keselamatan ICT (ICTSO) adalah merupakan Pengurus Teknologi Maklumat. Peranan dan tanggungjawab beliau adalah seperti berikut:

a. Mengurus keseluruhan program-program keselamatan ICT organisasi;
b. Menguatkuasakan PKS organisasi;
c. Memberi penerangan dan pendedahan berkenaan PKS KEJORA kepada semua pengguna;
d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS;
e. Menjalankan pengurusan risiko;
f. Mengkaji semula dan merumus tindakbalas pengurusan berdasarkan hasil penemuan audit dan menyediakan laporan berkaitan dengannya;

g. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti perisian hasad dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
h. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT(GCERT), KPLB dan memaklumkannya kepada CIO;
i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baikpulih dengan segera;
j. Menyiasat dan mengenalpasti pengguna yang melanggar PKS organisasi; dan
k. Menyediakan dan melaksanakan program-program kesedaran mengenai keselamatan ICT.

Pentadbir Sistem ICT

Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:

a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam perkhidmatan tugas;
b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan Ketua Pegawai Maklumat (CIO) sebagaimana yang telah ditetapkan di dalam PKS;
c. Memantau aktiviti capaian harian pengguna;
d. Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data yang berlaku tanpa kebenaran dan membatalkan atau memberhentikan aktiviti tersebut dengan serta merta;
e. Menyimpan dan menganalisis rekod jejak audit; dan
f. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala;
g. Membaca, memahami dan mematuhi PKS;
h. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan;

i. Menentukan kawalan akses semua pengguna terhadap aset ICT;
j. Melaporkan penemuan mengenai pelanggaran PKS kepada ICTSO; dan
k. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT.

Pasukan Tindak Balas Insiden Keselamatan ICT (CERT) KEJORA

Peranan dan tanggungjawab pasukan CERT KEJORA adalah seperti berikut:

a. Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden;
b. Merekod dan menjalankan siasatan awal insiden yang diterima;
c. Menangani tindak balas insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;
d. Menasihati KEJORA mengambil tindakan pemulihan dan pengukuhan; dan
e. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada KEJORA.

Pengguna ICT

Pengguna ICT merupakan semua pegawai dan kakitangan organisasi. Peranan dan tanggungjawab pengguna adalah seperti berikut:

a. Membaca, memahami dan mematuhi PKS organisasi;
b. Mengetahui dan memahami implikasi keselamatan ICT;
c. lulus tapisan keselamatan;
d. Melaksanakan prinsip-prinsip PKS dan menjaga kerahsiaan maklumat;
e. Melaksanakan langkah-langkah perlindungan seperti berikut :-
    1. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
    2. Meriksa maklumat dan menentukan ianya 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; dan
7. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

f. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO atau Pegawai Teknologi Maklumat dengan segera;
g. Menghadiri program kesedaran mengenai keselamatan ICT;
h. Bertanggungjawab ke atas aset-aset ICT di bawah jagaannya; dan
i. Menandatangani surat akuan pematuhan PKS.

Peranan dan Tanggungjawab Pengguna Terhadap Polisi Keselamatan Siber

Peranan dan tanggungjawab pengguna terhadap PKS mestilah lengkap dan jelas dan hendaklah direkod, dipatuhi, dilaksanakan dan dinyatakan di dalam fail meja atau kontrak perkhidmatan.

Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.

Tapisan keselamatan untuk setiap pengguna, pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu dilaksanakan selaras dengan keperluan perkhidmatan.

A.6.1.2 Pengasingan Tugas
Segregation of Duties

Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubahsuai tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;
b. Tanggungjawab untuk tugasan mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlulah diasingkan. Ini bertujuan untuk mengelakkan daripada capaian yang tidak dibenarkan dan juga melindungi aset ICT daripada berlakunya kesilapan, ketirisan maklumat terperingkat atau disalahgunakan.

A.6.1.3 Hubungan Dengan Pihak Berkuasa
Contact with Authorities

Hubungan yang baik dengan pihak berkuasa yang berkaitan perlu dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Hendaklah mengenalpasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab KEJORA; dan
b. Mewujud dan mengemaskini prosedur/senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan adalah Polis Diraja Malaysia dan Suruhanjaya Komunikasi dan Multimedia. Pihak yang dihubungi semasa kecemasan adalah termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan dan bomba;

A.6.1.4 Hubungan Dengan Kumpulan Berkepentingan Yang Khusus
Contact with Special Interest Groups

Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan professional hendaklah dikekalkan.

Menganggotai pertubuhan profesional ataupun forum bagi:

a. Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat;

b. Menerima amaran awal dan nasihat berhubung kerentenan dan ancaman keselamatan maklumat terkini;
c. Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentenan; dan
d. Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.

A.6.1.5 Keselamatan Maklumat dalam Pengurusan Projek
Information Security in Project Management

Keselamatan maklumat perlu ditangani dalam pengurusan projek. Menjadi tanggungjawab Pengurus Projek untuk memastikan ciri-ciri keselamatan Maklumat dimasukan proses pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek KEJORA;

a. Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;
b. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenalpasti kawalan-kawalan yang diperlukan;
c. Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber KEJORA; dan
d. Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat.

A.6.2 Peranti mudah alih dan telekerja ***Mobile devices and teleworking***	
Objektif	Memastikan keselamatan maklumat apabila menggunakan peralatan mudah alih dan maklumat yang dicapai, diproses dan disimpan di lokasi luar.

A.6.2.1 Polisi Peranti Mudah Alih
Mobile Device Policy

Penggunaan aset peranti mudah alih yang bukan kepunyaan KEJORA perlu mendapat kebenaran dari pihak pengurusan.

Langkah-langkah keselamatan mengikut keperluan keselamatan semasa perlu dipatuhi untuk memastikan potensi risiko yang mungkin diperkenalkan disebabkan oleh penggunaan peranti mudah alih.

Perkara-perkara yang perlu dipatuhi:

a. Pendaftaran ke atas peralatan mudah alih;
b. Keperluan ke atas perlindungan secara fizikal;
c. Kawalan ke atas pemasangan perisian peralatan mudah alih;
d. Kawalan ke atas *versi* dan *patches* perisian;
e. Sekatan ke atas akses perkhidmatan maklumat secara atas talian;
f. Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi; dan
g. Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.

A.6.2.2 Telekerja
Teleworking

Polisi dan langkah-langkah keselamatan sokongan perlu dilaksanakan untuk melindungi maklumat yang dicapai, diproses atau disimpan di lokasi luar.

Kawalan perlindungan dan keselamatan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.

Perkara-perkara yang perlu dipatuhi:

a. Sebarang capaian ke dalam rangkaian KEJORA daripada luar hanya dibenarkan kepada pegawai-pegawai KEJORA yang perlu menggunakan sistem-sistem dalaman bagi melaksanakan tugas hakiki dan perlu mendapat kelulusan ICT Security Officer (ICTSO);
b. Memastikan tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran telekerja adalah sesuai dan selamat;
c. Tidak digalakkan untuk mengakses rangkaian KEJORA melalui 'Public Wifi' di lokasi seperti Kafe/Restoran bagi mengelakkan tumpuan dan ketirisan maklumat;
d. Memastikan kakitangan sentiasa boleh dihubungi dalam tempoh waktu bekerja;
e. Memastikan antivirus digunakan dan dikemaskini untuk peralatan mudah alih dan alatan komunikasi; dan
f. Menggunakan aplikasi sidang maya yang disediakan oleh pihak BTM, KEJORA

4.0 BIDANG A.7 KESELAMATAN SUMBER MANUSIA
HUMAN RESOURCE SECURITY

A.7.1 Sebelum Perkhidmatan ***Prior to Employment***	
Objektif	Memastikan bahawa pekerja dan kontraktor memahami tanggungjawab mereka dan mereka sesuai dengan peranan yang sedang dipertimbangkan.
A.7.1.1 Tapisan Keselamatan ***Security Screening***	
Ujian pengesahan latarbelakang ke atas semua calon yang berjaya untuk berkhidmat dengan KEJORA (kakitangan, kontraktor dan pihak luar/ketiga) perlulah dijalankan mengikut perundangan, peraturan dan nilai-nilai serta hendaklah selaras dengan keperluan perniagaan dan klasifikasi maklumat yang hendak didedahkan dan risiko yang bakal dihadapi.	
A.7.1.2 Terma dan Syarat Perkhidmatan ***Terms and Conditions of Employment***	
Perjanjian kontrak perkhidmatan dengan kakitangan dan pembekal perlulah dinyatakan serta tanggungjawab kakitangan dan organisasi pembekal hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan mengikut PKS dan peraturan semasa yang berkuatkuasa.	

A.7.2 Dalam Tempoh Perkhidmatan ***During Deployment***	
Objektif	Memastikan semua kakitangan, kontraktor dan pihak luar sedar dan memenuhi tanggungjawab keselamatan maklumat.

A.7.2.1 Tanggungjawab Pengurusan
Management Responsibilities

Pihak pengurusan perlu memastikan setiap pengguna ICT, pembekal, perunding dan pihak-pihak lain yang berkepentingan memberikan perkhidmatan dan menguruskan keselamatan aset ICT berdasarkan perundangan dan peraturan di dalam polisi, prosedur dan panduan yang telah ditetapkan oleh organisasi.

A.7.2.2 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat
Information Security Awareness, Education and Training

Kakitangan KEJORA dan Pengguna Luar perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber KEJORA, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka;
b. Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber (PKS) KEJORA perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan
c. Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.

1.7.1 A.7.2.3 Proses Tatatertib
Disciplinary Process

Proses tatatertib yang formal dan disampaikan kepada kakitangan KEJORA hendaklah tersedia bagi membolehkan tindakan diambil terhadap kakitangan KEJORA yang melakukan pelanggaran keselamatan maklumat.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Memastikan adanya proses tindakan disiplin dan /atau undang-undang ke atas kakitangan KEJORA sekiranya berlaku perlanggaran dengan perundangan dan peraturan yang ditetapkan oleh KEJORA;
b. Kakitangan KEJORA yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT KEJORA.

A.7.3 Penamatan dan Pertukaran Perkhidmatan ***Termination and Change of Employment***	
Objektif	Melindungi kepentingan KEJORA dari segi proses penamatan dan perubahan perkhidmatan dalam memastikan kakitangan, kontraktor dan pihak ketiga yang ditamatkan dari organisasi dan ditukarkan perkhidmatan diurus dengan teratur.

A.7.3.1 Penamatan atau Pertukaran Tanggungjawab Perkhidmatan
Termination or Change of Employment Responsibilities

Tanggungjawab dan tugas keselamatan maklumat yang masih sah selepas penamatan atau pertukaran penjawatan hendaklah ditakrifkan, disampaikan kepada kakitangan dan kontraktor, dan dikuatkuasakan.

Antara perkara-perkara yang perlu diambil adalah seperti berikut:

a. Memastikan semua aset ICT dikembalikan kepada KEJORA mengikut peraturan dan terma perkhidmatan yang ditetapkan;
b. Membatalkan atau menarik balik semua kebenaran capaian ke atas capaian maklumat; dan
c. Mengisi borang keselamatan maklumat selepas penamatan perkhidmatan.

Kakitangan KEJORA yang telah bertukar tanggungjawab perkhidmatan hendaklah:

a. Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada KEJORA mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan
b. Menyedia dan menyerahkan nota serah tugas dan Myportfolio kepada penyelia yang berkaitan.

5.0 BIDANG A.8 PENGURUSAN ASET
ASET MANAGEMENT

A.8.1 Tanggungjawab Terhadap Aset ***Responsibility for Assets***	
Objektif	Mengenalpasti aset ICT KEJORA dan mengariskan tanggungjawab perlindungan yang bersesuaian kepada aset tersebut.

A.8.1.1 Inventori Aset
Inventory of Assets

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT KEJORA. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut:

a) Pihak KEJORA hendaklah mengenalpasti Pegawai Penerima Aset setiap Bahagian untuk mengurus penerimaan aset-aset ICT bagi projek-projek ICT;
b) Memastikan semua aset ICT dikenal pasti, dikelasifikasi, didokumen, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemaskini sebagaimana arahan dan peraturan yang berkuatkuasa dari semasa ke semasa;
c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan
d) Pegawai Aset hendaklah mengesahkan penempatan aset ICT.

A.8.1.2 Pemilikan Aset ***Ownership of Assets***
Aset yang diselanggara hendaklah menjadi hak milik KEJORA. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut: a) Memastikan aset dibawah tanggungjawabnya telah dimasukkan dalam senarai aset; b) Memastikan aset telah dikelaskan dan dilindungi; c) Kenalpasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan; d) Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan e) Memastikan semua jenis aset dipelihara dengan baik.
A.8.1.3 Penggunaan Aset yang Dibenarkan ***Acceptable Use of Assets***
Peraturan untuk penggunaan aset mengikut kaedah atau polisi penggunaan yang dibenarkan dan aset yang berhubungkait dengan maklumat dan kemudahan memproses maklumat perlu dikenalpasti, direkodkan dan dilaksanakan.
A.8.1.4 Pemulangan Aset ***Return of Assests***
Semua pekerja dan pengguna pihak luar perlu memulangkan semua aset KEJORA yang ada di dalam milik mereka semasa penamatan perkhidmatan, kontrak atau perjanjian.

A.8.2 Pengelasan Maklumat ***Information Classification***	
Objektif	Memastikan maklumat yang diterima diberi perlindungan yang bersesuaian selaras dengan kepentingan maklumat berkenaan kepada KEJORA.
A.8.2.1 Pengelasan Maklumat ***Classification of Information***	
Maklumat perlu dikelaskan dari segi keperluan perundangan, nilai, kepentingan dan kepekaan terhadap pendedahan atau pengubahsuaian maklumat yang tidak mendapat kebenaran.	
A.8.2.2 Pelabelan Maklumat ***Labelling of Information***	
Maklumat perlu dilabelkan sewajarnya mengikut skim klasifikasi maklumat yang digunapakai oleh KEJORA.	
A.8.2.3 Pengendalian Aset ***Handling of Assets***	
Aset perlu dikendalikan sewajarnya mengikut skim klasifikasi maklumat yang digunapakai oleh KEJORA. Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan;	

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

f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

A.8.3 Pengendalian Media ***Media Handling***	
Objektif	Menghalang sebarang pendedahan, pengubahsuaian, pengalihan atau pemusnahan maklumat yang telah disimpan di dalam media.
A.8.3.1 Pengurusan Media Boleh Alih ***Management of Removal Media***	
Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengelasan yang diguna pakai oleh KEJORA. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan e) Menyimpan semua jenis media di tempat yang selamat.	
A.8.3.2 Pelupusan Media ***Disposal of Media***	
a) Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan. b) Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuatkuasa.	

1.7.2 A.8.3.3 Pemindahan Media Fizikal ***Physical Media Transfer***
c) Media yang mengandungi maklumat perlu dilindungi supaya tidak di perolehi oleh orang yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa proses pemindahan atau pengangkutan.

6.0 BIDANG A.9 KAWALAN AKSES
ACCESS CONTROL

A.9.1 Kawalan Akses ***Business Requirements of Access Control***	
Objektif	Menghadkan capaian kepada maklumat dan kemudahan memproses maklumat.
A.9.1.1 Polisi Kawalan Akses ***Access Control Policy***	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong polisi kawalan capaian pengguna sedia ada.	
A.9.1.2 Capaian kepada Rangkaian dan Perkhidmatan Rangkaian ***Access to Networks and Network Services***	
Pengguna hendaklah diberi akses kepada rangkaian dan perkhidmatan rangkaian yang telah dibenarkan secara khusus kepada mereka untuk digunakan.	

A.9.2 Pengurusan Akses Pengguna ***User Access Management***	
Objektif	Memastikan akses pengguna yang dibenarkan dan menghalang capaian yang tidak dibenarkan kepada sistem dan perkhidmatan.
A.9.2.1 Pendaftaran dan Pembatalan Pengguna ***User Registration and De-Registration***	
Proses pendaftaran dan pembatalan perlu dilaksanakan berdasarkan kepada tugas pemberian dan pengambilan semula capaian ke atas segala sistem dan perkhidmatan ICT mengikut keperluan semasa KEJORA.	
A.9.2.2 Peruntukan Akses Pengguna ***User Access Provisioning***	
Proses peruntukan formal akses pengguna perlu dilaksanakan untuk memberi atau mambatalkan hak akses untuk semua jenis pengguna untuk semua sistem dan perkhidmatan ICT organisasi.	
A.9.2.3 Pengurusan Hak Akses Istimewa ***Management of Privileged Access Rights***	
Pemberian dan penggunaan hak keistimewaan perlu dihadkan dan dikawal.	
A.9.2.4 Pengurusan Maklumat Pengesahan Rahsia Pengguna ***Management of Secret Authentication Information of Users***	
Pemberian maklumat rahsia pengguna yang telah disahkan perlu dikawal melalui proses pengurusan yang rasmi dan merujuk kepada Polisi Katalaluan.	
A.9.2.5 Kajian Semula Hak Akses Pengguna ***Review of User Access Rights***	
Semakan kepada kebenaran capaian pengguna mesti dikaji secara berkala.	

A.9.2.6 Pembatalan atau Pelarasan Hak Akses ***Removal or Adjustment of Access Rights***
Hak akses untuk maklumat dan kemudahan pemprosesan maklumat bagi semua kakitangan dan pengguna pihak luar perlu disingkirkan selepas penamatan perkhidmatan, kontrak atau perjanjian atau diselaraskan jika ada perubahan.

A.9.3 Tanggungjawab pengguna ***User Responsibilities***	
Objektif	Memastikan pengguna bertanggungjawab untuk melindungi maklumat rahsia mereka yang telah disahkan.
A.9.3.1 Penggunaan Maklumat Pengesahan Rahsia ***Use of Secret Authentication Information***	
Pengguna perlu mematuhi peraturan KEJORA dari segi penggunaan pengesahan maklumat rahsia.	

A.9.4 Kawalan Akses Sistem dan Aplikasi ***System and Application Access Control***	
Objektif	Menghalang capaian tanpa kebenaran ke atas maklumat yang terkandung di dalam sistem dan aplikasi.
A.9.4.1 Sekatan Akses Maklumat ***Information Access Restriction***	
Capaian ke atas maklumat dan fungsi sistem aplikasi oleh pengguna perlu dihadkan mengikut Polisi Kawalan Capaian.	
A.9.4.2 Prosedur Log Masuk yang Selamat ***Secure Log-On Procedure***	
Akses kepada sistem dan aplikasi perlu dikawal oleh prosedur "*log-on*" yang selamat mengikut keperluan keselamatan yang sesuai.	
A.9.4.3 Sistem Pengurusan Kata Laluan ***Password Management System***	
Sistem pengurusan kata laluan perlu interaktif dan perlu memastikan kata laluan yang berkualiti. a. Panjang kata laluan mestilah sekurang kurangnya dua belas (12) aksara dengan gabungan antara huruf, aksara khas dan nombor (*alphanumerik*); dan b. Pengguna hendaklah menukar kata laluan sekurang-kurangnya enam (6) bulan sekali. c. Pengguna yang tidak pernah membuat capaian ke dalam aplikasi selama 90 hari akan dinyahaktifkan hak capaian mereka.	

A.9.4.4 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa ***Use of Privileged Utility Programs***
Penggunaan program utiliti yang berkemungkinan mampu untuk mengatasi kawalan sistem dan aplikasi perlu dihadkan dan dikawal ketat.
A.9.4.5 Kawalan Akses Kepada Kod Sumber Program ***Access Control to Program Source Code***
Capaian kepada Kod Sumber hendaklah dihadkan. Perkara yang perlu dipertimbangkan seperti berikut: a. Log audit perlu dikekalkan kepada semua akses kepada Kod Sumber; b. Penyelenggaraan dan penyalinan Kod Sumber hendaklah tertakluk kepada kawalan perubahan; dan c. Kod Sumber bagi semua aplikasi dan perisian hendaklah menjadi hakmilik KEJORA.

7.0 BIDANG A.10 KRIPTOGRAFI
CRYPTOGRAPHY

1.8 A.10.1 Kawalan Kriptografi ***Cryptography Controls***	
Objektif	Memastikan penggunaan kriptografi yang sesuai dan berkesan untuk melindungi kerahsiaan, kesahihan dan integriti maklumat.
1.8.1 A.10.1.1 Polisi Pengunaan Kawalan Kriptografi ***Policy on the use of cryptographic control***	
Penggunaan kawalan kriptograpi bagi melindungi maklumat perlu dilaksanakan bagi memastikan kerahsiaan, kesahihan dan integriti maklumat mengikut keperluan semasa KEJORA.	
1.8.2 A.10.1.2 Pengurusan Kunci Awam ***Public Key Management***	
Pengurusan kunci hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	

8.0 BIDANG A.11 KESELAMATAN FIZIKAL DAN PERSEKITARAN *PHYSICAL AND ENVIRONMENTAL SECURITY*

A.11.1 Kawasan Selamat ***Secure Areas***	
Objektif	Menghalang capaian fizikal tanpa kebenaran, kemusnahan dan ganggu gugat kepada maklumat dan kemudahan memproses maklumat KEJORA.
A.11.1.1 Perimeter Keselamatan Fizikal ***Physical Security Parameter***	
Perimeter keselamatan perlu dikenalpasti dan digunakan untuk melindungi kawasan-kawasan yang mengandungi maklumat dan kemudahan memproses maklumat yang sensitif atau kritikal.	
A.11.1.2 Kawalan Kemasukan Fizikal ***Physical Entry Controls***	
Kawasan terkawal perlu dilindungi dengan kawalan kemasukan yang sesuai untuk memastikan hanya kakitangan yang dibenarkan sahaja dibenarkan masuk.	
A.11.1.3 Keselamatan Pejabat, Bilik dan Kemudahan ***Securing Offices, Rooms and Facilities***	
Keselamatan fizikal untuk pejabat, bilik dan kemudahan perlu dilaksanakan mengikut keperluan KEJORA bagi memastikan maklumat dan kemudahan pemprosesan maklumat tidak dapat dicapai tanpa kebenaran yang disahkan dan juga bagi menghalang sebarang bentuk kemusnahan dan ganggu gugat yang boleh memberi ancaman kepada keselamatan.	

A.11.1.4 Perlindungan Daripada Ancaman Luar Dan Persekitaran ***Protecting Against External and Environmental Threats***
Perlindungan fizikal terhadap kejadian bencana alam, serangan berbahaya atau insiden seperti kebakaran, banjir, gempa bumi, letupan, rusuhan awam dan lain-lain bentuk bencana alam atau buatan manusia perlu dilaksanakan mengikut keperluan semasa.
A.11.1.5 Bekerja di Kawasan Selamat ***Working in Secure Area***
Kawasan larangan ialah kawasan yang dihadkan kemasukan untuk pihak tertentu sahaja. Semua pelawat perlu mendaftar di buku log pelawat sebelum masuk ke premis KEJORA.
A.11.1.6 Kawasan Penyerahan dan Pemunggahan ***Delivery and Loading Areas***
Semua akses seperti kawasan penghantaran dan pemunggahan dan kawasan lain di mana orang yang tidak dibenarkan boleh memasuki premis organisasi perlu dikawal dan diasingkan dari kemudahan memproses maklumat untuk menghalang akses yang tidak dibenarkan.

A.11.2 Peralatan ICT ***ICT Equipment***	
Objektif	Menghalang kehilangan, kerosakan, kecurian atau bertolak ansur ke atas aset yang menyebabkan gangguan kepada operasi KEJORA.

A.11.2.1 Penempatan dan Perlindungan Peralatan ICT
Equipment Sitting and Protection

Kelengkapan hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran, dan peluang kemasukan yang tidak dibenarkan.

Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:

a) Penggunaan katalaluan untuk akses ke sistem komputer adalah diwajibkan;
b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;
c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;
d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem;
e) Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemaskini di samping melakukan imbasan ke atas media storan yang digunakan;
f) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, kerosakan, diubahsuai tanpa kebenaran dan salah guna;
g) Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;

h) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Gen-Set);

i) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan.

j) Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;

k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;

l) Peralatan ICT yang hendak dibawa ke luar dari premis KEJORA, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan;

m) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden;

n) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa;

o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ianya ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

p) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaikpulih;

q) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau tulisan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa dalam keadaan baik;

r) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal;

s) Pengguna dilarang sama sekali mengubah ***password administrator*** yang telah ditetapkan oleh pihak ICT; dan

Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat dibawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan Jabatan sahaja.

A.11.2.2 Utiliti sokongan
Supporting Utilities

Peralatan yang kritikal perlu dilindungi dari kegagalan kuasa elektrik dan sebarang gangguan lain yang disebabkan oleh kegagalan utiliti sokongan.

A.11.2.3 Keselamatan Kabel
Cabling security

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:

a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;
c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan

Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.

A.11.2.4 Penyenggaraan Peralatan
Equipment Maintenance

Kelengkapan hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan.

Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.

Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

a) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;

b) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;

c) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;

d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan

Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

A.11.2.5 Peralatan Dibawa Keluar Premis
Removal of Assets

Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu.

Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

a) Peralatan ICT yang hendak dibawa keluar dari premis KEJORA untuk tujuan rasmi, perlulah mendapat kelulusan Pengurus Besar KEJORA atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan

b) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.

A.11.2.6 Keselamatan Peralatan di Luar Premis
Security of Equipment Off-Premises

Keselamatan aset di luar hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis KEJORA.

Peralatan yang dibawa keluar dari premis KEJORA adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut:

a) Peralatan perlu dilindungi dan dikawal sepanjang masa;
b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan

Keselamatan peralatan yang dibawa keluar adalah dibawah tanggungjawab pegawai yang berkenaan.

A.11.2.7 Pelupusan yang Selamat atau Penggunaan Semula Peralatan
Secure Disposal or Re-Use of Equipment

Semua peralatan bagi kelengkapan yang mengandungi media penyimpanan hendaklah disahkan bagi memastikan apa-apa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya 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 KEJORA dan ditempatkan di KEJORA.

Peralatan ICT yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuatkuasa.

Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KEJORA.

Langkah-langkah seperti berikut hendaklah diambil:

a) Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;

b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

c) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

d) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;

e) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:

   i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi.

   ii) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *CPU* seperti *RAM*, *Hardisk*, *Motherboard* dan sebagainya.

   iii) Menyimpan dan memindahkan perkakasan luaran komputer seperti *AVR*, *speake*r dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di jabatan.

   iv) Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan

   v) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan dibawah tanggungjawab KEJORA.

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

g) Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal;

h) Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan;

i) Maklumat lanjut berhubung pelupusan bolehlah merujuk kepada Pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuatkuasa;

j) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan

Pegawai asset bertanggungjawab merekod butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam sistem inventori Sistem Pengurusan Aset

A.11.2.8 Peralatan Pengguna Tanpa Kawalan
Unattended User Equipment

Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya.

Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut:

a) Tamatkan sesi aktif apabila selesai tugas;

b) *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan

Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.

A.11.2.9 Polisi Meja Kosong dan Skrin Kosong
Policy Clear Desk dan Clear Screen

Polisi meja kosong untuk kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan.

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

Clear Desk bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkah-langkah perlu diambil termasuklah seperti berikut:

a) Menggunakan kemudahan *password, screensaver* atau log keluar apabila meninggalkan komputer;
b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci;
c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat; dan
d) E-mel masuk dan keluar hendaklah dikawal.

Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.

9.0 BIDANG A.12 KESELAMATAN OPERASI
OPERATIONS SECURITY

A.12.1 Prosedur dan Tanggungjawab Operasi ***Operational Procedures and Responsibilities***	
Objektif	Memastikan operasi kemudahan pemprosesan maklumat betul dan selamat.

A.12.1.1 Prosedur Operasi yang Didokumenkan
Documented Operating Procedures

a. Semua prosedur keselamatan ICT yang diwujudkan, dikenalpasti dan masih digunapakai hendaklah didokumenkan, disimpan dan dikawal;
b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti;
c. Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan; dan
d. Semua kakitangan KEJORA hendaklah mematuhi prosedur yang telah ditetapkan.

A.12.1.2 Pengurusan Perubahan
Change Management

a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada Pengurus Bahagian Teknologi Maklumat terlebih dahulu;
b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh Pentadbir Sistem ICT atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;

c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

A.12.1.3 Pengurusan Kapasiti
Capacity Management

a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan
b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

A.12.1.4 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi
Separation of Development, Test and Operational Facilities

Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (*production*).
b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan

Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.

A.12.2 Perlindungan Daripada Perisian Hasad ***Protection from Malware***	
Objektif	Memastikan maklumat dan kemudahan memproses maklumat dilindungi daripada perisian hasad.

A.12.2.1 Kawalan Daripada Perisian Hasad
Controls Against Malware

Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada perisian hasad hendaklah dilaksanakan, digabungkan dengan kesedaran pengguna yang sewajarnya. Antaranya:

a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti *antivirus* dan mengikut prosedur penggunaan yang betul dan selamat;
b. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997;
c. Mengimbas semua perisian atau sistem dengan *antivirus* sebelum menggunakannya;
d. Mengemaskini *pattern* anti virus sekerap yang mungkin;
e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;
f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;
g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;
h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan
i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

A.12.3 Sandaran ***Backup***	
Objektif	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan disimpan di *off site*.

1.8.3 A.12.3.1 Sandaran Maklumat
Information Backup

a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;
b. Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan sandaran bergantung pada tahap kritikal maklumat;
c. Menguji sistem sandaran sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.
d. Menyimpan sekurang-kurangnya tiga (3) generasi sandaran; dan
e. Merekod dan menyimpan rekod sandaran di lokasi yang berlainan dan selamat

A.12.4 Pengelogan dan Pemantauan ***Logging and monitoring***	
Objektif	Merekod aktiviti dan mewujudkan bukti.

A.12.4.1 Pengelogan Kejadian
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 adalah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan.

Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data.

Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti berikut:

a) Fail log sistem pengoperasian;
b) Fail log servis (contoh: web, e-mel);
c) Fail log aplikasi (*audit trail*); dan
d) Fail log rangkaian (contoh: *switch, firewall*, IPS).

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:

a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;

b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan

Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada pasukan CERT KEJORA.

A.12.4.2 Perlindungan Maklumat Log
Protection of Log Information

Kemudahan dan maklumat pengrekodan log perlu dilindungi terhadap pengubahsuaian dan sebarang capaian yang tidak dibenarkan.

A.12.*4.3 Log pentadbir dan Pengendali*
Administrator and Operator Logs

Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap.

a) Memantau penggunaan kemudahan memproses maklumat secara berkala;

b) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa kesemasa dan menyediakan laporan jika perlu;

c) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;

d) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan

Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada pasukan CERT KEJORA.

A.12.4.4 Penyegerakan Jam ***Clock Synchronisation***
Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diselaraskan mengikut satu sumber rujukan masa.
A.12.5 Kawalan Perisian yang Beroperasi ***Control of Operational Software***

Objektif	Memastikan integriti sistem operasi.

A.12.5.1 Pemasangan Perisian Pada Sistem yang Beroperasi ***Installation of Software on Operational Systems***
Kawalan ini hendaklah dilaksanakan untuk memastikan pemasangan perisian sewaktu sistem sedang beroperasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti berikut: a) Strategi "*rollback*" perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; b) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperakui berjaya; dan Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.

A.12.6 Pengurusan Kerentanan Teknikal ***Technical Vulnerability Management***	
Objektif	Menghalang eksploitasi dari sebarang kelemahan teknikal.

A.12.6.1 Pengurusan Kerentanan Teknikal
Management of Technical Vulnerabilities

Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem aplikasi dan operasi yang digunakan.

Perkara yang perlu dipatuhi adalah seperti berikut:

a) Melaksanakan ujian penembusan untuk memperolehi maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;
b) Menganalisis tahap risiko kerentanan; dan
c) Mengambil tindakan pengolahan dan kawalan risiko.

A.12.6.2 Sekatan ke atas Pemasangan Perisian
Restriction on Software Installation

Pemasangan perisian oleh pengguna perlu dikawal dan disemak secara berkala bagi memastikan tiada sebarang bentuk ancaman atau gangguan ke atas sistem yang beroperasi.

A.12.7 Pertimbangan Tentang Audit Sistem Maklumat ***Information systems audit considerations***	
Objektif	Mengurangkan implikasi aktiviti audit ke atas sistem yang beroperasi.
A.12.7.1 Kawalan Audit Sistem Maklumat ***Information Systems Audit Controls***	
Keperluan dan aktiviti audit yang memerlukan pengesahan sistem yang beroperasi perlulah dirancang sebaik mungkin dan dipersetujui untuk mengurangkan gangguan kepada proses-proses lain yang sedang beroperasi di dalam organisasi.	

10.0 BIDANG A.13 KESELAMATAN KOMUNIKASI
COMMUNICATIONS SECURITY

A.13.1 Pengurusan Keselamatan Rangkaian ***Network Security Management***	
Objektif	Memastikan perlindungan kepada maklumat dalam rangkaian dankemudahan pemprosesan maklumat sokongan yang lain.
A.13.1.1 Kawalan Rangkaian ***Network Control***	
Rangkaian perlu diurus dan dikawal untuk memastikan maklumat di dalam sistem dan aplikasi dilindungi daripada sebarang ancaman.	
A.13.1.2 Keselamatan Perkhidmatan Rangkaian ***Security of Network Services***	
Ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi keseluruhan perkhidmatan rangkaian perlu dikenalpasti dan dimasukkan ke	

dalam perjanjian perkhidmatan rangkaian sama ada rangkaian itu disediakan sendiri oleh atau pihak luar ("*outsource*").
A.13.1.3 Pengasingan Dalam Rangkaian ***Segregation in Networks***
a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; dan b. Rangkaian untuk pengguna, sistem perkhidmatan dan sistem maklumat juga perlu diasingkan.
A.13.2 Pemindahan Data dan Maklumat ***Information Transfer***

Objektif	Memastikan keselamatan maklumat yang dipindahkan di dalam organisasi dan yang melibatkan entiti luar.

A.13.2.1 Polisi dan Prosedur Pemindahan Data dan Maklumat ***Information Transfer Policies and Procedures***
a. Polisi, prosedur dan kawalan pertukaran maklumat dilaksanakan mengikut keperluan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; dan b. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KEJORA.
A.13.2.2 Perjanjian Mengenai Pemindahan Data dan Maklumat ***Agreements on Information Transfer***
KEJORA perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara KEJORA dengan pihak luar.

Perkara yang perlu dipertimbangkan adalah:

a) Pengurus Bahagian hendaklah mengawal penghantaran dan penerimaan maklumat KEJORA;

b) Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat KEJORA;

c) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan

KEJORA hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.

A.13.2.3 Pesanan Elektronik
Electronic Messaging

Maklumat yang terkandung di dalam pesanan elektronik perlu dilindungi. Penggunaan pesanan elektronik hanya boleh digunakan untuk aktiviti kerja harian di mana penggunaan untuk kepentingan peribadi hendaklah dilarang untuk mengelakkan daripada sebarang bentuk gangguan dan ancaman kepada keselamatan maklumat.

A.13.2.4 Perjanjian Kerahsiaan Atau Ketakdedahan
Confidentiality or Non-Disclosure Agreements

Keperluan bagi perjanjian kerahsiaan atau ketidaktirisan maklumat yang mencerminkan keperluan organisasi untuk melindungi maklumat perlu dikenalpasti, dikaji secara berkala dan didokumenkan.

11.0 BIDANG A.14 PEMEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM

SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

A.14.1 Keperluan Keselamatan Sistem Maklumat ***Security Requirements of Information Systems***	
Objektif	Memastikan keselamatan maklumat adalah sebahagian daripada sistem maklumat yang menyeluruh yang mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

A.14.1.1 Analisis dan Spesifikasi Keperluan Keselamatan Maklumat
Information Security Requirements Analysis and Specifications

Keperluan berkaitan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada.

Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut:

a) Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk pengkonsepan perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan pelupusan;

b) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Polisi Keselamatan Siber KEJORA;

c) Penyediaan rekabentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan

d) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data.

A.14.1.2 Melindungi Perkhidmatan Aplikasi dalam Rangkaian Awam
Securing Application Services on Public Networks

Kawalan keselamatan aplikasi di rangkaian awam perlu dikawal dan disemak secara berkala untuk memastikan kawalan keselamatan yang sesuai dapat diolah dan diterapkan ke dalam aplikasi bagi menghalang sebarang bentuk kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat daripada berlaku kepada aplikasi.

Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut:-

a. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin kesahihan dan ketepatan;
b. Menggabungkan semakan pengesahan ke dalam aplikasi untuk mengenal pasti sebarang kerosakan maklumat sama ada disebabkan oleh ralat pemprosesan atau tindakan yang disengajakan;
c. Mengenal pasti dan melaksanakan kawalan untuk mengesah dan melindungi integriti mesej dalam sistem aplikasi; dan
d. Melaksanakan proses pengesahan ke atas output data bagi menjamin kesahihan dan ketepatan pemprosesan sistem aplikasi.

A.14.1.3 Melindungi Transaksi Perkhidmatan Aplikasi
Protecting Application Services Transactions

Maklumat yang terlibat dalam urus niaga perkhidmatan permohonan hendaklah dilindungi untuk mencegah penghantaran yang tidak lengkap, salah penghantaran dan pendedahan, pengubahan mesej dan duplikasi mesej yang tidak dibenarkan atau berulang.

A.14.2 Keselamatan Dalam Proses Pembangunan dan Sokongan ***Security in Development and Support Services***	
Objektif	Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.
A.14.2.1 Polisi Pembangunan Selamat ***Secure Development Policy***	
Pembangunan perisian dan sistem serta sebarang pembangunan yang melibatkan proses sokongan maklumat dan aplikasi perlu dilaksanakan mengikut keperluan dan ianya hendaklah dikaji dan disemak secara berkala untuk memastikan keberkesanannya.	
A.14.2.2 Prosedur Kawalan Perubahan Sistem ***System Change Control Procedures***	
a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum ianya digunapakai; dan b. Menghalang sebarang peluang untuk membocorkan maklumat.	
A.14.2.3 Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi ***Technical Review of Applications after Operating Platform Changes***	
Apabila pengoperasian sistem ditukar, aplikasi yang kritikal mesti disemak dan diuji untuk memastikan tiada kesan sampingan terhadap keselamatan dan operasi KEJORA secara khususnya dan organisasisecara amnya berlaku.	
A.14.2.4 Sekatan Ke atas Perubahan Dalam Pakej Perisian ***Restrictions on Changes to Software Packages***	
Mengawal perubahan dan pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja.	

A.14.2.5 Prinsip Kejuruteraan Sistem Yang Selamat
Secure System Engineering Principles

Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat.

Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari masa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada **Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V)** sektor awam yang terkini.

A.14.2.6 Persekitaran Pembangunan Selamat
Secure Development Environment

KEJORA hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.

Persekitaran pembangunan sistem hendaklah selamat bagi melindungi keseluruhan kitaran hayat pembangunan sistem.

KEJORA perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira:

a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem;
b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran;
c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem;
d) Kawalan pemindahan data dari atau kepada persekitaran pembangunan sistem;
e) Pegawai yang bekerja di dalam persekitaran pembangunan sistem adalah yang boleh dipercayai; dan

Kawalan ke atas capaian kepada persekitaran pembangunan sistem.

A.14.2.7 Pembangunan oleh Khidmat Luaran
Outsourced Software Development

KEJORA hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar.

Kod sumber (*Source code*) adalah menjadi **HAK MILIK** KEJORA.

Perkara yang perlu dipatuhi adalah seperti berikut:

a) Perkiraan perlesenan, kod sumber adalah **HAK MILIK** KEJORA dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource;*
b) Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori "**Pembekal hendaklah membenar Kerajaan hak mencapai kod sumber dan melaksanakan pentaksiran risiko**";
c) Keperluan kontrak untuk rekabentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik;
d) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem;
e) Menggunapakai prinsip dan tatacara ***escrow;*** dan

Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.

A.14.2.8 Pengujian Keselamatan Sistem ***System Security Testing***
Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan.
A.14.2.9 Pengujian Penerimaan Sistem ***System Accepting Testing***
Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu.

A.14.3 Data Ujian ***Test Data***	
Objektif	Untuk memastikan perlindungan data yang digunakan untuk ujian.
A.14.3.1 Perlindungan Data Ujian ***Protection of Test Data***	
Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Sekiranya data ujian yang digunakan dipilih dari data sebenar yang sah perkara-perkara berikut perlu dipatuhi: a) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; b) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; c) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan Mengaktifkan audit log bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.	

12.0 BIDANG A.15 HUBUNGAN PEMBEKAL

SUPPLIER RELATIONSHIP

A.15.1 Keselamatan Maklumat Dalam Hubungan Pembekal ***Information Security in Supplier Relationships***	
Objektif	Memastikan perkhidmatan yang diberi mempunyai tahap keselamatan ICT yang bersesuaian selari dengan kontrak perjanjian.

A.15.1.1 Polisi Keselamatan Maklumat Untuk Hubungan Pembekal
Information Security Policy for Supplier Relationships

Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset KEJORA.

Perkara yang perlu dipertimbangkan adalah seperti berikut:

a) Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori;
b) Proses kitaran hayat (*lifecycle*) yang seragam untuk menguruskan pembekal;
c) Mengawal dan memantau akses pembekal;
d) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian;
e) Jenis-jenis obligasi kepada pembekal;
f) Pelan kontigensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat;
g) Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber KEJORA kepada pembekal;

Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa.

A.15.1.2 Menangani Keselamatan Dalam Perjanjian Pembekal ***Addressing Security within Supplier Agreements***
Semua keperluan keselamatan maklumat yang berkaitan hendaklah diwujudkan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur IT untuk maklumat KEJORA.
A.15.1.3 Rantaian Bekalan Teknologi Maklumat dan Komunikasi ***Information and Communication Technology Supply Chain***
Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk menangani risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk.

A.15.2 Pengurusan Penyampaian Perkhidmatan Pembekal ***Supplier Service Delivery Management***	
Objektif	Memastikan perkhidmatan yang diberi mempunyai tahap keselamatan ICT yang bersesuaian selari dengan kontrak perjanjian.
A.15.2.1 Memantau Dan Mengkaji Semula Perkhidmatan Pembekal ***Monitoring and Review Supplier Services***	
KEJORA hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan	

A.15.2 Pengurusan Penyampaian Perkhidmatan Pembekal ***Supplier Service Delivery Management***	
Objektif	Memastikan perkhidmatan yang diberi mempunyai tahap keselamatan ICT yang bersesuaian selari dengan kontrak perjanjian.
Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	
A.15.2.2 Menguruskan Perubahan Kepada Perkhidmatan Pembekal ***Managing Changes to Supplier Services***	
Sebarang perubahan skop perkhidmatan yang berikan oleh pihak ketiga perlu diurus mengikut keperluan semasa. Ia termasuklah bekalan, perubahan terhadap perkhidmatan sedia ada dan pertambahan perkhidmatan baru. Penilaian risiko perlu dilakukan berdasarkan tahap kritikal sesebuah sistem dan impak yang ada terhadap perubahan ini.	

13.0 BIDANG A.16 PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

INFORMATION SECURITY INCIDENT MANAGEMENT

A.16.1 Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan ***Management of Information Security Incidents and Improvements***	
Objektif	Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.
A.16.1.1 Tanggungjawab dan Prosedur ***Responsibilities and Procedures***	
Prosedur pelaporan insiden keselamatan ICT perlu dilaksanakan berdasarkan Prosedur Pengurusan Insiden Keselamatan ICT.	
A.16.1.2 Pelaporan Kejadian Keselamatan Maklumat ***Reporting Information Security Events***	
Sebarang kejadian yang melibatkan keselamatan maklumat perlu dilaporkan kepada ICTSO dengan segera mengikut prosedur yang telah digariskan.	
A.16.1.3 Pelaporan Kelemahan Keselamatan Maklumat ***Reporting Security Weaknesses***	
Pelaporan juga perlu dilakukan sekiranya terdapat kelemahan keselamatan didalam sistem atau perkhidmatan.	
A.16.1.4 Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat ***Assessment of and Decision on Information Security Events***	
Kejadian keselamatan maklumat perlu dinilai dan diklasifikasikan sebagai insiden keselamatan maklumat.	

A.16.1.5 Tindak Balas Terhadap Insiden Keselamatan Maklumat ***Response to Information Security Incidents***
Insiden keselamatan maklumat perlu diberi tindakbalas mengikut prosedur yang didokumenkan.
A.16.1.6 Pembelajaran Daripada Insiden Keselamatan Maklumat ***Learning from Information Security Incidents***
Mekanisma yang bersesuaian perlu dilaksanakan untuk membolehkan jenis, jumlah, kos insiden keselamatan ICT dapat dikaji, disemak dan dipantau secara berkala.
A.16.1.7 Pengumpulan Bahan Bukti ***Collection of Evidence***
Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah direkod, disimpan dan dikemaskini. Kawalan-kawalan yang perlu diambilkira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a) Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti; b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; dan d) Menyediakan tindakan pemulihan segera; dan Memaklumkan atau mendapatkannasihat pihak berkuasa perundangan sekiranya perlu.

14.0 BIDANG A.17 ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

A.17.1 Kesinambungan Keselamatan Maklumat ***Information Security Continuity***	
Objektif	Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.
A.17.1.1 Perancangan Kesinambungan Keselamatan Maklumat ***Planning Information Security Continuity***	
Pelan kesinambungan perkhidmatan hendaklah dilaksanakan mengikut keperluan semasa bagi menentukan suatu pendekatan yang menyeluruh dapat diambil bagi mengekalkan kesinambungan perkhidmatan. Ini juga bertujuan untuk memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan KEJORA dan menjamin keselamatan maklumat ICT KEJORA.	
A.17.1.2 Pelaksanaan Kesinambungan Keselamatan Maklumat ***Implementing Information Security Continuity***	
Tindakan dan langkah susulan yang sesuai hendaklah diambil dan direkodkan untuk memastikan pelan kesinambungan yang telah dipersetujui dapat dilaksanakan bersesuaian dengan keperluan semasa KEJORA.	
A.17.1.3 Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat ***Verify, Review and Evaluate Information Security Continuity***	
Pengesahan kawalan kesinambungan keselamatan maklumat perlu dilaksanakan secara berkala untuk memastikan bahawa ianya adalah sah dan berkesan semasa keadaan tidak diingini berlaku.	

A.17.2 Memastikan Ketersediaan ***Redundancy***	
Objektif	Memastikan ketersediaan kemudahan pemprosesan maklumat.
A.17.2.1 Ketersediaan Kemudahan Pemprosesan Maklumat ***Availability of Information Process Facilities***	
Kemudahan pemprosesan maklumat perlu dilaksanakan dengan redundansi yang mencukupi untuk memenuhi keperluan ketersediaan.	

15.0 BIDANG A.18 PEMATUHAN

COMPLIANCE

A.18.1 Pematuhan Terhadap Keperluan Perundangan dan Kontrak ***Compliance with Legal and Contractual Requirements***	
Objektif	Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Polisi Keselamatan Siber KEJORA.

A.18.1.1 Pengenalpastian Keperluan Undang-Undang dan Kontrak Yang Terpakai
Identification of Applicable Legislation and Contractual Agreement

Setiap pengguna KEJORA hendaklah membaca dan memahami PKS KEJORA dan perlu mengambil langkah-langkah yang sesuai demi untuk memastikan PKS dipatuhi dari semasa ke semasa.

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua kakitangan KEJORA dan pembekal:

i. Akta KEJORA 2017
ii. Enakmen Negeri 1975
iii. Arahan Keselamatan;
iv. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi”;
v. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (*MyMIS)*;
vi. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
vii. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi”;
viii. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

ix.	Surat Pekeliling Am Bil. 4 Tahun 2006 – "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam";
x.	Surat Pekeliling Perbendaharaan Bil.2 / 1995 (Tambahan Pertama) - "Tatacara Penyediaan, Penilaian dan Penerimaan Tender"; 10. Surat Pekeliling Perbendaharaan Bil. 3 / 1995 - "Peraturan Perolehan Perkhidmatan Perundingan";
xi.	Akta Tandatangan Digital 1997;
xii.	Akta Rahsia Rasmi 1972;
xiii.	Akta Jenayah Komputer 1997;
xiv.	Akta Hak Cipta (Pindaan) Tahun 1997;
xv.	Akta Komunikasi dan Multimedia 1998;
xvi.	Perintah-Perintah Am;
xvii.	Arahan Perbendaharaan;
xviii.	Arahan Teknologi Maklumat 2007;
xix.	Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam";
xx.	Etika Penggunaan E-mel dan Internet Kakitangan Kerajaan;
xxi.	Dasar Kriptografi Negara 12 Julai 2013
xxii.	Akta Badan Berkanun (Tatatertib &Surcaj) 2000 (Akta 605)

A.18.1.2 Hak Harta Intelek
Intellectual Property Rights

Prosedur yang sesuai dilaksanakan untuk memastikan pematuhan keperluan perundangan, kawal selia dan kontrak yang berkaitan dengan hak harta intelektual dan penggunaan produk perisian hak milik.

A.18.1.3 Perlindungan Rekod ***Protection of Records***
Setiap rekod perlu dilindungi daripada kehilangan, kemusnahan, pemalsuan, akses dan pembebasan yang tidak dibenarkan, mengikut keperluan perundangan, peraturan, kontrak dan perkhidmatan.
A.18.1.4 Privasi dan perlindungan maklumat peribadi ***Privacy and Protection of Personally Identifiable Information***
Privasi dan perlindungan maklumat peribadi hendaklah dipastikan seperti yang dikehendaki dalam undang-undang dan peraturan yang relevan jika berkenaan.
A.18.1.5 Peraturan Kawalan Kriptografi ***Regulation of Cryptographic Controls***
Kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang dan peraturan yang relevan mengikut keperluan semasa.

A.18.2 Kajian Semula Keselamatan Maklumat ***Information Security Reviews***	
Objektif	Untuk memastikan bahawa keselamatan maklumat dilaksanakan dan dikendalikan mengikut polisi dan prosedur organisasi.
A.18.2.1 Kajian Semula Keselamatan Maklumat Secara Berkecuali ***Independent Review of Information Security***	
Pendekatan KEJORA untuk menguruskan keselamatan maklumat dan pelaksanaan hendaklah dikaji secara berkala atau apabila perubahan ketara berlaku pada sebarang maklumat ICT KEJORA dan ianya perlu dilakukan oleh pihak berkecuali atau pihak bebas.	

A.18.2.2 Pematuhan Polisi dan Standard Keselamatan ***Compliance with Security Policies and Standards***
Pengurus perlu meneliti pematuhan pemprosesan dan prosedur maklumat di dalam bidang tanggungjawab mereka dengan polisi keselamatan, piawaian dan sebarang keperluan keselamatan yang sesuai.
A.18.2.3 Kajian Semula Pematuhan Teknikal ***Technical Compliance Review***
Sistem ICT mestilah diperiksa secara berkala untuk memastikan ianya mematuhi standard keselamatan yang sedia ada. Sebarang pematuhan teknikal mestilah dijalankan oleh individu yang kompeten yang diberi kebenaran.