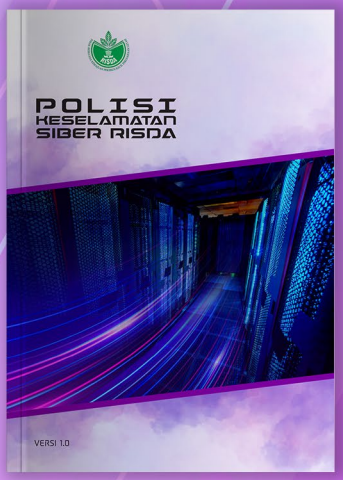
POLISI KESELAMATAN SIBER RISDA

VERSI 1.0

Polisi Keselamatan Siber RISDA

Versi 1.0



Bahagian Teknologi Maklumat RISDA

Tingkat 3 dan Tingkat 1,
Ibu Pejabat RISDA, Jalan Ampang, Kuala Lumpur
No. Telefon : 03-42529131
No. Faks : 03-42511855
Emel : btmr@risda.gov.my / btm@risda.gov.my

Rekabentuk:

Unit Multimedia dan Laman Web,
Bahagian Teknologi Maklumat.

Diterbitkan oleh:

Bangunan RISDA,
Km 7, Jalan Ampang,
Karung Berkunci 11067,
50990 Kuala Lumpur.
No. Telefon : 03-42564022
No. Faks : 03-42576726
Portal rasmi: www.risda.gov.my

Sekapur Sireh

Ketua Pengarah RISDA

Alhamdulillah di atas rahmat dan limpah kurnia daripada Allah SWT. Bersyukur kita ke hadratNya kerana diberikan hidayah untuk terus melaksanakan amanah, khususnya dalam mengemaskini dan menerbitkan Polisi Keselamatan Siber RISDA sebagai rujukan untuk seluruh warga RISDA dan Kumpulan RISDA Holdings (KRH).

Polisi ini mengandungi dasar yang perlu dipatuhi oleh semua warga RISDA dan KRH, terutamanya semasa mengendalikan aset-aset ICT. Setiap ketetapan yang digariskan dalam polisi ini menekankan aspek keselamatan maklumat untuk meningkatkan kesedaran, pembudayaan amalan terbaik dan kawalan keselamatan ICT untuk melindungi maklumat dari ancaman.

Polisi Keselamatan Siber RISDA yang menggantikan Dasar Keselamatan ICT RISDA (DKICT) ini telah diperkemas dengan mengambil kira prinsip-prinsip keselamatan maklumat bagi setiap domain keselamatan yang terkandung dalam standard Sistem Pengurusan Keselamatan Maklumat ISO/EIC 27001, garis panduan peraturan berkaitan keselamatan maklumat kerajaan yang berkuat kuasa serta perkembangan aplikasi ICT dan trend semasa ancaman siber.

Semoga kandungan polisi ini dapat diteliti, difahami dan dipatuhi dengan sebaiknya oleh seluruh warga RISDA dan KRH untuk memastikan keselamatan aset ICT di RISDA dan KRH terjamin dan tidak dikompromi.

Syabas diucapkan kepada Timbalan Ketua Pengarah (Pengurusan) selaku Ketua Pegawai Digital (CDO), Pengarah Bahagian Teknologi Maklumat dan semua pihak yang menjayakan usaha pengemaskinian dan penerbitan dokumen polisi ini.

Sekian, terima kasih.

Datuk Abdullah Bin Zainal

Kata Aluan

Timbalan Ketua Pengarah (Pengurusan)
Ketua Pegawai Digital (CDO) RISDA

Syukur ke hadrat Ilahi dan di atas segala limpah kurniaNya, Polisi Keselamatan Siber RISDA versi 1.0 berjaya diterbitkan sebagai rujukan untuk semua warga RISDA dan Kumpulan RISDA Holdings (KRH). Penerbitan dokumen ini bertepatan dengan situasi cabaran baharu ancaman keselamatan maklumat dan siber yang semakin kompleks dan pantas berubah.

Sejajar dengan arus pemodenan, transformasi digital dan perkembangan pesat dalam bidang ICT, perkhidmatan RISDA/KRH semakin bergantung kepada maklumat yang tepat, terkini dan berintegriti. Untuk mencapai objektif tersebut, pengukuhan keselamatan bagi keseluruhan infrastruktur ICT di RISDA dan KRH bukan sahaja bergantung kepada proses, aplikasi dan teknologi, tetapi juga diperkukuh dengan dasar serta polisi keselamatan siber yang jelas kepada setiap pengguna ICT.

Polisi Keselamatan Siber RISDA ini menggariskan 14 domain keselamatan maklumat utama yang melibatkan tanggungjawab semua pengguna dalam melindungi aset ICT. Dokumen ini perlu diteliti dan difahami bagi mengelakkan pelanggaran atau ketidakpatuhan yang boleh mengakibatkan ancaman keselamatan ICT di RISDA dan KRH seterusnya menjejaskan penyampaian perkhidmatan.

Saya penuh yakin dengan adanya Polisi Keselamatan Siber ini, ia akan meningkatkan kepercayaan pelanggan dalam berurusan dan mendapatkan perkhidmatan di RISDA dan KRH tanpa rasa ragu atau khuatir mengenai integriti, kerahsiaan, dan ketersediaan maklumat. Oleh itu, saya menyeru semua warga RISDA dan KRH untuk meneliti dan memahami kandungan polisi ini seterusnya mengaplikasikannya dalam tugas harian.

Tahniah dan terima kasih kepada semua yang terlibat dalam menjayakan penerbitan Polisi Keselamatan Siber RISDA ini.

Sekian, terima kasih.

Haniza Binti Ab Shukor

KANDUNGAN **MUKASURAT**

PENGENALAN

Polisi Keselamatan Siber RISDA mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Polisi ini menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT di RISDA dan Kumpulan RISDA Holdings (KRH).

OBJEKTIF

Polisi Keselamatan Siber RISDA diwujudkan untuk :-

a) Menghalang dan meminimumkan sebarang insiden keselamatan yang berlaku.
b) Memastikan kerahsiaan dokumen dan maklumat elektronik sentiasa terpelihara.
c) Memastikan kelancaran operasi serta meminimumkan kerosakan atau kemusnahan.
d) Memastikan kesinambungan perkhidmatan sekiranya berlaku sebarang insiden keselamatan yang tidak diingini.
e) Memastikan integriti dokumen dan maklumat elektronik supaya sentiasa tepat, lengkap, sahih dan kemas kini. Ia hanya boleh diubah dengan kaedah yang dibenarkan.
f) Memastikan punca dokumen dan maklumat adalah daripada sumber yang sah dan tanpa keraguan.
g) Meminimumkan kos penyenggaraan ICT akibat ancaman dan penyalahgunaan sumber.
h) Memastikan akses hanya kepada pengguna-pengguna yang sah.
i) Mencegah salah guna atau kecurian aset ICT kerajaan.
j) Memperkukuhkan pengurusan risiko.

PERNYATAAN DASAR

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

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT adalah berkait rapat dengan perlindungan aset ICT.

Terdapat empat komponen asas keselamatan ICT iaitu :-

a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah.
b) Menjamin setiap maklumat adalah tepat dan sempurna.
c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna.
d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Polisi Keselamatan Siber RISDA merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut :-

a) Kerahsiaan

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

b) Integriti

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

c) Tidak Boleh Disangkal

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

d) Kesahihan

Data dan maklumat hendaklah dijamin kesahihannya.

e) Ketersediaan

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

SKOP

Aset ICT terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Polisi Keselamatan Siber RISDA menetapkan keperluan-keperluan asas berikut :-

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

b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat. Bagi menentukan aset ICT ini terjamin keselamatannya sepanjang masa, Polisi Keselamatan Siber RISDA ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan keselamatan.

Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut :-

a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan seperti komputer, pelayan, peralatan komunikasi dan sebagainya.

b) Perisian Program

Prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada RISDA dan KRH.

c) Perkhidmatan

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

Contoh :

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

ci) Data atau Maklumat

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

cii) Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian bagi mencapai misi dan objektif organisasi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

ciii) Premis Komputer dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan setiap perkara di atas perlu diberikan perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Polisi Keselamatan Siber RISDA dan perlu dipatuhi adalah seperti berikut :-

a) Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan akses di bawah prinsip ini adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut :-

i. Klasifikasi maklumat seperti yang tercatat di dalam Arahan Keselamatan, di mana maklumat dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad.
ii. Tapisan keselamatan pengguna yang mematuhi prinsip bahawa pengguna boleh diberi kebenaran mengakses kategori maklumat tertentu setelah siasatan latar belakang menunjukkan tiada sebab atau faktor untuk menghalang pengguna daripada berbuat demikian.

b) Hak akses minimum

Hak akses kepada pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan diperlukan untuk membolehkan pegawai mewujud, menyimpan, mengemaskini, mengubah dan membatalkan sesuatu data atau maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan peranan dan tanggungjawab atau bidang kerja pengguna.

c) Akauntabiliti

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

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.
ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa.
iii. Menentukan maklumat sedia untuk digunakan.
iv. Menjaga kerahsiaan kata laluan.

v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.

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

vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

d) Pengasingan

Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. Secara minimum, semua sistem ICT memerlukan persekitaran operasi yang berasingan seperti berikut :-

i. Persekitaran pembangunan bagi aplikasi dalam proses pembangunan.

ii. Persekitaran penerimaan bagi pengujian aplikasi.

iii. Persekitaran sebenar bagi pengoperasian aplikasi.

e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenalpasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*.

f) Pematuhan

Polisi Keselamatan Siber RISDA hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penyalinan semula penduaan (*restore backup*) dan mewujudkan pelan pemulihan bencana ataupun pelan kesinambungan perkhidmatan.

h) Saling Bergantung

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

PENILAIAN RISIKO KESELAMATAN ICT

Pihak RISDA dan KRH hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan kelemahan (*vulnerability)* yang semakin meningkat ketika ini. Justeru itu, pengurusan RISDA dan KRH perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT. Pihak pengurusan hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat dalam organisasi termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik server, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain. Pengurusan RISDA bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005 : Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam atau lain-lain panduan yang bersesuaian. Pihak RISDA dan KRH perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut :-

a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian.
b) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan.
c) Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko.
d) Memindahkan risiko ke pihak lain seperti pembekal, perunding dan pihak-pihak lain yang berkepentingan.

BIDANG 01 PEMBANGUNAN DAN PENYENGGARAAN POLISI

0101 Polisi Keselamatan Siber

010101 Pelaksanaan Polisi

010102 Penyenggaraan Polisi

BIDANG 01 PEMBANGUNAN DAN PENYENGGARAAN POLISI	
0101 Polisi Keselamatan Siber	
Objektif : Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan RISDA dan perundangan yang berkaitan.	
010101 Pelaksanaan Polisi	
Dokumen ini adalah merupakan satu set polisi untuk keselamatan maklumat bagi RISDA yang perlu ditakrifkan, diluluskan, diterbitkan dan dikomunikasikan oleh pihak pengurusan RISDA kepada semua pengguna RISDA/KRH (termasuk staf, pembekal, perunding dan lain-lain). Ketua Pengarah RISDA selaku Pengerusi Jawatankuasa Pemandu ICT (JPICT) RISDA adalah bertanggungjawab terhadap pelaksanaan polisi ini dengan dibantu ahli-ahli JPICT RISDA yang terdiri daripada Timbalan Ketua Pengarah (Pengurusan) merangkap Ketua Pegawai Digital (CDO), Timbalan Ketua Pengarah (Pembangunan), Pengurus ICT, semua Pengarah Bahagian, Pegawai Undang-Undang, Pegawai Keselamatan ICT (ICTSO) dan wakil KRH.	Ketua Pengarah
010102 Penyenggaraan Polisi	
Polisi Keselamatan Siber RISDA ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Polisi Keselamatan Siber RISDA :- a) Kenalpasti dan tentukan perubahan yang diperlukan. b) Kemukakan cadangan pindaan secara bertulis kepada ICTSO untuk dibentangkan kepada Jawatankuasa Keselamatan ICT RISDA bagi mendapatkan kelulusan dalam Mesyuarat JPICT RISDA. c) Perubahan yang telah dipersetujui oleh JPICT RISDA perlu dimaklumkan kepada semua pengguna RISDA. d) Polisi ini hendaklah dikaji semula sekurang-kurangnya sekali dalam tempoh tiga tahun atau mengikut keperluan semasa.	ICTSO

BIDANG 02 ORGANISASI KESELAMATAN MAKLUMAT

0201 Organisasi Dalaman

020101 Ketua Pengarah RISDA

020102 Ketua Pegawai Digital (CDO)

020103 Pegawai Keselamatan ICT (ICTSO) RISDA

020104 Pengurus ICT, Pentadbir Sistem ICT, Pentadbir Sistem Aplikasi, Pentadbir Pangkalan Data, Pentadbir Portal, Pentadbir E-mel, Pentadbir Rangkaian dan Pusat Data, Pentadbir Media Sosial

020105 Pegawai Aset (ICT)

020106 Pengguna

020107 Jawatankuasa Pemandu ICT (JPICT) RISDA

020108 Jawatankuasa Teknikal ICT (JTI) RISDA

020109 Pasukan Tindak Balas Insiden Keselamatan Siber RISDA (CSIRT RISDA)

020110 Jawatankuasa Pelan Kesinambungan Perkhidmatan (PKP) RISDA

0202 Pihak Ketiga

020201 Keperluan Keselamatan Kontrak Dengan Pihak Ketiga

0203 Keselamatan Maklumat Dalam Pengurusan Projek

BIDANG 02 ORGANISASI KESELAMATAN MAKLUMAT	
0201 Organisasi Dalaman	
Objektif : Menerangkan peranan dan tanggungjawab semua pihak yang terlibat dengan lebih jelas dan teratur untuk mencapai objektif Polisi Keselamatan Siber RISDA.	
020101 Ketua Pengarah RISDA	
Peranan serta tanggungjawab Ketua Pengarah RISDA adalah seperti berikut :- a) Memastikan semua pegawai dan kakitangan RISDA memahami peruntukan-peruntukan keselamatan ICT RISDA. b) Memastikan semua pegawai dan kakitangan RISDA mematuhi dan akur tentang keselamatan ICT RISDA. c) Memastikan semua keperluan organisasi seperti sumber kewangan, sumber manusia (staf) dan keselamatan persekitaran pejabat adalah mencukupi. d) Memastikan penilaian dan kajian risiko dan program keselamatan ICT dilaksanakan mengikut ketetapan yang ditentukan dalam Polisi Keselamatan Siber RISDA. e) Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) RISDA.	Ketua Pengarah RISDA
020102 Ketua Pegawai Digital (CDO)	
Ketua Pegawai Digital (CDO) bagi RISDA ialah Timbalan Ketua Pengarah (Pengurusan). Peranan serta tanggungjawab CDO adalah seperti berikut :- a) Membantu Ketua Pengarah RISDA dalam melaksanakan bidang tugas berkaitan keselamatan ICT RISDA. b) Menentukan serta memastikan keselamatan ICT RISDA. c) Memastikan pelan strategik pendigitalan RISDA atau lain-lain dokumen yang seumpamanya mengandungi aspek keselamatan siber. d) Menyelaras dan menguruskan keperluan dan pelan latihan dan program kesedaran keselamatan ICT bagi keperluan Polisi Keselamatan Siber RISDA serta pengurusan risiko dan sistem pengauditannya.	CDO

e) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT RISDA. f) Menentukan penguatkuasaan Polisi Keselamatan Siber RISDA dijalankan seperti apa yang telah ditentukan.	
020103 Pegawai Keselamatan ICT (ICTSO) RISDA	
Pegawai Keselamatan ICT (ICTSO) RISDA dilantik daripada Pegawai Teknologi Maklumat gred F44 dan ke atas dari Bahagian Teknologi Maklumat, RISDA. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut :- a) Mengurus keseluruhan program-program keselamatan ICT RISDA. b) Menentukan penguatkuasaan pelaksanaan Polisi Keselamatan Siber RISDA diikuti dan dipatuhi oleh staf RISDA. c) Memberi penerangan dan pendedahan tentang Polisi Keselamatan Siber RISDA kepada semua pengguna. d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber RISDA. e) Melaksanakan pengurusan risiko ICT bagi RISDA. f) Menjalankan auditan, mengkaji semula, merumus tindak balas pengurusan RISDA berdasarkan hasil penemuan dan menyediakan laporan berkaitan mengenainya. g) Memberi amaran serta menyebarkan maklumat terhadap kemungkinan berlakunya ancaman berbahaya seperti virus serta memberi khidmat nasihat dan menyediakan langkah-langkah perlindungan yang bersesuaian. h) Melaporkan masalah atau insiden keselamatan siber kepada Agensi Keselamatan Siber Negara (NACSA) dan memaklumkan kepada CDO. i) Bekerjasama dengan semua pihak yang berkaitan ICT dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera. j) Melaporkan insiden keselamatan siber kepada CDO bagi insiden yang memerlukan pengaktifan Pelan Pengurusan Kesinambungan Perkhidmatan (PKP). k) Berperanan sebagai koordinator PKP RISDA. l) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	ICTSO

020104 Pengurus ICT, Pentadbir Sistem ICT, Pentadbir Sistem Aplikasi, Pentadbir Pangkalan Data, Pentadbir Portal, Pentadbir E-mel, Pentadbir Rangkaian dan Pusat Data, Pentadbir Media Sosial	
Pengurus ICT adalah Pengarah Bahagian Teknologi Maklumat (RISDA) dan Pengurus Besar Jabatan Teknologi Maklumat (KRH). Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut :- a) Memastikan pelaksanaan sistem baharu sama ada dengan pendekatan pembangunan secara dalaman atau luaran yang melibatkan teknologi baharu yang bersesuaian. b) Merancang pembelian dan peningkatan perisian dan sistem komputer. c) Merancang perolehan teknologi dan perkhidmatan komunikasi baharu. d) Mengkaji semula dan melaksanakan kawalan keselamatan ICT jabatan selaras dengan keperluan agensi pusat/kerajaan. e) Memastikan pelan strategik ICT atau dokumen yang seumpama mengandungi inisiatif berkaitan aspek keselamatan ICT. f) Memastikan aspek keselamatan maklumat dilaksanakan dalam setiap pengurusan projek. g) Mengesahkan garis panduan, prosedur dan tatacara bagi semua aplikasi yang dibangunkan agar mematuhi keperluan polisi keselamatan siber ini.	Pengurus ICT.
Pentadbir Sistem ICT RISDA/KRH. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah :- a) Mengambil tindakan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas. b) Menentukan kawalan akses pengguna terhadap aset ICT serta ketetapan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat. c) Memastikan setiap pengguna dikenali dengan menggunakan satu ID pengguna yang unik.	Pentadbir Sistem ICT (Pegawai ICT).

d) Melaporkan sebarang perkara atau penemuan mengenai sesuatu yang mencurigakan mengenai keselamatan ICT kepada ICTSO. Memantau aktiviti capaian harian sistem aplikasi pengguna. e) Menyimpan rekod, bahan bukti dan laporan terkini terhadap ancaman keselamatan ICT, disamping perlu mengenali aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dengan bertindak membatal atau memberhentikannya dengan serta-merta. f) Memastikan *virus pattern*, *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemaskini supaya terhindar daripada ancaman virus dan penggodam. g) Memastikan kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya; h) Membuat pemantauan dan penyenggaraan terhadap sistem dari semasa ke semasa. i) Menganalisis serta menyimpan rekod jejak audit. j) Menyediakan laporan mengenai aktiviti capaian secara berkala. k) Memastikan pembangunan sistem aplikasi mengambil kira dan mematuhi ciri-ciri keselamatan yang termaktub dalam Polisi Keselamatan Siber RISDA. **Pentadbir Sistem Aplikasi RISDA/KRH.** Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah :- a) Mengkaji cadangan penambahbaikan sistem atau modul sedia ada berdasarkan keperluan semasa. b) Bertanggungjawab dalam aspek pelaksanaan keseluruhan sistem dan modul. c) Memastikan kelancaran operasi sistem aplikasi agar perkhidmatan yang disediakan tidak terjejas. d) Memastikan setiap pengguna dikenali dengan menggunakan satu ID pengguna yang unik. e) Menyediakan dokumentasi sistem serta manual pangguna sistem.	Pentadbir Sistem Aplikasi (Pemilik Sistem).

f) Menghadkan capaian kepada semua dokumentasi berkaitan sistem aplikasi bagi mengelakkan dari penyalahgunaannya. g) Bertanggungjawab memantau setiap perkakasan yang melibatkan pengguna RISDA seperti komputer, komputer riba, pencetak, pengimbas dan sebagainya agar sentiasa berada dalam keadaan baik. h) Melaporkan sebarang insiden pelanggaran polisi keselamatan ke atas sistem aplikasi kepada ICTSO. i) Melibatkan diri dalam aktiviti penilaian tahap keselamatan ICT (*Security Posture Assessment*) serta penilaian risiko keselamatan maklumat.	
Pentadbir Pangkalan Data RISDA/KRH. Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah :- a) Melaksanakan instalasi dan penambahbaikan pangkalan data serta lain-lain peirisian yang berkaitan dengan pangkalan data. b) Memastikan pangkalan data boleh digunakan pada setiap masa. c) Melaksanakan pemantauan dan penyenggaraan yang berterusan ke atas pangkalan data. d) Melaksanakan *data masking* dalam menyediakan data latihan. e) Memastikan pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur. f) Melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip dalam Polisi Keselamatan Siber RISDA. g) Melaksanakan proses *housekeeping* di dalam pangkalan data. h) Melaporkan sebarang insiden pelanggaran polisi keselamatan pangkalan data kepada ICTSO.	Pentadbir Pangkalan Data.
Pentadbir Portal dan Laman Web RISDA/KRH. Peranan dan tanggungjawab Pentadbir Portal adalah :- a) Menerima kandungan laman web/portal yang telah disahkan kesahihan dan terkini daripada sumber yang sah.	Pentadbir Laman Web/Portal.

b) Memantau prestasi capaian dan menjalankan penalaan prestasi laman web/portal untuk memastikan akses lancar. c) Memastikan data-data sulit tidak boleh disalin atau dicetak oleh pihak yang tidak berhak. d) Memastikan rekabentuk laman web/portal dibangunkan dengan ciri-ciri keselamatan supaya tidak diceroboh. e) Mengasingkan kandungan dan aplikasi bagi capaian umum dan dalaman. f) Memastikan *housekeeping* keselamatan terhadap sistem pengoperasian, web server serta lain-lain perisian berkaitan. g) Melaporkan pelanggaran keselamatan laman web/portal kepada ICTSO.	
Pentadbir E-mel RISDA/KRH. Peranan dan tanggungjawab Pentadbir E-mel adalah :- a) Menentukan setiap akaun yang diwujudkan, dibekukan atau dibatalkan telah mendapat kelulusan. b) Mengesah dan memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan melalui saluran rasmi. c) Memastikan kemudahan membuat capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi. d) Memastikan pengguna e-mel RISDA/KRH berkemahiran menggunakan kemudahan e-mel yang disediakan. e) Memastikan polisi dan konfigurasi emel yang selamat dilaksanakan.	Pentadbir E-mel.
Pentadbir Rangkaian dan Pusat Data RISDA/KRH. Peranan dan tanggungjawab Pentadbir Rangkaian dan Pusat Data adalah :- a) Memastikan kerahsiaan akaun pentadbir. b) Merangka, melaksana dan menguatkuasakan polisi keselamatan ICT seperti perlindungan dan perkongsian data. c) Merancang dan melaksana polisi bagi pengukuhan keselamatan ICT. d) Merancang peningkatan dan keselamatan infrastruktur sedia ada. e) Memastikan keselamatan infrastruktur ICT sentiasa berada dalam ketersediaan yang tinggi untuk melindungi aset ICT.	Pentadbir Rangkaian dan Pusat Data.

f) Memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat. g) Memastikan keselamatan data dan sistem aplikasi yang berada dalam pusat data. h) Menjadual dan melaksanakan proses backup dan ujian *restore* ke atas pangkalan data dan sistem secara berkala. i) Melaksanakan Pelan Pemulihan Bencana berdasarkan prinsip dalam Pengurusan Kesinambungan Perkhidmatan. j) Melibatkan diri dalam sebarang aktiviti penilaian tahap keselamatan ICT (*Security Posture Assessment*) serta penilaian risiko keselamatan maklumat.	
Pentadbir Media Sosial RISDA/KRH. Peranan dan tanggungjawab Pentadbir Media Sosial adalah :- a) Mengambil maklum terhadap peraturan dan syarat-syarat yang digariskan oleh penyedia platform media sosial. b) Menggunakan platform media sosial bagi menyampaikan maklumat yang tepat, sahih dan terkini. c) Merangka strategi agar maklumat yang disampaikan boleh disebarkan secara teratur, berkesan dan meluas. d) Memberi maklum balas kepada pertanyaan dan keraguan yang ditinggalkan di platform media sosial dalam jangka masa yang bersesuaian. e) Menegur hantaran (*posting)* atau komen untuk memastikan perbincangan berada di landasan yang betul. f) Sentiasa membuat semakan posting atau komen. g) Mempertimbangkan untuk mengeluarkan atau menyekat pengguna yang membuat hantaran atau komen yang jelik. h) Berupaya menjalankan kajian untuk mengetahui pendapat dan maklum balas daripada pengikut media sosial.	Pentadbir Media Sosial RISDA/KRH.
020105 Pegawai Aset (ICT)	
Pegawai Aset (ICT) berperanan dan bertanggungjawab seperti berikut :-	Pegawai Aset RISDA/KRH.

a) Memastikan pengurusan aset ICT dijalankan selaras dengan peraturan yang ditetapkan; b) Memastikan penerimaan aset ICT dilaksanakan oleh pegawai yang dilantik oleh Ketua Jabatan; c) Memastikan semua aset ICT yang diterima, didaftarkan menggunakan sistem pengurusan aset dalam tempoh yang ditetapkan; d) Memastikan semua aset ICT yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan secara bertulis daripada Ketua Jabatan/ Pegawai Aset/ Pegawai-pegawai lain yang diberi kuasa oleh Ketua Jabatan; e) Memastikan daftar aset ICT dikemas kini apabila berlaku penambahan/ penggantian/ naik-taraf aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira; f) Memastikan semua aset ICT diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia atau nama organisasi/agensi di tempat yang mudah dilihat dan sesuai pada aset berkenaan; g) Memastikan semua aset ICT ditandakan dengan nombor siri pendaftaran mengikut susunan yang ditetapkan; h) Memastikan senarai daftar induk aset ICT disediakan; i) Memastikan senarai aset ICT disediakan dipaparkan mengikut lokasi; j) Memastikan setiap kerosakan aset ICT dilaporkan untuk tujuan penyelenggaraan; k) Bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT; l) Merancang, memantau dan memastikan pemeriksaan aset ICT dilaksanakan ke atas keseluruhan aset ICT sekurang-kurangnya sekali setahun; dan m) Memastikan setiap kes kehilangan aset ICT dilaporkan dan diuruskan dengan teratur.	
020106 Pengguna	
Pengguna berperanan dan bertanggungjawab seperti berikut :- a) Membaca dengan teliti, memahaminya dan seterusnya mematuhi Polisi Keselamatan Siber RISDA sepenuhnya.	Pengguna

b) Mengetahui dan memahami implikasi keselamatan ICT kesan dan tindakan-tindakannya. c) Melepasi tapisan keselamatan (jika berkaitan khususnya berurusan dengan maklumat rasmi terperingkat). d) Melaksanakan prinsip-prinsip Polisi Keselamatan Siber RISDA dan sentiasa akur menjaga kerahsiaan maklumat RISDA. e) Melaporkan sebarang aktiviti dan insiden yang mengancam keselamatan ICT RISDA kepada ICTSO dengan kadar segera. f) Perlu memberikan pengesahan Akuan Pematuhan Polisi Keselamatan Siber RISDA (manual atau secara atas talian). g) Menghadiri program-program kesedaran mengenai keselamatan ICT bagi tujuan meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai teknologi dan keselamatan maklumat.	
020107 Jawatankuasa Pemandu ICT (JPICT) RISDA	
Jawatankuasa Pemandu ICT ditubuhkan untuk meluluskan, menyelaras dan memantau projek-projek ICT di RISDA. Jawatankuasa ini juga adalah bertanggungjawab sebagai Jawatankuasa Keselamatan ICT RISDA yang berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan serta strategi keselamatan ICT RISDA. Keanggotaan jawatankuasa ini adalah ditetapkan seperti berikut :- Pengerusi : Ketua Pengarah. Ahli : 1. Timbalan Ketua Pengarah (Pengurusan). 2. Timbalan Ketua Pengarah (Pembangunan). 3. Semua Pengarah Bahagian. 4. Pegawai Undang-Undang. 5. ICTSO. 6. Wakil Kumpulan RISDA Holdings. Urus setia : Bahagian Teknologi Maklumat. Peranan dan tanggungjawab jawatankuasa ini adalah seperti berikut :- a) Menetapkan hala tuju dan strategi bagi pelaksanaan ICT RISDA. b) Merancang, menyelaras dan memantau pelaksanaan program/projek ICT RISDA.	Jawatankuasa Pemandu ICT RISDA

c) Meluluskan projek-projek ICT RISDA. d) Meluluskan Polisi Keselamatan Siber RISDA. e) Merancang dan menentukan langkah-langkah keselamatan ICT. f) Mengatasi sebarang isu yang gagal ditangani diperingkat Jawatankuasa Teknikal atau Pasukan Projek. g) Menetapkan keutamaan bagi pembangunan dan pelaksanaan projek-projek ICT di RISDA.	
020108 Jawatankuasa Teknikal ICT RISDA (JTI RISDA)	
Jawatankuasa Teknikal ICT akan menilai permohonan projek ICT yang dicadangkan oleh pengarah program dari aspek daya maju teknikal, pengoptimuman sumber dan keberkesanan kos bagi menyokong keperluan perkhidmatan teras RISDA. Jawatankuasa ini bertanggungjawab untuk memastikan projek ICT yang dilaksanakan mempunyai nilai tambah serta dapat memberi pulangan nilai untuk wang, impak dan keberkesanan yang tinggi kepada pelanggan sekaligus meningkatkan kecekapan penyampaian perkhidmatan RISDA. Keanggotaan jawatankuasa ini adalah ditetapkan seperti berikut :- Pengerusi : Timbalan Ketua Pengarah (Pengurusan). Ahli : 1. Pengarah Bahagian Teknologi Maklumat. 2. Timbalan Pengarah semua bahagian. 3. Semua Ketua Unit di Bahagian Teknologi Maklumat, RISDA. 4. Ahli-ahli jemputan. Urus setia : Bahagian Teknologi Maklumat. Peranan dan tanggungjawab jawatankuasa ini adalah seperti berikut :- a) Menerima, meneliti dan menilai semua permohonan bagi perolehan atau pembangunan sesuatu projek ICT baharu di RISDA; b) Melaksanakan mesyuarat JTI dari semasa ke semasa mengikut keperluan; c) Memberikan ulasan pengesyoran bagi perakuan aspek teknikal projek ICT kepada JPICT RISDA;	Jawatankuasa Teknikal ICT RISDA

d) Menyediakan laporan kepada JPICT RISDA atau Pihak Pengurusan RISDA mengikut keperluan.	
020109 Pasukan Tindak Balas Insiden Keselamatan Siber RISDA (CSIRT RISDA)	
Pasukan Tindak Balas Insiden Keselamatan Siber RISDA memiliki keanggotaan seperti yang berikut :- Pengerusi : Pengurus ICT. Urusetia : ICTSO. Ahli : 1. Pegawai Teknologi Maklumat. 2. Penolong Pegawai Teknologi Maklumat. Peranan dan tanggungjawab jawatankuasa ini adalah seperti berikut :- a) Menerima aduan keselamatan ICT, menilai tahap dan jenis insiden. b) Merekod dan menjalankan siasatan awal terhadap insiden yang diterima. c) Menangani tindak balas insiden keselamatan ICT dan mengambil tindakan baik pulih. d) Menghubungi dan melaporkan insiden yang berlaku kepada NACSA sama ada sebagai input atau untuk tindakan seterusnya. e) Merujuk Pusat Tanggungjawab yang berada di bawah kawalannya untuk mengambil tindakan pemulihan dan pengukuhan. f) Melaporkan sebarang maklumbalas dan insiden keselamatan ICT kepada Jawatankuasa Keselamatan ICT RISDA. g) Menasihati pengurusan RISDA dalam mengambil tindakan pemulihan dan pengukuhan keselamatan ICT. h) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT.	CSIRT RISDA
020110 Jawatankuasa Pelan Kesinambungan Perkhidmatan (PKP) RISDA	
Jawatankuasa Pelan Kesinambungan Perkhidmatan RISDA memiliki keanggotaan seperti yang berikut :- Pengerusi : Pengurus ICT. Urusetia : ICTSO.	

Ahli : 1. Pegawai Keselamatan Jabatan, Bahagian Pentadbiran. 2. Pegawai Tadbir Pejabat Ketua Pengarah. 3. Pegawai Tadbir Bahagian Pentadbiran. 4. Pegawai Tadbir Bahagian Komunikasi Korporat. 5. Pegawai Tadbir Bahagian Pengurusan Sumber Manusia. 6. Pegawai Tadbir Negeri, Pejabat RISDA Negeri Selangor. 7. Ketua Unit Pengurusan Aset, Bahagian Pentadbiran. 8. Ketua Unit Penyenggaraan Bangunan, Bahagian Khidmat Kejuruteraan. 9. Ketua Unit Penyelidikan dan Pembangunan Sistem, Bahagian Teknologi Maklumat. Peranan dan tanggungjawab Jawatankuasa PKP RISDA adalah seperti yang berikut :- a) Menyediakan skop dan terma rujukan program PKP. b) Memastikan program PKP dilaksanakan. c) Menilai keberkesanan pelaksanaan program PKP. d) Memantau pelaksanaan program PKP.	Jawatankuasa PKP RISDA.
0202 Pihak Ketiga	
Objektif : Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Perunding dan lain-lain pihak luar).	
020201 Keperluan Keselamatan Kontrak Dengan Pihak Ketiga	
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut :- a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber RISDA. b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian. c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga. d) Akses kepada aset ICT RISDA/KRH perlu berlandaskan kepada perjanjian kontrak.	CDO, Pengurus ICT, ICTSO, Pentadbir Sistem ICT dan pembekal.

e) Memastikan semua syarat keselamatan maklumat dinyatakan dengan jelas dalam/bersama perjanjian dengan pihak ketiga dan perkara-perkara berikut perlu dilengkapkan serta dipatuhi :- i. Akuan Pematuhan Polisi Keselamatan Siber RISDA (**Lampiran 1**). ii. *Non-Disclosure Agreement* (**Lampiran 2**). iii. Perakuan Akta Rahsia Rasmi 1972 (**Lampiran 3**). iv. Tapisan Keselamatan (sekiranya melibatkan capaian kepada data rasmi terperingkat dan sensitif). v. Hak harta intelek.	
0203 Keselamatan Maklumat Dalam Pengurusan Projek	
Setiap pengurusan projek (tanpa mengira jenis projek) yang dilaksanakan di RISDA dan KRH perlu mengambilkira aspek keselamatan maklumat secara holistik. Pengurus ICT/ICTSO adalah bertanggungjawab untuk :- a) Menjadikan objektif keselamatan maklumat sebahagian daripada objektif projek. b) Melaksanakan penilaian risiko keselamatan maklumat di fasa awal projek sebelum kawalan keselamatan yang berkaitan dikenal pasti. c) Menjadikan isu keselamatan maklumat sebagai agenda dalam setiap fasa kaedah pelaksanaan projek. d) Memastikan pengurusan projek mematuhi peraturan dan panduan seperti yang dinyatakan dalam polisi ini bagi setiap peringkat aktiviti projek. e) Memastikan pengurus projek telah mendapat latihan kesedaran dan pendedahan yang mencukupi berkenaan tanggungjawab untuk memastikan keselamatan maklumat sentiasa terjamin. f) Memastikan aktiviti bagi menjamin keselamatan maklumat dinyatakan secara jelas dalam jadual perancangan pelaksanaan projek. g) Sekiranya terdapat keperluan, seorang pegawai boleh dilantik untuk berperanan dalam memantau aspek keselamatan ICT sehingga tempoh serahan projek. h) Memastikan semua pihak yang terlibat dalam sesuatu projek maklum tentang arahan berkaitan keselamatan maklumat dan mereka diikat dengan perjanjian.	Pengurus ICT dan ICTSO.

BIDANG 03 KESELAMATAN SUMBER MANUSIA

0301 Sebelum Perkhidmatan

030101 Penilaian dan Tapisan

030102 Terma dan Syarat Pelantikan

0302 Dalam Perkhidmatan

030201 Tanggungjawab Pengurusan

030202 Kesedaran, Pendidikan dan Latihan Keselamatan Maklumat

030203 Tindakan Disiplin

0303 Bertukar, Tamat Perkhidmatan atau Cuti Belajar

030301 Tanggungjawab Penamatan dan Penukaran Lantikan

BIDANG 03 **KESELAMATAN SUMBER MANUSIA**	
0301 Sebelum Perkhidmatan	
Objektif : Memastikan kakitangan RISDA, KRH, pihak ketiga dan lain-lain pihak luar yang berkepentingan memahami tanggungjawab serta peranan masing-masing dalam keselamatan aset ICT.	
030101 Penilaian dan Tapisan	
Tapisan keselamatan yang bersesuaian untuk calon kakitangan RISDA, KRH, pihak ketiga dan lain-lain pihak yang berkepentingan perlu dilaksanakan berasaskan keperluan perundangan, peraturan dan etika yang terpakai selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Pengguna dan Pengurusan Sumber Manusia.
030102 Terma dan Syarat Pelantikan	
Terma dan syarat perkhidmatan dengan kakitangan dan kontraktor yang dilantik perlu menjelaskan tanggungjawab mereka dan tanggungjawab organisasi berkaitan dengan keselamatan maklumat yang sedang berkuat kuasa.	Pengguna dan Pengurusan Sumber Manusia.
0302 Dalam Perkhidmatan	
Objektif : Memastikan kakitangan RISDA, KRH, pihak ketiga dan lain-lain pihak yang berkepentingan menyedari dan memenuhi keperluan tanggungjawab keselamatan maklumat mereka.	
030201 Tanggungjawab Pengurusan	
Pihak pengurusan perlu memastikan semua kakitangan RISDA, KRH dan pihak ketiga yang berkepentingan :- a) Menguruskan keselamatan maklumat berdasarkan perundangan dan peraturan yang berkuat kuasa. b) Mempunyai tahap kesedaran, pengetahuan dan kemahiran mengenai keselamatan maklumat pada tahap yang baik. c) Disediakan dengan saluran pelaporan pelanggaran polisi dan prosedur berkaitan dengan keselamatan maklumat.	Pengguna dan Pengurusan Sumber Manusia.

d) Memastikan adanya proses tindakan disiplin atau undang-undang ke atas pegawai dan kakitangan RISDA, KRH serta pihak ketiga yang berkepentingan sekiranya berlaku pelanggaran perundangan dan peraturan yang ditetapkan.	
030202 Kesedaran, Pendidikan dan Latihan Keselamatan Maklumat	
Semua kakitangan RISDA, KRH dan pihak ketiga yang berkepentingan perlu :- a) Mengikuti latihan serta program kesedaran yang berkaitan dengan pengurusan keselamatan ICT dan sekiranya perlu kepada pihak ketiga dari semasa ke semasa. b) Memantapkan pengetahuan berkaitan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	Pengguna dan Pengurusan Sumber Manusia.
030203 Tindakan Disiplin	
Proses tindakan disiplin dan undang-undang yang formal perlu ada dan dimaklumkan kepada kakitangan RISDA, KRH dan pihak ketiga yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan ditetapkan. Kakitangan yang melanggar polisi ini akan digantung daripada mendapat capaian kepada kemudahan ICT RISDA/KRH.	Pengguna dan Pengurusan Sumber Manusia.
0303 Bertukar, Tamat Perkhidmatan atau Cuti Belajar	
Objektif : Bagi melindungi kepentingan organisasi dalam proses pertukaran atau penamatan perkhidmatan.	
030301 Tanggungjawab Penamatan dan Penukaran Lantikan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Memastikan semua aset ICT RISDA/KRH dikembalikan kepada jabatan mengikut peraturan dan terma perkhidmatan yang ditetapkan. b) Menyalurkan maklumat pembatalan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh RISDA/KRH dan terma perkhidmatan kepada Pentadbir Sistem ICT. c) Sebarang keperluan untuk perlanjutan terhadap capaian haruslah dibuat permohonan rasmi kepada Pengurus ICT. d) Pegawai perlu menyedia dan menyerahkan nota serah tugas kepada penyelia yang berkaitan. e) Pegawai dan kakitangan menandatangani perakuan Akta Rahsia Rasmi 1972 apabila meninggalkan perkhidmatan kerajaan.	Pengguna dan Pengurusan Sumber Manusia.

BIDANG 04	**PENGURUSAN ASET**
0401	**Akauntabiliti dan Tanggungjawab Terhadap Aset**
040101	Aset ICT
040102	Pegawai Bertanggungjawab
040103	Penggunaan Aset ICT
040104	Pemulangan Aset ICT
0402	**Klasifikasi Maklumat**
040201	Kategori dan Pengelasan Maklumat
040202	Pelabelan Maklumat
040203	Pengendalian Maklumat
0403	**Pengendalian Media**
040301	Pengurusan Media Mudah Alih (*Removal Media*)
040302	Pemindahan Media Fizikal
040303	Pelupusan Media
040304	Sanitasi Media

BIDANG 04
PENGURUSAN ASET

0401 Akauntabiliti dan Tanggungjawab Terhadap Aset

Objektif : Untuk mengenal pasti aset bagi memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT.

040101 Aset ICT

Ketua Jabatan adalah bertanggungjawab untuk memastikan aset ICT diberi kawalan dan perlindungan oleh pemilik atau pemegang amanah meliputi penerimaan, pendaftaran, penggunaan, penyimpanan dan pemeriksaan, penyelenggaraan, pelupusan, kehilangan dan hapus kira. Pengurusan aset ICT dilaksanakan secara cekap, teratur dan berkesan mengikut peraturan yang telah ditetapkan dengan melaksanakan perkara-perkara berikut :- a) Semua aset ICT diuruskan mengikut tatacara pengurusan aset yang berkuatkuasa. b) Setiap aset hendaklah didaftarkan dan ditentukan pemiliknya. Ketua Jabatan adalah bertanggungjawab untuk mengenalpasti pemilik bagi aset ICT. c) Memastikan aset ICT disimpan di tempat yang yang sesuai dan selamat mengikut Arahan Keselamatan dan garis panduan yang berkuat kuasa. d) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja. e) Pegawai Aset hendaklah mengesahkan penempatan aset ICT. f) Semua pengguna aset ICT mestilah mematuhi keperluan kawalan yang telah ditetapkan oleh pemilik aset atau pentadbir sistem.	Pegawai Aset dan pengguna.

040102 Pegawai Bertanggungjawab

Setiap pengguna aset ICT perlu mematuhi perkara-perkara berikut :- a) Memastikan semua aset ICT di bawah tanggungjawabnya telah dimasukkan dalam senarai aset. b) Menyemak dan memastikan semua aset ICT di bawah kawalannya berfungsi dengan sempurna. c) Bertanggungjawab sepenuhnya ke atas aset ICT dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan.	Pegawai Aset dan pengguna.

d) Bertanggungjawab di atas kerosakan atau kehilangan aset ICT di bawah kawalannya. e) Melindungi aset ICT daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran. f) Melaporkan kerosakan aset ICT kepada Pentadbir ICT untuk dibaik pulih. g) Memastikan semua aset ICT dalam keadaan '*OFF*' apabila meninggalkan pejabat. h) Melaporkan penyelewengan atau salah guna aset ICT kepada ICTSO. i) Melaporkan dengan menguruskan kehilangan aset ICT mengikut tatacara kehilangan aset alih.	
040103 Penggunaan Aset ICT	
Penggunaan aset ICT hendaklah mematuhi peraturan berikut :- a) Semua aset ICT digunakan bagi tujuan rasmi sahaja. b) Mengikut fungsi sebenar yang terdapat dalam manual/buku panduan pengguna. c) Dikendalikan oleh pegawai yang mahir dan berkelayakan jika perlu. d) Kerosakan hendaklah dilaporkan menggunakan borang yang ditetapkan. e) Daftar aset ICT dikemaskini apabila berlaku perubahan penempatan, perubahan pegawai penempatan, penambahan, penggantian, naik taraf, pemeriksaan, pelupusan, pindahan dan hapus kira. f) Memastikan semua pengguna mengesahkan penempatan aset ICT tersebut disimpan mengikut ruang penempatan yang diklasifisikan sama ada ruang pejabat atau bilik sepertimana ditentukan oleh tatacara pengurusan aset jabatan. g) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumenkan dan dilaksanakan dengan sebaik-baiknya. h) Kehilangan aset ICT atas sebab kecuaian pengguna akan dikenakan surcaj selaras dengan peraturan semasa. i) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT dan aksesori yang berkaitan di bawah kawalannya.	Pegawai Aset dan pengguna.
040104 Pemulangan Aset ICT	
a) Pegawai bertanggungjawab ke atas aset ICT perlu memulangkan kepada jabatan apabila meninggalkan jawatan yang disandang atau meninggalkan jabatan (bertukar, bersara, tamat perkhidmatan) atau kontrak perjanjian tamat.	Pegawai Aset dan pengguna RISDA dan KRH.

b) Aset ICT yang dipulangkan kepada Pegawai Aset hendaklah bersekali dengan senarai aset alih jabatan dan nota serah tugas. c) Pegawai yang mengambil alih aset ICT hendaklah menyemak dan mengesahkan fizikal dan penempatan aset tersebut. d) Memastikan segala maklumat sulit dan rahsia serta perisian-perisian dalam aset ICT dilupus atau dikeluarkan sebelum tindakan pemulangan dan pelupusan dilaksanakan.	
0402 Klasifikasi Maklumat	
Objektif : **Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.**	
040201 Kategori dan Pengelasan Maklumat	
Mengenalpasti kategori maklumat merupakan satu langkah penting dalam memastikan perlindungan yang mencukupi dan bersesuaian dengan kategori maklumat berkenaan. Semua maklumat yang dijana atau dikumpul oleh kementerian dan agensi hendaklah diasingkan mengikut kategori Maklumat Rasmi dan Maklumat Rahsia Rasmi. Kedua-dua kategori boleh mengandungi Maklumat Pengenalan Peribadi (*Personal Identifiable Information* - PII). Data Terbuka juga merupakan sebahagian daripada Maklumat Rasmi. 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 mana-mana agensi Kerajaan semasa menjalankan	Pegawai Pengelas.

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 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 yang juga dikategorikan sebagai Maklumat Rahsia Rasmi. d) Data Terbuka Data Terbuka adalah maklumat yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi Kerajaan dan organisasi swasta untuk pelbagai tujuan. Kementerian dan agensi hendaklah mematuhi pekeliling yang sedang berkuat kuasa. PII dikecualikan daripada Data Terbuka. Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam Arahan Keselamatan Kerajaan seperti berikut :- a) Rahsia Besar. b) Rahsia. c) Sulit. d) Terhad.	
040202 Pelabelan Maklumat	
Prosedur pelabelan maklumat hendaklah dilaksanakan mengikut klasifikasi maklumat yang diguna pakai oleh RISDA dan KRH.	Pengguna.
040203 Pengendalian Maklumat	
Aktiviti pengendalian makumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut :- a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa.	Pengguna.

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 pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan. g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	
0403 Pengendalian Media	
Objektif : Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
040301 Pengurusan Media Mudah Alih (*Removal Media*)	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut :- a) Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu dengan menandatangani *Non-Disclosure Agreement* (NDA) seperti di **Lampiran 2**. b) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat. c) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja dan merekodkan penggunaannya. d) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja. e) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan. f) Menyimpan semua jenis media di tempat yang selamat. g) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Pengurus ICT dan ICTSO.
040302 Pemindahan Media Fizikal	
Pihak RISDA dan KRH hendaklah memastikan media yang mengandungi maklumat rasmi dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa	Pengurus ICT, ICTSO dan pengguna.

pengangkutan atau penghantaran. Sekiranya maklumat sulit pada media tidak dapat dibuat penyulitan (*encryption*), perlindungan fizikal tambahan pada media wajar dipertimbangkan.	
040303 Pelupusan Media	
Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT selaras dengan tatacara pelupusan aset alih kerajaan atau lain-lain tatacara yang berkuat kuasa. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul serta selamat dan dengan kebenaran Ketua Jabatan. Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal.	Pengurus ICT, ICTSO dan pengguna.
040304 Sanitasi Media	
Sanitasi media merupakan proses pelupusan data dan maklumat secara kekal agar maklumat tidak diguna pakai atau dimanipulasi oleh mana-mana pihak yang mempunyai kepentingan tertentu. Semasa melaksanakan sanitasi media, perkara-perkara berikut hendaklah dipatuhi :- a) Prosedur yang berkaitan dengan sanitasi media perlu dibangunkan, diterbitkan, dibudayakan dan dikemas kini selaras dengan perkembangan teknologi, amalan terbaik serta mengikut garis panduan yang ditetapkan oleh kerajaan. b) Kaedah sanitasi yang sesuai sama ada secara logikal atau fizikal perlu ditentukan mengikut jenis media yang digunakan. c) Sanitasi logikal boleh dilaksanakan sama ada secara sanitasi fail, sanitasi partition, sanitasi media storan ataupun tetapan asal (*factory setting*). d) Sanitasi fizikal boleh dilaksanakan melalui tiga kaedah iaitu tulis ganti secara fizikal, penyingkiran (*purging*) dan pemusanahan media secara fizikal (*destroying*). e) Keputusan untuk melaksanakan proses sanitasi perlu bersandarkan kepada pengelasan data, maklumat, rekod rasmi dan rahsia rasmi serta tahap risiko berkaitan dan bukannya terhadap jenis media. f) Tadbir urus sanitasi media boleh dilaksanakan dengan mengguna pakai Jawatankuasa Menyemak, Menilai dan Mengelaskan Semula Rahsia Rasmi yang sedia ada bagi tujuan pelupusan dengan keahlian yang bersesuaian seperti mana berikut :-	Pengurus ICT, Pegawai Aset dan ICTSO.

i. Pegawai Keselamatan Jabatan/Ketua Pegawai Maklumat.
ii. Pegawai Keselamatan Kerajaan (selaku penasihat).
iii. Pegawai Arkib Negara.
iv. Pegawai Jabatan Alam Sekitar.
v. Pegawai Keselamatan ICT.
vi. Pegawai Aset.
vii. Pengurus Rekod.
viii. Pengguna.

g) Proses sanitasi media rahsia rasmi perlu memenuhi aspek perundangan dan pentadbiran yang berkuat kuasa.

h) Setiap aktiviti sanitasi media elektronik hendaklah direkodkan dengan jelas bagi menjamin akauntabiliti pengurusan sanitasi di RISDA dan KRH.

i) Sanitasi media elektronik secara fizikal perlu mematuhi keperluan undang-undang yang ditetapkan oleh Jabatan Alam Sekitar.

j) Pihak RISDA boleh melaksanakan proses sanitasi terhadap media yang ada melalui perkhidmatan yang dibangunkan oleh Jabatan Digital Negara (dahulunya dipanggil MAMPU) seperti Makmal Forensik Digital (MyDFLab) MDFlab atau lain-lain kemudahan yang seumpama.

BIDANG 05	**KAWALAN CAPAIAN**
0501	**Keperluan Kawalan Capaian**
050101	Dasar Kawalan Capaian
050102	Capaian Kepada Rangkaian dan Perkhidmatan Rangkaian
050103	Capaian Internet
0502	**Pengurusan Capaian Pengguna**
050201	Pendaftaran dan Pembatalan Pengguna
050202	Semakan Akses Pengguna
050203	Pengurusan *Priviledge Access Rights*
050204	Pengurusan Kata Laluan Pengguna
050205	Kajian Semula Hak Capaian Pengguna
050206	Pembatalan atau Pelarasan Hak Akses
0503	**Tanggungjawab Pengguna**
050301	Penggunaan Kata Laluan
0504	**Kawalan Capaian Sistem dan Aplikasi**
050401	Had Kawalan Capaian Maklumat
050402	Prosedur *Log On* (Log Masuk)
050403	Sistem Pengurusan Kata Laluan
050404	Penggunaan Sistem Utiliti
050405	Kawalan Akses Kepada Kod Sumber (*Source Code*)
050406	Peralatan Mudah Alih
050407	Kerja Jarak Jauh
050408	Pengurusan Peralatan Persendirian (*Bring Your Own Device/*BYOD)

BIDANG 05
KAWALAN CAPAIAN

0501 Keperluan Kawalan Capaian

Objektif : Menghadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan ICT dalam mengawal capaian ke atas maklumat.

050101 Dasar Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Setiap keperluan akses mestilah dirancang, didokumentasikan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini mengikut keperluan dan menyokong peraturan kawalan capaian pengguna sedia ada. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna. b) Undang-undang dan peraturan berkaitan yang sedang berkuat kuasa. c) Kawalan capaian keatas perkhidmatan rangkaian dalaman dan luaran. d) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih. e) Kawalan ke atas kemudahan pemprosesan maklumat. f) Keperluan semakan hak akses secara berkala. g) Kebenaran rasmi bagi permintaan dan pembatalan hak akses.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT.

050102 Capaian Kepada Rangkaian dan Perkhidmatan Rangkaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan :- a) Menempatkan atau memasang antaramuka yang bersesuaian di antara rangkaian organisasi, rangkaian agensi lain dan rangkaian awam. b) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian. c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT.

050103 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Penggunaan Internet hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian RISDA dan KRH. b) Kaedah *Content Filtering* boleh digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan. c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) boleh dilaksana bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan. d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya. e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Pengarah/pegawai yang diberi kuasa. f) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan. g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian/Ketua Jabatan Teknologi Maklumat sebelum dimuat naik ke Internet. h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara. i) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh jabatan. j) Penggunaan sebarang bentuk modem persendirian untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali. k) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut :- i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian Internet. ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	Semua.

0502 Pengurusan Capaian Pengguna	
Objektif : Memastikan kawalan capaian oleh pengguna yang dibenarkan sahaja.	
050201 Pendaftaran dan Pembatalan Pengguna	
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan capaian dan pembatalan hak capaian dikuatkuasakan. Perkara-perkara berikut hendaklah dipatuhi :- a) Setiap pengguna mempunyai akaun ID yang unik dan bertanggungjawab terhadap tindakan sendiri. Perkongsian ID adalah tidak dibenarkan. b) Akaun ID pengguna dibatalkan/ dihapuskan jika berhenti/ bersara/ bertukar organisasi. c) Tiada pertindihan akaun ID pengguna.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT.
050202 Semakan Akses Pengguna	
Proses semakan akses penguna perlu dilaksanakan dari semasa ke semasa untuk mengkaji semula kebenaran dan pembatalan capaian penguna ke atas aplikasi dan perkhidmatan.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT.
050203 Pengurusan *Priviledge Access Rights*	
Penggunaan *priviledge access rights* perlu dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	ICTSO dan Pentadbir Sistem ICT.
050204 Pengurusan Kata Laluan Pengguna	
Peruntukan kata laluan perlu melalui beberapa proses pengurusan yang formal seperti berikut :- a) Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan. b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna. c) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna. d) Pengguna perlu disediakan dengan kata laluan sementara, yang perlu ditukar pada penggunaan pertama.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT.

e) Prosedur perlu diwujudkan untuk mengesahkan identiti pengguna sebelum menyediakan kata laluan yang baharu, penggantian atau sementara. f) Kata laluan sementara perlu diedar kepada pengguna dengan selamat dimana katalaluan tidak boleh diedarkan kepada pihak ketiga dan dalam *clear text*. g) Pengguna perlu mengesahkan penerimaan kata laluan. h) Kata laluan *default* perlu diubah selepas pemasangan sistem atau perisian. i) Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem terlebih dahulu. j) Maklumat kata laluan sebaik-baiknya disimpan di dalam fail yang berasingan dengan fail data aplikasi. k) Penggunaan teknologi tambahan seperti kad pintar dan teknologi *biometric authentication* perlu dipertimbangkan untuk sistem yang terperingkat. l) Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab yang berikut :- i. Pengguna yang bercuti panjang untuk tempoh melebihi sebulan atau pada satu tempoh masa yang dipersetujui. ii. Bertukar bidang tugas kerja. iii. Bertukar ke agensi lain. iv. Bersara. v. Meninggal dunia. vi. Ditamatkan perkhidmatan. vii. Diarahkan oleh Ketua Jabatan. m) Penggunaan Multi-Factor Authentication (MFA) adalah digalakkan.	
050205 Kajian Semula Hak Capaian Pengguna	
Pemilik aset ICT hendaklah mengkaji semula hak capaian pengguna secara berkala atau sekurang-kurangnya satu kali setahun.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT.
050206 Pembatalan atau Pelarasan Hak Akses	
Hak capaian kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data dan maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian, atau diselaraskan apabila berlaku sebarang perubahan. Pembatalan akaun (pengguna yang tamat perkhidmatan, bertukar dan melanggar dasar dan tatacara	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT.

jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat. Pihak RISDA dan KRH boleh membekukan akaun pengguna, jika perlu, semasa pengguna bercuti panjang, berkursus atau pun menghadapi tindakan tatatertib.	
0503 Tanggungjawab Pengguna	
Objektif : Untuk memastikan pengguna bertanggungjawab melindungi maklumat yang digunakan untuk pengesahan identiti mereka.	
050301 Penggunaan Kata Laluan	
Setiap pengguna sistem ICT mestilah mempunyai ID pengguna (*user id*) dan kata laluan masing-masing serta mengambil perhatian terhadap perkara berikut :- a) Bertanggungjawab terhadap kata laluan masing-masing agar tidak berlaku kebocoran kepada orang lain. b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran katalaluan atau dikompromi. c) Katalaluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun. d) Pengguna disaran menggunakan kemudahan kata laluan *screen saver* atau *log off* sekiranya meninggalkan komputer. e) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi. f) Kata laluan mesti sekurang-kurangnya lapan aksara bagi pengguna dengan mempunyai kombinasi huruf, angka dan aksara khas. g) Kata laluan perlu ditukar sekurang-kurangnya setiap enam bulan sekali atau selepas tempoh masa yang bersesuaian. h) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang. i) Pengguna haruslah tidak menggunakan kata laluan baharu yang sama atau seakan-akan serupa seperti mana yang pernah digunakan pada masa sebelumnya. j) Pemilikan akaun pengguna bukanlah hakmilik mutlak seseorang dan ia tertakluk kepada peraturan di RISDA dan KRH. Akaun boleh ditarik jika penggunaannya melanggar peraturan yang ditetapkan.	Semua.

0504 Kawalan Capaian Sistem dan Aplikasi	
Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi.	
050401 Had Kawalan Capaian Maklumat	
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.	Pentadbir Sistem ICT dan semua staf.
050402 Prosedur *Log On*	
Capaian kepada sistem dan aplikasi hendaklah dikawal oleh prosedur *log on* mengikut keperluan. Bahagian/Jabatan Teknologi Maklumat hendaklah mengenal pasti teknik pengesahan *log on* yang sesuai iaitu :- a) Paparkan suatu notis amaran bahawa komputer hanya boleh diakses oleh pengguna yang sah. b) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan. c) Mengesahkan pengguna yang dibenarkan. d) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian termasuk pengguna bertaraf *super user*. e) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin. f) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. g) Menamatkan sesi yang tidak aktif selepas tempoh yang tertentu. Tempoh minima yang disyorkan terutama kepada aplikasi kritital adalah selama 10 minit. h) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja. i) Menghadkan dan mengawal penggunaan program. j) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi. k) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan. l) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log).	Pentadbir Sistem ICT.

m) Menghadkan capaian sistem dan aplikasi kepada tiga kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat. n) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah.	
050403 Sistem Pengurusan Kata Laluan	
Sistem pengurusan kata laluan mestilah interaktif dan menjamin kata laluan yang berkualiti seperti berikut :- a) Membenarkan pengguna untuk menukar kata laluannya sendiri. b) Menekankan pilihan kata laluan yang kukuh dan berkualiti. c) Kata laluan perlu ditukar secara berkala. d) Tidak memaparkan kata laluan pada skrin semasa proses log masuk. e) Kata laluan mesti sekurang-kurangnya lapan aksara bagi pengguna dengan mempunyai kombinasi huruf, angka dan aksara khas.	Semua.
050404 Penggunaan Sistem Utiliti	
Penggunaan program utiliti yang mungkin boleh *Over-Riding System* perlu dihadkan hanya kepada Pentadbir Sistem ICT dan dikawal ketat penggunaannya.	Pengurus ICT dan ICTSO.
050405 Kawalan Akses Kepada Kod Sumber (*Source Code*)	
Pembangunan aplikasi di RISDA dan KRH perlu diluluskan oleh Jawatankuasa Pemandu ICT dan dipantau oleh Bahagian/Jabatan Teknologi Maklumat atau pegawai yang bertanggungjawab terhadap aplikasi berkenaan. Selain itu, semua kod sumber aplikasi adalah tertakluk kepada perkara seperti berikut :- a) Kakitangan sokongan RISDA dan KRH perlu dihadkan akses kepada kod sumber. b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada prosedur kawalan perubahan yang ketat. c) Kod sumber bagi semua aplikasi dan perisian adalah hak milik RISDA/KRH. d) Sekiranya perlu, kod sumber perlu diasingkan daripada *production serv*er.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT.

050406 Peralatan Mudah Alih	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Peralatan mudah alih seperti telefon pintar, *tablet* dan komputer riba yang digunakan untuk tujuan rasmi sama ada yang disediakan oleh RISDA, KRH atau milik persendirian hendaklah dipastikan patuh pada polisi dan prosedur yang ditetapkan. b) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. c) Memastikan bahawa antivirus digunakan dan sentiasa dikemas kini untuk aset ICT yang digunakan. d) Semasa menggunakan rangkaian komputer awam (*public Wi-fi*), capaian kepada dokumen terperingkat hendaklah dihadkan. Sekiranya terdapat keperluan untuk berbuat demikian, langkah-langkah kawalan keselamatan perlu diambil supaya maklumat tersebut tidak boleh dicapai oleh pihak yang tidak berkenaan. e) Maklumat dokumen terperingkat tidak dibenarkan untuk disimpan di dalam peralatan mudah alih tanpa kebenaran CDO. f) Memastikan peralatan mudah alih yang dibawa keluar dari pejabat disimpan dan dijaga dengan baik bagi mengelakkan kehilangan, pendedahan maklumat, capaian tidak sah dan salah guna kemudahan. g) Proses backup perlu dilaksanakan bagi menjamin keselamatan data. h) Merekodkan pergerakan peralatan mudah alih bagi mengesan berlakunya kehilangan atau kerosakan.	Semua.
050407 Kerja Jarak Jauh	
Capaian jarak jauh adalah bermaksud capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan *telecommuting*. Penggunaannya adalah terhad kepada kemudahan yang dibenarkan sahaja dan perkara-perkara yang perlu dipatuhi adalah :- a) Penghantaran maklumat terperingkat/sensitif yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi. b) Penggunaan perkhidmatan jarak jauh hendaklah mendapat kebenaran daripada Pengurus ICT. c) Lokasi bagi akses ke sistem ICT berkenaan hendaklah dipastikan selamat. d) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua.

e) Memastikan bahawa antivirus digunakan dan sentiasa dikemas kini untuk aset ICT yang digunakan. f) Pengguna yang diberi hak adalah bertanggungjawab sepenuhnya ke atas penggunaan kemudahan yang diberikan.	
050408 Pengurusan Peralatan Persendirian (*Bring Your Own Device*/BYOD)	
BYOD adalah peralatan mudah alih persendirian seperti telefon pintar, *tablet* dan komputer riba yang digunakan untuk tujuan rasmi. Berikut adalah langkah-langkah bagi memastikan keselamatan maklumat semasa penggunaan peralatan mudah alih peribadi: a) Aplikasi yang dimuat turun oleh pengguna melalui Internet ke dalam peranti mudah alih peribadi boleh mendatangkan ancaman dan risiko serta impak yang besar terhadap keselamatan apabila peranti yang sama digunakan untuk mencapai maklumat dan aplikasi rasmi RISDA dan KRH. Oleh itu, pengguna haruslah memastikan peranti dipasang perisian antivirus yang sah. b) Menggunakan peranti secara berhemah sepanjang masa dan mematuhi peraturan yang berkuatkuasa. c) Bertanggungjawab memadam segala maklumat yang berkaitan dengan urusan rasmi kerajaan sewaktu dihantar ke pusat servis untuk penyelenggaraan. d) Bertanggungjawab dan boleh dikenakan tindakan tatatertib sekiranya didapati menyalahgunakan BYOD yang menyebabkan kehilangan/ kerosakan/ pendedahan maklumat rasmi kerajaan. e) Pengguna adalah dilarang menggunakan BYOD untuk akses, simpan dan sebar maklumat Rasmi dan Terperingkat kepada pihak yang tidak dibenarkan. f) Mengelakkan penggunaan BYOD untuk tujuan peribadi yang boleh mengganggu produktiviti kerja. g) Menghindari untuk merakam komunikasi dan dokumen rasmi untuk tujuan peribadi.	Semua.

BIDANG 06	**KRIPTOGRAFI**

0601	**Kawalan Penyulitan Maklumat (*Cryptography*)**
060101	Polisi Pengunaan Penyulitan Maklumat
060102	Pengurusan Infrastruktur Kunci Awam
060103	Tandatangan Digital

BIDANG 06 KRIPTOGRAFI	
0601 Kawalan Penyulitan Maklumat (*Cryptography*)	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
060101 Polisi Pengunaan Penyulitan Maklumat	
Perkara-perkara berkaitan penyulitan maklumat yang perlu dipatuhi adalah seperti berikut :- a) Pengurusan maklumat rahsia rasmi hendaklah dilaksanakan dengan menggunakan teknologi atau kaedah yang bersesuaian bagi melindungi maklumat rahsia rasmi supaya tidak terdedah kepada mereka yang tidak sah. Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat rahsia rasmi pada setiap masa. b) Mengenal pasti tahap perlindungan pengunaan penyulitan dengan mengambil kira jenis, kekuatan dan kualiti algoritma yang diperlukan. c) Maklumat terperingkat atau maklumat rahsia rasmi hendaklah melalui proses penyulitan setiap masa sebelum dihantar atau disalurkan ke dalam sistem rangkaian yang tidak selamat (seperti Internet, *mobile network* dan sebagainya).	ICTSO.
060102 Pengurusan Infrastruktur Kunci Awam	
Kunci penyulitan perlu diuruskan dengan baik, iaitu :- a) Kaedah yang selamat hendaklah digunakan bagi melindungi komuniksi rangkaian seperti *Secure Socket Layer* (SSL) dan *Virtual Private Network* (VPN). b) Diuruskan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut. c) Perkongsian token untuk sebarang capaian sistem adalah tidak dibenarkan. d) Peralatan yang digunakan untuk menjana, menyimpan dan arkib kunci penyulitan perlu dilindungi secara fizikal. e) Sebarang kehilangan, kerosakan dan katalaluan yang disekat, pengguna perlu merujuk kepada bahagian/pihak yang berkaitan. f) Sistem pengurusan kunci perlu berdasarkan satu set piawaian, prosedur dan kaedah yang dipersetujui. g) Pemegang sijil digital perlu memulangka token apabila tamat perkhidmatan, bersara atau tidak digunakan dalam sistem.	Pengurus ICT dan ICTSO.

060103 Tandatangan Digital	
Penggunaan tandatangan digital adalah digalakkan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik. Akta Tandatangan Digital 1997 tidak membenarkan sijil pengguna untuk dipindah milik kerana sijil digital tersebut merupakan identiti pengguna dalam ruang siber.	Pengurus ICT dan ICTSO.

BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN

0701 Keselamatan Kawasan

070101 Lingkungan Keselamatan Fizikal
070102 Kawalan Masuk Fizikal
070103 Kawalan Pejabat, Bilik dan Tempat Operasi
070104 Perlindungan Terhadap Ancaman Luaran dan Persekitaran
070105 Bertugas Dalam Kawasan Larangan
070106 Keselamatan Pusat Data dan Bilik Server
070107 Kawasan Penghantaran dan Pemunggahan

0702 Keselamatan Peralatan ICT

070201 Kedudukan dan Kawalan Peralatan ICT
070202 Alat Sokongan
070203 Keselamatan Kabel
070204 Penyelenggaraan Peralatan
070205 Peralatan Dibawa Keluar Premis
070206 Keselamatan Peralatan di Luar Premis
070207 Pelupusan Peralatan dan Kitar Semula
070208 Penjagaan Peralatan Yang Tidak Diguna
070209 *Clear Desk* dan *Clear Screen*
070210 Media Storan
070211 Media Tandatangan Digital
070212 Media Perisian dan Aplikasi
070213 Keselamatan Dokumen
070214 Kejuruteraan Sosial
070215 Prosedur Kecemasan

BIDANG 07
KESELAMATAN FIZIKAL DAN PERSEKITARAN

0701 Keselamatan Kawasan

Objektif : Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

070101 Lingkungan Keselamatan Fizikal

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut :- a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko. b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat. c) Memperkukuhkan struktur tingkap dan pintu yang dikunci untuk kawalan kemasukkan serta kunci harus disimpan oleh pegawai bertanggungjawab. d) Memperkukuhkan struktur dinding dan siling. e) Memasang alat penggera atau kamera (sistem CCTV). f) Menghadkan jalan keluar masuk. g) Mengadakan kaunter kawalan. h) Menyediakan tempat atau bilik khas untuk pelawat-pelawat. i) Mewujudkan perkhidmatan kawalan keselamatan. j) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini. k) Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan. l) Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana. m) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad.	Pegawai Keselamatan Jabatan.

n) Memastikan kawasan-kawasan penghantaran, pemunggahan dan juga tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya.
o) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada garis panduan keselamatan jabatan yang berkuatkuasa.
p) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) atau peranan setara yang dilantik.

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK) atau pihak-pihak lain yang bertanggungjawab. Perkara-perkara berikut hendaklah dipatuhi bagi menjamin keselamatan persekitaran :-

a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data, bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya dengan teliti.
b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan.
c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan.
d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT.
e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT.
f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer.
g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.
h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.

070102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut :- a) Setiap pegawai dan kakitangan RISDA dan KRH hendaklah memakai atau mengenakan kad pekerja atau pas keselamatan sepanjang waktu bertugas. b) Semua kad pekerja atau pas keselamatan hendaklah diserahkan semula kepada jabatan apabila berhenti, tamat perkhidmatan atau bersara. c) Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di pintu kawalan utama bangunan pejabat RISDA dan KRH serta mengembalikannya setelah selesai lawatan. d) Kehilangan kad pekerja atau pas keselamatan mestilah dilaporkan kepada jabatan dengan segera.	Pegawai Keselamatan Jabatan.
070103 Kawalan Pejabat, Bilik dan Tempat Operasi	
Perkara yang perlu dipatuhi adalah seperti berikut :- a) Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada akses oleh pihak luar. b) Kawalan keluar masuk perlu teratur sama ada melalui sistem berkunci ataupun dengan sistem *Security Access Door*. c) Pegawai pengiring perlu sentiasa berada bersama pihak pembekal sekiranya perlu melaksanakan tugas di pusat data atau bilik server. d) Penunjuk ke lokasi bilik operasi dan tempat larangan tidak seharusnya menonjol dan hanya memberikan petunjuk yang minimum.	Pegawai Keselamatan Jabatan.
070104 Perlindungan Terhadap Ancaman Luaran dan Persekitaran	
Pengurusan RISDA dan KRH perlu merekabentuk dan melaksanakan perlindungan fizikal yang sewajarnya daripada ancaman kebakaran, banjir, letupan, kacau bilau dan bencana.	Pegawai Keselamatan Jabatan.
070105 Bertugas Dalam Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Antara kawasan larangan di RISDA adalah Bilik Ketua Pengarah,	

Bilik Timbalan Ketua Pengarah, Bilik Pengarah Bahagian, Bilik Ketua Pusat Tanggungjawab, pusat data, bilik server, bilik fail dan seumpamanya. a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja. b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan mereka hendaklah diiringi atau boleh dibantu melalui pemantauan CCTV sehingga tugas/janji temu di kawasan berkenaan selesai.	Pegawai Keselamatan Jabatan.
070106 Keselamatan Pusat Data dan Bilik Server	
Semua pelayan hendaklah diletakkan di dalam pusat data yang mempunyai kemudahan keselamatan, penyaman udara khas, kemudahan perlindungan suhu dan kebakaran. Lokasi pusat data juga perlu dilengkapi dengan ciri-ciri keselamatan lain seperti pemantauan sistem CCTV dan UPS. Berikut adalah beberapa langkah untuk melindungi server di pusat data/bilik server tersebut: a) Memastikan hanya pegawai-pegawai yang mempunyai kebenaran sahaja yang dibenarkan memasuki pusat data/bilik server. b) Menyediakan buku log pelawat bagi memantau dan mengawal pergerakan keluar masuk pelawat. c) Memastikan pusat data/bilik server sentiasa bersih dan peralatan ICT tidak terdedah kepada habuk. d) Memastikan bilik server mempunyai kitar pengudaraan yang bersesuaian. e) Memastikan penyaman udara berfungsi dengan baik dan suhunya bersesuaian. f) Memastikan pusat data dilengkapi dengan sistem pencegahan dan penggera kebakaran yang berfungsi dengan baik. g) Memastikan semua peralatan keselamatan, UPS dan penyaman udara diselenggara secara berkala. h) Memastikan setiap rak perkakasan pelayan dan rangkaian dikunci dan kunci tersebut disimpan di tempat yang selamat. i) Peralatan media perakaman adalah tidak dibenarkan di bawa masuk ke dalam pusat data/bilik server. j) Aktiviti mengambil gambar, merakam video, merekod suara atau penggunaan peralatan yang tidak dibenarkan adalah dilarang.	Pentadbir Pusat Data.

070107 Kawasan Penghantaran dan Pemunggahan	
Kawasan penghantaran dan pemunggahan hendaklah dikawal dan jika boleh, ia diasingkan daripada kemudahan pemprosesan maklumat. Pengurusan RISDA/KRH hendaklah memastikan kawasan-kawasan penghantaran, pemunggahan dan tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya.	Pegawai Keselamatan Jabatan.
0702 Keselamatan Peralatan ICT	
Objektif : Melindungi peralatan ICT RISDA daripada kehilangan, kerosakan, kecurian dan disalahgunakan.	
070201 Kedudukan dan Kawalan Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna. b) Pengguna adalah bertanggungjawab diatas kerosakan atau kehilangan peralatan ICT di bawah kawalannya. c) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja. d) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran. e) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan. f) Pengguna dilarang sama sekali menambah, menanggalkan atau mengganti sebarang perkakasan ICT yang telah ditetapkan. g) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Bahagian/Jabatan Teknologi Maklumat. h) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini disamping melakukan imbasan ke atas semua media storan yang digunakan.	Semua.

i) Bagi sistem rangkaian komputer yang telah sedia dengan kemudahan perkhidmatan *Active Directory*, setiap komputer pengguna perlu menyertai (*join*) domain bagi membolehkan akaun pada *Active Directory* tersebut digunakan sebagai log masuk.

j) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan.

k) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci.

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

m) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS).

n) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik.

o) Memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan '*OFF*' apabila meninggalkan pejabat.

p) Menutup suis dan menanggalkan palam kuasa bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.

q) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset.

r) Peralatan ICT yang hendak dibawa keluar dari premis RISDA atau KRH, perlulah mendapat kelulusan Bahagian/Jabatan Teknologi Maklumat dan direkodkan bagi tujuan pemantauan.

s) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera.

t) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal.

u) Pengguna dilarang sama sekali mengubah kata laluan pentadbir (*administrator password)* yang telah ditetapkan.

v) Semua mesin penyalin (pengimbas/fotostat) yang berupaya menyimpan memori hendaklah dipadamkam memorinya apabila tamat tempoh kegunaan atau penyewaan.

a) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Bahagian/Jabatan Teknologi Maklumat untuk tujuan dibaik pulih.

b) Pengendalian peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih.

c) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO ataupun Pengurus ICT.

d) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa.	
070202 Alat Sokongan	
a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT. b) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di pusat data/bilik server supaya mendapat bekalan kuasa berterusan. c) Semua alat sokongan perlu disemak dan diuji secara berjadual bagi memastikan ia dapat berfungsi dengan baik.	Pegawai Keselamatan Jabatan.
070203 Keselamatan Kabel	
Keselamatan kabel adalah meliputi kabel elektrik dan kabel telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat. 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*. d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Pengurus ICT dan Pegawai Keselamatan Jabatan.
070204 Penyelenggaraan Peralatan	
Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Semua peralatan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar. b) Memastikan peralatan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja. c) Bertanggungjawab terhadap setiap peralatan bagi penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan.	Pengurus ICT dan Pegawai Aset.

d) Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan. e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan. f) Penyenggaraan perkakasan oleh pembekal perlu dilakukan secara *onsite* dengan pengawasan oleh pihak yang berkenaan. g) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	
070205 Peralatan Dibawa Keluar Premis	
Peralatan ICT yang hendak dibawa keluar daripada premis RISDA atau KRH untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Jabatan atau pegawai yang diturunkan kuasa mempunyai tempoh had masa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan. Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	Pengurus ICT dan Pegawai Aset.
070206 Keselamatan Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari premis RISDA atau KRH adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Peralatan perlu dilindungi dan dikawal sepanjang masa. b) Pergerakan aset perlu melalui prosedur yang ditetapkan. c) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian. d) Sebarang sambungan ke rangkaian dan Internet di tempat awam perlu mengambilkira faktor keselamatan rangkaian terutamanya melibatkan kerja rasmi. e) Perkakasan perlu dipastikan tidak digunakan oleh mana-mana pihak ketiga. f) Sebarang laporan kehilangan peralatan hendaklak mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa.	Semua.
070207 Pelupusan Peralatan dan Kitar Semula	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh jabatan. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan RISDA/KRH. Perkara yang perlu dipatuhi adalah seperti berikut :-	

a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui kaedah atau teknik yang bersesuaian (s*hredding, grinding, degaussing* atau pembakaran) agar maklumat tidak dapat dicapai semula. b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat pendua (salinan maklumat). c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat. d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya. e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut. f) Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem pengurusan aset RISDA/KRH. g) Pelupusan peralatan ICT hendaklah dilaksanakan mengikut tatacara pelupusan semasa yang berkuat kuasa. h) Pengguna adalah dilarang menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hard disk*, *motherboard* dan sebagainya. i) Pengguna adalah dilarang memindah keluar dari RISDA mana-mana peralatan ICT yang hendak dilupuskan. j) Pengguna adalah dilarang melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan adalah di bawah tanggungjawab RISDA/KRH. k) Prosedur pelupusan rekod elektronik adalah tertakluk kepada garis panduan yang berkuat kuasa yang dikeluarkan kerajaan melalui Arkib Negara Malaysia.	Pegawai Aset.
070208 Penjagaan Peralatan Yang Tidak Diguna	
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* server, *log* keluar daripada aplikasi dan komputer pejabat serta apabila sesi bertugas selesai.	Semua.

c) Kawal keselamatan komputer dan peralatan mudah alih daripada akses yang tidak dibenarkan dengan menggunakan katalaluan, *lock screen* dan sebagainya apabila tidak digunakan.	
070209 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear desk* dan c*lear screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara yang perlu dipatuhi adalah seperti berikut :- a) Menggunakan kemudahan kata laluan pada *screen saver* atau *logout* apabila meninggalkan komputer. b) Menyimpan bahan-bahan sensitif seperti media storan dan dokumen terperingkat di dalam laci atau kabinet fail yang berkunci. c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat. d) Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital. e) Mengawal e-mel yang masuk dan keluar.	Semua.
070210 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti cakera padat, pita magnetik, *optical disk*, *flash disk*, CD-ROM, *thumb drive* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat. b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja. c) Semua media storan perlu dikawal bagi mencegah daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan.	Semua.

d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet. e) Akses dan pergerakan media storan hendaklah direkodkan. f) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal. g) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data. h) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat mengikut tatacara pelupusan yang berkuatkuasa. i) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
070211 Media Tandatangan Digital	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Pengguna hendaklah bertanggungjawab sepenuhnya keatas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan. b) Media ini tidak boleh dipindah milik atau dipinjamkan. c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO atau pegawai lain yang bertanggungjawab untuk tindakan seterusnya.	Semua.
070212 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Hanya perisian yang diperakui oleh pihak Bahagian/Jabatan Teknologi Maklumat sahaja dibenarkan bagi kegunaan di RISDA atau KRH. b) Sistem aplikasi dalaman tidak dibenarkan didemontrasikan atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT. c) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada CD-ROM, disk atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak. d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua.

070213 Keselamatan Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar. b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan. c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimalumkan mengikut prosedur Arahan Keselamatan. d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara serta lain-lain peraturan yang berkaitan. e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik. f) Penyimpanan dokumen rasmi (data terkawal dan rahsia rasmi) di storan atas talian umum adalah perlu mengikut pekeliling perkomputeran awan (*cloud computing*) dalam perkhidmatan awam yang sedang berkuatkuasa. g) Pengguna di RISDA dan KRH adalah dilarang untuk memuatnaik dokumen dan maklumat-maklumat rasmi ke Internet terutamanya untuk tujuan pemprosesan dokumen (salinan *softcopy*) atau berkongsi dokumen di platform-platform perkhidmatan prosesan dokumen komersil. Hal ini adalah kerana aktiviti tersebut akan merisikokan kandungan dalam dokumen/fail tersebut menjadi tatapan umum dan terus boleh dicapai secara terbuka di Internet.	Semua.
070214 Kejuruteraan Sosial	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Pengurusan aset ICT juga hendaklah mengambil kira keperluan kawalan keselamatan terhadap kejuruteraan sosial (*social engineering*) bagi melindungi kerahsiaan dan integriti maklumat kerajaan. b) Kejuruteraan sosial merujuk kepada serangan siber yang memanipulasi kelemahan manusia melalui penggunaan teknik interaksi dan kemahiran sosial untuk memperoleh maklumat tentang sesebuah organisasi atau sistem pengkomputeran organisasi. Ia	Semua.

merupakan satu kaedah bukan teknikal bagi menceroboh atau menggodam sistem maklumat dengan melakukan penyamaran/helah muslihat.	
070215 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada garis panduan berkaitan pelan tindakan dan kecemasan jabatan yang berkuatkuasa. b) Semasa berlaku kecemasan persekitaran seperti kebakaran, ia hendaklah dilaporkan kepada pegawai keselamatan kebakaran yang dilantik mengikut aras/unit/bahagian.	

BIDANG 08 PENGURUSAN OPERASI

0801 Pengoperasian dan Tanggungjawab

080101 Dokumentasi Prosedur Pengoperasian

080102 Pengurusan Perubahan

080103 Pengurusan Kapasiti

080104 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi

0802 Perlindungan Daripada *Malware*

080201 Kawalan Daripada Perisian Berbahaya

080202 Sekatan Dalam Instalasi Perisian

0803 Backup

080301 *Backup* Maklumat

0804 Log dan Pemantauan

080401 Jejak Audit

080402 Perlindungan Maklumat Log

080403 Log Pentadbir dan Operator

080404 Penyelarasan Waktu

0805 Kawalan Perisian Operasi

080501 Pemasangan Perisian Pada Sistem Operasi

0806 Pengurusan Keterdedahan Teknikal

080601 Pengurusan Kelemahan Teknikal

080602 Kawalan Pemasangan Perisian

0807 Pertimbangan Pelaksanaan Audit Sistem Maklumat

080701 Pematuhan Keperluan Audit dan Kawalan Audit Sistem Maklumat

080702 Pengauditan dan Forensik ICT

0808 Keselamatan Sistem Dokumentasi

0809 Pengurusan Pertukaran Maklumat

BIDANG 08 PENGURUSAN OPERASI	
0801 Pengoperasian dan Tanggungjawab	
Objektif : Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan ke atas fasiliti pemprosesan maklumat.	
080101 Dokumentasi Prosedur Pengoperasian	
Bagi memastikan prosedur pengoperasian didokumentasikan dan disediakan untuk pengguna-pengguna yang berkaitan, perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Semua prosedur pengurusan operasi yang diwujudkan, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal. b) Salinan prosedur adalah digalakkan untuk dibuat dalam dua salinan (*hardcopy/softcopy*) bagi tujuan rujukan dan penggunaan sekiranya berlaku bencana. c) 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. d) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan. e) Aspek penyimpanan dokumentasi perlu dilengkapi dengan ciri-ciri keselamatan yang memberikan perlindungan kepada dokumen yang disimpan.	Pengurus ICT dan ICTSO.
080102 Pengurusan Perubahan	
Perubahan terhadap organisasi, proses, operasi, sistem dan fasiliti pemprosesan maklumat yang memberi kesan terhadap keselamatan maklumat perlu dikawal. Oleh itu, perkara yang perlu dipatuhi adalah seperti berikut :- a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada Ketua Jabatan atau Pengurus ICT. b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan.	Pengurus ICT, CDO, Pentadbir Sistem ICT dan semua staf.

c) Semua aktiviti pengubahsuaian komponen peralatan ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak. e) Untuk perubahan yang membabitkan sistem aplikasi kritikal, kajian awal perlu dibuat bagi menilai dan memastikan impak yang boleh berlaku terhadap operasi perkhidmatan dan keselamatan maklumat.	
080103 Pengurusan Kapasiti	
a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. 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.	Pengurus ICT dan Pentadbir Sistem ICT.
080104 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi	
a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT. b) Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. d) Menyediakan perkakasan atau persekitaran sistem yang khusus untuk tujuan latihan (platform sistem ICT untuk mode latihan) juga adalah amat digalakkan.	Pentadbir Sistem ICT.
0802 Perlindungan Daripada *Malware*	
Objektif : Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.	

080201 Kawalan Daripada Perisian Berbahaya	
Perkara yang perlu dipatuhi adalah seperti berikut :- a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, *Intrusion Detection System (*IDS*)* dan *Intrusion Prevention System (*IPS*)* serta mengikut prosedur penggunaan yang betul dan selamat. b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa. c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya. d) Mengemaskini antivirus dengan paten antivirus yang terkini, pengemaskinian perlu dilakukan sekurang-kurangnya sekali sehari atau apabila terdapat paten terkini. e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat. f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya. g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi perisian berbahaya. h) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus. i) Memaklumkan sebarang peringatan, amaran, ancaman atau kerosakan yang dikesan kepada Pentadbir Sistem atau ICTSO. j) Penggunaan *mobile code* terutamanya dari Internet dan e-mel yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan. k) Mengambil tindakan yang sewajarnya terhadap semua peringatan dan arahan yang dikeluarkan oleh Pentadbir Sistem atau ICTSO.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT.
080202 Sekatan Dalam Instalasi Perisian	
Peraturan berhubung instalasi perisian perlu diwujudkan dan dilaksanakan dengan perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut :- a) Polisi yang jelas berkaitan jenis perisian yang dibenar (seperti *patch* keselamatan untuk perisian sedia ada) dan tidak dibenarkan (seperti perisian untuk kegunaan peribadi) untuk instalasi perlu dibangun dan dikuatkuasakan.	Semua.

b) Pengguna tidak boleh sewenang-wenangnya memasang perisian melainkan terlebih dahulu mendapat kelulusan daripada pihak Bahagian/Jabatan Teknologi Maklumat. c) Prinsip keutamaan rendah wajar diadaptasi dalam peraturan instalasi perisian. Jika sesuatu keizinan diberikan oleh pihak Bahagian/Jabatan Teknologi Maklumat, pengesahan terhadap lesen, keserasian perisian dan kemampuan pengguna perlu dipastikan untuk melaksanakan proses instalasi.	
0803 Backup	
Objektif : Melindungi daripada kehilangan data.	
080301 Backup Maklumat	
Untuk memastikan sistem dapat diaktifkan semula setelah berlakunya bencana, backup hendaklah dilakukan setiap kali konfigurasi berubah. Perkara yang perlu dipatuhi adalah seperti berikut :- a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaharu. b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat. Ia boleh dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan dan sebagainya. c) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat. d) Salinan direkodkan dan di simpan di *off-site*. Lokasi *off-site* tidak boleh di bangunan yang sama dan pemilihan lokasi mestilah praktikal dengan mengambil kira aspek geografi, kemudahan, keselamatan, kos dan persekitaran. e) Menyimpan sekurang-kurangnya tiga generasi salinan *backup*. f) Menguji sistem *backup* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.	Pentadbir Sistem ICT.
0804 Log dan Pemantauan	
Objektif : Merekodkan peristiwa dan menjana bukti.	
080401 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti pengguna ICT yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan	

pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu peristiwa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Semua perkakasan atau utiliti mestilah mengaktifkan audit log yang merekodkan setiap aktiviti transaksi. Audit log perlu disimpan untuk tempoh masa yang dipersetujui sebelum dilupuskan. b) Semua laporan log atau *audit trail* dan program atau utiliti mestilah dikawal agar mengekalkan integriti data dan hanya boleh diakses oleh Pentadbir Sistem ICT dan personel keselamatan sahaja. c) Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti sistem pengoperasian, log *service*, log aplikasi dan log rangkaian. d) Aktiviti-aktiviti Pentadbir Sistem ICT mestilah dilogkan. e) Sebarang cubaan memasuki sistem (*login*) yang tidak berjaya mestilah dilogkan dan perlu diberi perhatian. f) Maklumat jejak audit perlu mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan. g) Jejak audit perlu mengandungi aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya. h) Jejak audit perlu mengandungi maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. i) Jejak audit disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. j) Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan. k) Penggera keselamatan boleh dipertimbangkan untuk memberikan amaran kepada Pentadbir Sistem ICT secara automatik sebagai tanda peringatan. l) Semua sistem komputer dan peranti rangkaian mestilah mempunyai catatan masa yang seragam bagi memastikan kesahihan masa yang tercatat dalam log audit. m) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian. n) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO atau CDO.	Pentadbir Sistem ICT.

o) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian. p) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala.	
080402 Perlindungan Maklumat Log	
Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan.	Pentadbir Sistem ICT.
080403 Log Pentadbir dan Operator	
a) Pentadbir Sistem ICT dan Pentadbir Rangkaian dikehendaki menganalisa log atau *audit trail* dari semasa ke semasa. b) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. c) Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu. d) Fail log hendaklah disimpan untuk tempoh sekurang-kurangnya enam bulan di tempat selamat dan boleh dikemukakan kepada NACSA atau lain-lain pihak berwajib apabila diperlukan untuk pngendalian insiden keselamatan ICT. e) Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti berikut:- i. Fail log sistem pengoperasian; ii. Fail log servis (web, emel); iii. Fail log aplikasi (*audit trails*); iv. Fail log rangkaian (*switch*, *firewall* dan sebagainya); dan v. Fail log backup.	Pentadbir Sistem ICT.
080404 Penyelarasan Waktu	
a) Waktu yang berkaitan dengan sistem pemprosesan maklumat di RISDA/KRH atau perkakasan keselamatan ICT perlu diselaraskan kepada satu sumber waktu yang piawai. b) Pentadbir sistem perlu menyemak dan memastikan penyelarasan masa (*clock syncronisation*) mempunyai rekod tarikh dan masa yang selaras waktu piawai;	Pentadbir Sistem ICT.

c) *NTP Server* (*Network Time Protocol Server*) atau menggunakan mana-mana sumber waktu setempat yang mematuhi *Malaysian Standard Time* boleh digunapakai.	
0805 Kawalan Perisian Operasi	
Objektif : Memastikan integriti sistem yang beroperasi.	
080501 Pemasangan Perisian Pada Sistem Operasi	
a) Pengemaskinian perisian operasi, aplikasi dan program *libraries* hanya boleh dilakukan oleh pentadbir terlatih setelah mendapat kelulusan pengurusan. b) Sistem operasi hanya boleh memegang "*executable code*" dan tidak kod pembangunan atau penyusun. c) Penggunaan aplikasi dan sistem operasi hanya boleh dilaksanakan selepas ujian yang terperinci dan diperakui berjaya. d) Setiap konfigurasi ke atas sistem perlu dikawal dan didokumentasikan melalui satu sistem kawalan konfigurasi, konfigurasi hanya boleh dilaksanakan selepas mendapat persetujuan daripada pihak berkaitan. e) Pengurusan rekod konfigurasi hendaklah dilaksanakan secara teratur, disemak secara berkala dan disimpan dengan selamat. f) Satu "*rollback*" strategi harus diadakan sebelum perubahan dilaksanakan. g) Versi perisian perlu disimpan sebagai pelan konfigurasi. h) Versi lama perisian perlu diarkib bersama dengan maklumat dan parameter, prosedur, maklumat konfigurasi terperinci dan perisian yang menyokongnya selama mana data boleh disimpan di dalam arkib (*archive*). i) Capaian kepada kod sumber hendaklah dikawal bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian.	Pentadbir Sistem ICT.
0806 Pengurusan Keterdedahan Teknikal	
Objektif : Memastikan pengurusan keterdedahan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.	
080601 Pengurusan Kelemahan Teknikal	
Kawalan daripada ancaman teknikal ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut :-	Pentadbir Sistem ICT.

a) Organisasi perlu memberi definisi dan tanggungjawab berkaitan pengurusan kelemahan teknikal termasuk pemantauan kelemahan, penilaian risiko kelemahan, *paterning*, *asset tracking* dan tanggungjawab koordinasi. b) Memperoleh maklumat keterdedahan teknikal yang tepat pada masanya ke atas sistem maklumat yang digunakan. c) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi. d) Mengambil langkah kawalan untuk mengatasi risiko berkaitan.	
080602 Kawalan Pemasangan Perisian	
a) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa. b) Selain daripada perisian automasi pejabat yang ditetapkan oleh RISDA, pengguna perlulah mendapatkan kebenaran daripada pemilik aset ICT terlebih dahulu. c) Mengimbas semua perisian, aplikasi atau sistem dengan antivirus sebelum menggunakannya.	Pentadbir Sistem ICT dan pengguna.
0807 Pertimbangan Pelaksanaan Audit Sistem Maklumat	
Objektif : Untuk meminimakan impak aktiviti audit terhadap sistem pengoperasian.	
080701 Pematuhan Keperluan Audit dan Kawalan Audit Sistem Maklumat	
a) Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. b) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlakunya gangguan dalam penyediaan perkhidmatan. c) Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan. d) Pelaksanaan audit keatas sistem pengoperasian dilaksanakan sekurang-kurangnya setahun sekali atau bertakluk kepada keperluan yang ditentukan. e) Ujian audit perlu diberi akses terhad kepada *read only* sahaja pada perisian dan data. f) Pentadbir Sistem ICT perlu mengambil tindakan keatas penemuan audit yang berstatus *critical* dan *high*. g) Semakan audit (audit dalam dan audit luar) perlu bagi memastikan pematuhan kepada peraturan dan polisi yang sedang berkuat kuasa.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT.

h) Audit luar hendaklah dilaksanakan oleh pihak yang tiada kepentingan terhadap RISDA/KRH dan sistem yang diaudit. Juruaudit luar yang dilantik mestilah mempunyai tahap kompetensi yang cukup dan memiliki kelayakan/pensijilan yang diiktiraf oleh kerajaan Malaysia.	
080702 Pengauditan dan Forensik ICT	
ICTSO bersama Jawatankuasa Tindak Balas Insiden Keselamatan Siber RISDA mestilah bertanggungjawab merekodkan dan menganalisis perkara-perkara berikut :- a) Sebarang percubaan pencerobohan kepada sistem ICT RISDA. b) Serangan kod perosak(*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phishing*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*). c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan. e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan. f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian. g) Aktiviti penyalahgunaan akaun e-mel. h) Aktiviti penukaran alamat IP *dynamic* kepada *static* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT. i) Merujuk kepada Makmal Forensik Digital (MyDFLab), Jabatan Digital Negara atau lain-lain pihak yang membekal perkhidmatan/kemudahan yang boleh memberikan bantuan teknikal dan kepakaran dalam bidang forensik digital seperti forensik komputer, forensik peranti mudah alih serta pemulihan data (mengekstrak data).	ICTSO.
0808 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut :- a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan. b) Menyedia dan memantapkan keselamatan sistem dokumentasi. c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Semua.

d) Setiap dokumen yang dihasilkan oleh pihak ketiga haruslah dikawal dari segi penyataan penafian (*statement of disclaimer*), Hak Cipta (*Copyright*) dan Hak Pemilikan Data (*Data Ownership*), bagi memastikan tiada penyalahgunaan informasi, ketirisan rahsia dan kehilangan integriti terhadap data-data milik RISDA atau KRH.	
0809 Pengurusan Pertukaran Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi. b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara RISDA atau KRH dengan agensi luar. c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari RISDA atau KRH. d) Maklumat yang terdapat dalam e-mel perlu dilindungi dengan sebaik-baiknya. e) Pemilik dokumen perlu memastikan maklumat asal pemilik fail dokumen yang ingin dikongsi kepada umum, khususnya fail dokumen yang akan dimuatnaik ke laman web, portal, sistem atau aplikasi yang dicapai secara terbuka, adalah dipadam (*Remove Properties and Personal Information*) terlebih dahulu sebelum membuat tindakan muatnaik fail dokumen tersebut. Tindakan ini adalah untuk mengelakkan sebarang kebocoran maklumat yang tidak sepatutnya diketahui pihak umum.	Semua.

BIDANG 09 PENGURUSAN KOMUNIKASI

0901 Pengurusan Keselamatan Rangkaian

090101 Kawalan Infrastruktur Rangkaian

090102 Keselamatan Perkhidmatan Rangkaian

090103 Pengasingan Rangkaian

0902 Pemindahan Maklumat

090201 Polisi dan Prosedur Pemindahan Maklumat

090202 Perjanjian Mengenai Pemindahan Maklumat

090203 Pengurusan Mel Elektronik (E-mel)

090204 Kerahsiaan dan *Non-Disclosure Agreement*

090205 Perkhidmatan Atas Talian dan e-Dagang

090206 Maklumat Umum

090207 Perkomputeran Awan (*Cloud Computing*)

090208 Penghantaran Mesej Segera (*Instant Messaging*)

090209 Media Sosial

BIDANG 09
PENGURUSAN KOMUNIKASI

0901 Pengurusan Keselamatan Rangkaian

Objektif : Memastikan perlindungan maklumat dalam rangkaian dan fasiliti yang membantu pemprosesan maklumat.

090101 Kawalan Infrastruktur Rangkaian

Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti berikut :- a) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan. b) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk. c) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. d) Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check (*FAC*)* semasa pemasangan dan konfigurasi. e) *Firewall* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian. f) Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan RISDA/ KRH. g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran daripada ICTSO. h) Memasang perisian *Intrusion Prevention System (*IPS*)* bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat RISDA. i) Memasang *Web Content Filtering* pada *Internet Gateway* bagi menyekat aktiviti yang dilarang. j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan RISDA/KRH adalah tidak dibenarkan. k) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di jabatan sahaja dan penggunaan *modem* persendirian adalah dilarang sama sekali. l) Kemudahan bagi *wireless LAN* hendaklah dipantau dan dikawal penggunaannya. m) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja.	Pentadbir Sistem ICT.

n) Mengawal capaian fizikal dan logikal ke atas kemudahan *port* diagnostik dan konfigurasi jarak jauh. o) Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan di RISDA dan KRH.	
090102 Keselamatan Perkhidmatan Rangkaian	
Semua perkhidmatan rangkaian yang disediakan secara *inhouse* atau *outsourced* perlu dikenal pasti mekanisme keselamatan, pengurusan dan tahap perkhidmatan serta perlu dimasukkan dalam perjanjian perkhidmatan rangkaian.	Pentadbir Sistem ICT.
090103 Pengasingan Rangkaian	
Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian di jabatan.	Pentadbir Sistem ICT.
0902 Pemindahan Maklumat	
Objektif : Menjamin keselamatan perpindahan/pertukaran maklumat dan perisian antara RISDA dengan pihak luar terjamin.	
090201 Polisi dan Prosedur Pemindahan Maklumat	
Perkara berkaitan dasar dan prosedur pemindahan maklumat yang perlu dipatuhi adalah seperti berikut :- a) Dasar, prosedur dan kawalan pemindahan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan maklumat melalui sebarang jenis kemudahan komunikasi. b) Terma pemindahan maklumat dan perisian antara RISDA/KRH dengan pihak luar hendaklah dimasukkan dalam kontrak. c) Media yang mengandungi maklumat perlu dilindungi daripada semua pengguna, Pentadbir Rangkaian, Pentadbir E-mel dan capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan maklumat. d) Memastikan maklumat yang terdapat dalam e-mel hendaklah dilindungi sebaik-baiknya.	Semua.

090202 Perjanjian Mengenai Pemindahan Maklumat	
Pihak RISDA dan KRH perlu mengambil kira keselamatan maklumat organisasi atau menandatangani perjanjian bertulis apabila berlaku pemindahan maklumat organisasi antara jabatan dengan pihak luar. Perkara yang perlu dipertimbangkan adalah :- a) Tanggungjawab pengurusan bagi mengawal penghantaran dan penerimaan maklumat organisasi. b) Prosedur bagi pengesanan maklumat organisasi semasa pemindahan maklumat. c) Tanggungjawab dan liabiliti sekiranya berlaku insiden keselamatan maklumat seperti kehilangan data.	Pengurus ICT dan ICTSO.
090203 Pengurusan Mel Elektronik (E-mel)	
Penggunaan e-mel di RISDA dan KRH hendaklah dipantau secara berterusan oleh Pentadbir E-mel yang dilantik untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan" dan mana-mana undang-undang bertulis/peraturan yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut :- a) Akaun atau alamat e-mel yang diperuntukkan oleh jabatan sahaja boleh digunakan. Penggunaan akaun milik orang lain adalah dilarang. b) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan. c) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul. d) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu dan saiz fail tidak melebihi saiz yang ditetapkan, kaedah pemampatan untuk mengurangkan saiz adalah disarankan. e) Sekiranya pengguna ingin membuat penghantaran fail bersaiz besar, pengguna boleh menggunakan *tools* dan kemudahan yang dibenarkan sahaja. f) Pengguna hendaklah mengelak daripada membuka e-mel daripada penghantar yang tidak diketahui atau diragui. g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel.	Semua.

h) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail/dokumen elektronik yang telah ditetapkan. i) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan. j) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat. k) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera. l) Pengguna hendaklah memastikan alamat e-mel persendirian (Contoh: Gmail dan sebagainya) tidak digunakan untuk tujuan rasmi. m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan e-mel masing-masing. n) Penggunaan kemudahan e-mel adalah untuk tujuan perkhidmatan rasmi sahaja. o) Semua pihak bertanggungjawab sepenuhnya terhadap kandungan e-mel dalam akaun masing-masing. p) Kelayakan kakitangan untuk mendapat akaun e-mel sesuai dengan jawatan dan mengikut polisi semasa. Sebarang perubahan status penggunaan (bertukar keluar atau berhenti) hendaklah dimaklumkan kepada Pentadbir E-mel. q) Penghantaran maklumat terperingkat melalui Internet mestilah menggunakan kaedah penyulitan yang dibenarkan. r) Kenyataan penafian (*disclaimer*) perlu diletakkan dalam setiap mesej e-mel rasmi.	
090204 Kerahsiaan dan *Non-Disclosure Agreement*	
Syarat-syarat perjanjian kerahsiaan atau *Non-Disclosure Agreement* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan dari semasa ke semasa.	Pengurus ICT, ICTSO dan pembekal.
090205 Perkhidmatan Atas Talian dan e-Dagang	
Bagi menggalakkan pertumbuhan perkhidmatan atas talian serta e-Dagang sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Maklumat yang terlibat dalam perkhidmatan atas talian dan e-Dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan.	Semua.

b) Maklumat yang terlibat dalam transaksi dalam talian (*online*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan. c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	
090206 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti yang berikut :- a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisma yang bersesuaian. b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu. c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web/portal rasmi.	Semua.
090207 Perkomputeran Awan (*Cloud Computing*)	
Pengkomputeran awan adalah perkhidmatan sumber-sumber ICT yang dimayakan tanpa penyediaan infrastruktur di pihak pengguna. Perkomputeran awan menyediakan medium penyimpanan, capaian dan perkongsian maklumat seperti dokumen, gambar, audio atau video dengan menggunapakai kemudahan Internet. Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut :- a) Setiap dokumen rasmi hanya dibenarkan disimpan di storan awan RISDA atau KRH (*private cloud*) yang diluluskan oleh Pengurus ICT. b) Dokumen rasmi dan dokumen terperingkat tidak boleh dimuat naik dalam storan awan awam komersial/percuma. c) Setiap dokumen yang disimpan atau dikongsikan di atas talian haruslah ditetapkan kata laluan untuk membuka dokumen. d) Memastikan perkongsian fail dan dan *folder* hanya dibuat kepada pengguna yang dibenarkan sahaja. e) Memastikan kandungan storan awan yang disediakan oleh jabatan diurus dengan baik dan dibuat *housekeeping* dari semasa ke semasa.	Semua

f) Pengguna RISDA dan KRH perlu mendapat kelulusan Pengurus ICT untuk mencapai *private cloud storage* yang disediakan oleh Bahagian/Jabatan Teknologi Maklumat.	
090208 Penghantaran Mesej Segera (*Instant Messaging*)	
Kawalan keselamatan dan perlindungan bagi teknologi mesej segera adalah meliputi tindakan mengurus aktiviti penyediaan, penyimpanan dan pengedaran maklumat melalui mesej segera secara teratur bagi melindungi data dan maklumat tersebut daripada pengubahsuaian, pemindahan atau pemusnahan tanpa izin. Pengurusan penggunaan mesej segera (Contoh: Whatsapp, Twitter, Telegram dan sebagainya) hendaklah dilaksanakan selaras dengan peraturan yang berkuatkuasa merangkumi perkara-perkara seperti yang berikut :- a) Memantau penggunaan dan penghantaran mesej segera secara berterusan. b) Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang. c) Menetapkan had penggunaan telefon bimbit atau lain-lain peralatan komunikasi yang boleh merakam, menyimpan dan memindahkan maklumat rahsia rasmi yang dibincangkan dalam mesyuarat di jabatan. Perincian garis panduan terperinci boleh dirujuk pada Surat Pekeliling Bahagian Pentadbiran Bilangan 2 Tahun 2019 - Larangan Penggunaan Telefon Bimbit dan Lain-Lain Peralatan Komunikasi Dalam Mesyuarat Kerajaan atau lain-lain surat pekeliling yang sedang berkuat kuasa.	Semua
090209 Media Sosial	
Kawalan keselamatan dan perlindungan bagi penggunaan media sosial (Contoh: Facebook, Instagram, YouTube, TikTok dan sebagainya) meliputi tindakan mengurus aktiviti penyebaran dan perkongsian maklumat melalui media sosial hendaklah dilaksana secara teratur bagi mengawal dan mengelakkan isu salah laku dan penyebaran maklumat tidak beretika di media sosial. Tanggungjawab pengurusan media sosial hendaklah dilaksanakan selaras dengan peraturan yang berkuatkuasa merangkumi perkara-perkara seperti yang berikut :- a) Memantau penggunaan media sosial secara berterusan selaras dengan etika penggunaan Internet di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Organisasi-Organisasi Kerajaan".	Semua

b) Memastikan sebarang bentuk maklumat yang dikongsi dan disebar tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara.

c) Memastikan sebarang bentuk maklumat yang dikongsi dan disebar tidak melibatkan penyebaran maklumat dan dokumen terperingkat.

d) Memastikan sebarang bentuk maklumat yang dikongsi dan disebar tidak memaparkan kenyataan yang boleh menjejaskan imej kerajaan.

e) Memastikan sebarang bentuk maklumat yang dikongsi dan disebar tidak menyentuh isu sensitif seperti agama, politik dan perkauman.

f) Memastikan sebarang bentuk maklumat yang dikongsi dan disebar tidak memaparkan kenyataan yang berunsur fitnah atau hasutan.

g) Tidak menyebarkan maklumat yang berunsur provokasi kepada sesuatu isu yang menyalahi peraturan, undang-undang atau mana-mana perkara yang boleh menyentuh sensitiviti individu atau kumpulan tertentu.

h) Tidak menggunakan saluran media sosial hingga boleh mengganggu fokus dalam urusan kerja.

i) Identiti pentadbir media sosial hendaklah dilindungi daripada pengetahuan pihak luar.

j) Pentadbir media sosial harus mengelakkan untuk membuat pengemaskinian kandungan media sosial di luar pejabat.

BIDANG 10	PEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM

1001 Keperluan Keselamatan Sistem Maklumat

100101 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat

100102 Keselamatan Perkhidmatan Aplikasi di Rangkaian Umum

100103 Melindungi Perkhidmatan Transaksi Aplikasi

1002 Keselamatan Dalam Pembangunan Sistem

100201 Dasar Keselamatan Dalam Pembangunan Sistem

100202 Prosedur Kawalan Perubahan Sistem

100203 Kajian Teknikal Selepas Permohonan Perubahan Platform

100204 Sekatan Perubahan Pakej Perisian

100205 Prinsip Kejuruteraan Keselamatan Sistem

100206 Kod Selamat (*Secure Coding*)

100207 Keselamatan Persekitaran Pembangunan Sistem

100208 Pembangunan Sistem Secara *Outsource*

100209 Pengujian Keselamatan Sistem

100210 Penerimaan Pengujian Sistem

1003 Data Ujian

100301 Perlindungan Data Ujian

BIDANG 10
PEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM

1001 Keperluan Keselamatan Sistem Maklumat

Objektif : Memastikan sistem aplikasi yang dibangunkan secara dalam atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian. Hal ini juga rangkumi keperluan keselamatan maklumat apabila menggunakan rangkaian luar.

100101 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat

Perkara-perkara berkaitan analisis keperluan dan spesifikasi keselamatan maklumat yang perlu dipatuhi adalah seperti berikut :- a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat. b) Ujian keselamatan hendaklah dijalankan ke atas input sistem untuk menyemak pengesahan dan integriti data yang dimasukkan, pemprosesan sistem untuk menentukan sama ada program berjalan betul serta sempurna dan ujian output sistem adalah untuk memastikan data yang telah diproses adalah tepat. c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan. d) Semua sistem yang dibangunkan sama ada secara dalaman atau luaran hendaklah diuji bagi memastikan sistem berkenaan memenuhi keperluan. e) Pembangunan aplikasi mudah alih yang melibatkan integrasi dengan sistem utama hendaklah menggunakan *Application Pogramming Interface (*API*)* atau lain-lain kaedah bersesuaian yang tidak memberi risiko ancaman keselamatan maklumat.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO.

100102 Keselamatan Perkhidmatan Aplikasi di Rangkaian Umum

Maklumat aplikasi yang melalui rangkaian umum (*public networks*) hendaklah dilindungi daripada aktiviti penipuan dan pendedahan maklumat yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti berikut :- a) Tahap kerahsiaan bagi mengenal pasti identiti pengguna, misalnya melalui pengesahan (*authentication*).	Pemilik Sistem, Pentadbir Sistem ICT dan pengguna.

b) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi. c) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan perkhidmatan ICT. d) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	
100103 Melindungi Perkhidmatan Transaksi Aplikasi	
Maklumat yang terlibat dalam perkhidmatan transaksi hendaklah dilindungi daripada penghantaran yang tidak lengkap, *mis-routing*, pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan dan duplikasi mesej. Perkara yang perlu dipertimbangkan adalah seperti berikut :- a) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi. b) Memastikan semua aspek transaksi dipatuhi :- i. Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan. ii. Mengekalkan kerahsiaan maklumat. iii. Mengekalkan privasi pihak yang terlibat. iv. Komunikasi antara semua pihak yang terlibat dirahsiakan. v. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi. c) Pihak yang mengeluar dan mengekalkan pensijilan digital atau tandatangan adalah dilantik oleh kerajaan.	Pemilik Sistem, Pembangun Sistem dan Pentadbir Sistem ICT.
1002 Keselamatan Dalam Pembangunan Sistem	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.	
100201 Dasar Keselamatan Dalam Pembangunan Sistem	
Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan selaras dengan perkembangan dan perubahan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti berikut :- a) Keselamatan persekitaran pembangunan meliputi proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang telah diberi kuasa dan mengikut prosedur yang telah ditetapkan.	Pemilik Sistem, Pembangun Sistem dan Pentadbir Sistem ICT.

b) Keperluan keselamatan dalam fasa rekabentuk sistem dan pangkalan data. c) Mengadakan titik semakan keselamatan di dalam jadual perbatuan projek pembangunan sistem maklumat. d) Kod atau aturcara program yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji. e) Mengamalkan kaedah penulisan kod pengaturcaraan dengan teknik pengaturcaraan yang selamat dan berupaya mengurangkan risiko kelemahan aspek keselamatan sistem. f) Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian. g) Keselamatan dalam kawalan versi fail, kod program, dokumen dan sebagainya. h) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal. i) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	
100202 Prosedur Kawalan Perubahan Sistem	
Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti berikut :- a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, didokumentasi dan disahkan sebelum diguna pakai. b) Setiap perubahan kepada sistem pengoperasian perlu dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap operasi dan keselamatan agensi. c) Kawalan perlu dibuat ke atas sebarang perubahan atau pindaan ke atas sistem bagi memastikan ianya terhad mengikut keperluan sahaja. d) Akses kepada kod sumber aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja. e) Menghalang sebarang peluang untuk membocorkan maklumat. f) Sebarang cadangan perubahan konfigurasi sistem ICT hendaklah dinilai impaknya daripada segi keselamatan sebelum ianya dilaksanakan. Sebarang perubahan konfigurasi sistem ICT yang diterima hendaklah didokumenkan. g) Sekiranya sesuatu perubahan melibatkan aplikasi kritikal, seseorang pegawai atau satu kumpulan tertentu perlu diberikan tanggungjawab untuk memantau aktiviti penambahbaikan dan pembetulan yang dilakukan.	Pemilik Sistem, Pembangun Sistem dan Pentadbir Sistem ICT.

100203 Kajian Teknikal Selepas Permohonan Perubahan Platform	
Perkara yang perlu dipatuhi adalah seperti berikut :- a) Kawalan aplikasi dan prosedur integriti disemak untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform. b) Perubahan platform dimaklumkan dari semasa ke semasa bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan. c) Memastikan perubahan yang sesuai dibuat kepada Pelan Kesinambungan Perkhidmatan RISDA serta lain-lain pelan yang setara.	Pengurus ICT, ICTSO, Pemilik Sistem, Pembangun Sistem dan Pentadbir Sistem ICT.
100204 Sekatan Perubahan Pakej Perisian	
Perubahan kepada pakej perisian adalah tidak digalakkan tetapi terhad kepada perubahan yang diperlukan dan semua perubahan hendaklah dikawal dengan ketat.	Pengurus ICT, ICTSO, Pemilik Sistem, Pembangun Sistem dan Pentadbir Sistem ICT.
100205 Prinsip Kejuruteraan Keselamatan Sistem	
a) Keselamatan perlu diambil kira dalam semua peringkat pembangunan sistem. Prinsip dan prosedur keselamatan ICT hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan keselamatan maklumat. b) Garis panduan yang disediakan oleh kerajaan seperti Garis Panduan dan Pelaksanaan *Independent Verification and Validation (*IV&V*)* boleh dirujuk sebagai panduan.	Pengurus ICT, Pemilik Sistem, Pembangun Sistem dan Pentadbir Sistem ICT.
100206 Kod Selamat (*Secure Coding*)	
a) Perisian dan aplikasi yang akan digunakan di jabatan perlu dibangunkan dengan selamat bagi mengurangkan potensi kerentanan (*vulnerability*) keselamatan maklumat di dalam aplikasi tersebut. b) Pasukan pembangun aplikasi perlu mengamalkan teknik *secure coding* dimana prinsip merangka kod yang mematuhi amalan terbaik keselamatan kod, melindungi dan memelihara kod yang diterbitkan dari kerentanan yang diketahui, tidak diketahui dan tidak dijangka.	Pembangun Sistem dan Pentadbir Sistem ICT.

100207 Keselamatan Persekitaran Pembangunan Sistem	
Persekitaran pembangunan sistem hendaklah selamat bagi melindungi keseluruhan kitaran hayat pembangunan sistem.	Pengurus ICT, Pemilik Sistem, Pembangun Sistem dan Pentadbir Sistem ICT.
100208 Pembangunan Sistem Secara *Outsource*	
a) Pembangunan sistem secara *outsource* perlu sentiasa dikawal selia dan dipantau oleh pemilik sistem. b) Kod sumber bagi semua aplikasi dan perisian adalah menjadi hak milik RISDA/KRH kecuali bagi jenis aplikasi *Commercial Off-The-Shelf* (COTS). c) Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori seperti yang berikut: RISDA dan KRH berhak mencapai kod sumber dan data/maklumat dan RISDA/KRH berhak melaksanakan pengolahan risiko ke atas aplikasi/sistem ICT yang dibangunkan. d) Memastikan sistem ICT yang disediakan kepada RISDA/KRH sentiasa dalam keadaan selamat dan dilindungi dengan mengambil kira keselamatan data-dalam-simpanan (*data-at-rest),* data-dalam-pergerakan (*data-in-motion)* dan data-dalam-penggunaan (*data-in-use).* e) Dokumen kontrak bagi tujuan pengurusan *outsourcing* perlu merangkumi pengakuan kerahsiaan dan integriti maklumat jabatan oleh pihak pembekal/perunding. Pelanggaran perjanjian boleh dikenakan tindakan undang-undang yang berkaitan. f) *Intellectual property rights (*IPR) aplikasi dan perisian yang dibangun oleh pihak ketiga kepada RISDA adalah hak milik RISDA/KRH. g) Adalah amat digalakkan dalam sepanjang tempoh fasa pembangunan aplikasi/sistem ICT, kos penyenggaraan bagi lesen perisian ditanggung oleh pihak pembekal. Perkara ini perlu dipersetuju secara bersama dan boleh dinyatakan dalam klausa kontrak projek. h) Pembekal yang dilantik perlu berkebolehan untuk mengenalpasti dan menambah baik kelemahan aspek keselamatan semasa fasa pembangunan sistem.	Pengurus ICT, ICTSO, Pemilik Sistem, Pembangun Sistem, Pentadbir Sistem ICT dan Pembekal.

100209 Pengujian Keselamatan Sistem	
Pengujian keselamatan sistem hendaklah dijalankan semasa pembangunan. Perkara yang perlu dipatuhi adalah seperti berikut :- a) Semua sistem baharu dan penambahbaikan sistem hendaklah menjalani ujian *Security Posture Assessment (*SPA*)* termasuk penyediaan jadual terperinci aktiviti, ujian input dan output (*input and output validation*). b) Menyemak dan mengesahkan data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat. c) Mengenal pasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam aplikasi. d) Membuat semakan pengesahan dalam aplikasi untuk mengenal pasti sebarang pencemaran maklumat sama ada kerana kesilapan atau disengajakan. e) Menjalankan proses semak ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan dan kesesuaian. f) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan. g) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi. h) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan. i) Rujukan lanjut untuk melaksanakan pengujian sistem boleh dibuat dengan dokumen *ISO/IEC/IEEE 29119 Software Testing Standard* atau lain-lain rujukan yang bersesuaian.	Pemilik Sistem, Pasukan Pembangun Sistem dan Pentadbir Sistem ICT.
100210 Penerimaan Pengujian Sistem	
Perkara yang perlu dipatuhi adalah seperti berikut :- a) Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai. b) Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pemilik Sistem Pembangun Sistem, Pentadbir Sistem ICT dan pengguna.
1003 Data Ujian	
Objektif : Memastikan data ujian direkod dan diuruskan dengan sewajarnya.	
100301 Perlindungan Data Ujian	

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) Perlu dipertimbangkan untuk mengaktifkan audit log bagi merekodkan sebarang penyalinan dan pengguna data sebenar. d) Data dan aturcara program komputer yang hendak diuji perlu dipilih, dilindungi dan dikawal. e) Pengujian hendaklah dibuat ke atas kod aturcara yang terkini. f) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan. g) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian. h) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem, Pembangun Sistem dan Pentadbir Sistem ICT.

BIDANG 11 HUBUNGAN DENGAN PEMBEKAL

1101 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal

110101 Dasar Keselamatan Maklumat Untuk Pembekal

110102 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal

110103 Kawalan Rantaian Bekalan Maklumat dan Komunikasi

1102 Pengurusan Penyampaian Perkhidmatan Pembekal

110201 Pemantauan dan Kajian Perkhidmatan Pembekal

110202 Pengurusan Perubahan Perkhidmatan Pembekal

110203 Mekanisme Kawalan Peralatan Sewaan/Uji Cuba (*Proof of Concept*)

BIDANG 11
HUBUNGAN DENGAN PEMBEKAL

1101 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal

Objektif : Memastikan perlindungan aset ICT RISDA yang boleh diakses oleh pembekal.

110101 Dasar Keselamatan Maklumat Untuk Pembekal

Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan bersama pembekal bagi mengurangkan risiko terhadap aset ICT jabatan. Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut :- a) Mengenalpasti dan mendokumenkan senarai pembekal (seperti perkhidmatan ICT, pembekal infrastruktur ICT, logistik, kewangan dan sebagainya). b) Penekanan aspek keselamatan maklumat dalam projek-projek RISDA boleh diberikan pemakluman kepada pembekal seawal diperingkat taklimat tapak atau di mana-mana perbincangan awal yang dibuat bersama pasukan pembekal. c) Syarikat pembekal yang dilantik perlu mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam kod-kod bidang yang berkaitan. d) Syarikat pembekal yang mempunyai pensijilan keselamatan maklumat yang berkaitan hendaklah lebih mendapat keutamaan untuk terlibat dalam melaksanakan kerja dan memberi perkhidmatan. e) Mewujudkan mekanisma/proses pelantikan dan pengurusan pembekal dengan mengambil kira aspek keselamatan maklumat sebagai teras. f) Mewujudkan kontrak rasmi bersama pembekal yang dapat menjamin keselamatan maklumat jabatan disamping segala urusan bersama pembekal hendaklah dilaksanakan secara rasmi. g) Mewujudkan perjanjian yang jelas agar pihak pembekal memastikan keselamatan maklumat yang digunakan terjamin sepanjang akses dibenarkan dan selepas tamat kontrak seterusnya memulangkan kembali semua aset maklumat sekiranya kontrak mereka tamat atau ditamatkan. h) Mengenalpasti jenis aset maklumat yang dibenarkan untuk diakses oleh pembekal serta melakukan pemantauan dan pengawalan terhadap aset tersebut secara berterusan. i) Mengadakan latihan kesedaran kepada semua pihak yang terlibat (RISDA, KRH dan pembekal) untuk mendedahkan mereka dengan polisi, proses, dan prosedur berkaitan keselamatan maklumat. j) Memastikan pemantauan berterusan dilakukan terhadap semua pembekal dengan melaksanakan pengukuran prestasi dan pematuhan terhadap garis panduan keselamatan maklumat. Proses dan prosedur berkaitan perlu diwujudkan.	ICTSO dan pembekal.

k) Produk atau perkhidmatan yang ditawarkan oleh pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi. l) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang ditetapkan oleh RISDA. m) Memastikan pihak pembekal mewujudkan Pelan Kesinambungan Perkhidmatan dan Pelan Pemulihan Bencana (DRP) mereka khususnya jika pembekal menyediakan khidmat yang kritikal kepada RISDA dan KRH.	
110102 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal	
Semua keperluan keselamatan maklumat hendaklah relevan dan dipersetujui dengan setiap pembekal bagi mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur dan maklumat organisasi ICT. Perkara-perkara yang perlu diambil kira seperti berikut :- a) Penerangan maklumat keselamatan. b) Klasifikasi maklumat. c) Keperluan undang-undang dan peraturan. d) Obligasi setiap pihak bagi kawalan akses, pemantauan, pelaporan dan pengauditan. e) Penerimaan peraturan penggunaan maklumat oleh pembekal. f) Kesedaran keselamatan maklumat. g) Tapisan keselamatan pembekal. h) Hak untuk mengaudit pembekal. i) Kewajipan pembekal mematuhi keperluan keselamatan maklumat. j) Menandatangani *Non-Disclosure Agreement (*NDA*).*	Pembekal.
110103 Kawalan Rantaian Bekalan Maklumat dan Komunikasi	
Perjanjian dengan pembekal hendaklah mengambil kira keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan rantaian bekalan maklumat dan komunikasi. Perkara-perkara yang perlu diambil kira adalah seperti berikut :- a) Mengenalpasti keperluan keselamatan maklumat khusus berkaitan dengan perolehan rangkaian pembekal servis ICT dan produk sebagai tambahan kepada keperluan umum keselamatan maklumat berkaitan hubungan pembekal yang telah dikenal pasti. b) Memastikan rangkaian pembekal yang terlibat dalam menyediakan perkhidmatan ICT berkongsi hal berkaitan keselamatan maklumat (polisi, prosedur, proses) kepada setiap aras pembekal termasuk sub-pembekal atau sub-sub-pembekal.	ICTSO dan pembekal.

c) Khusus untuk rangkaian pembekal produk, RISDA dan KRH perlu memastikan pembekal utama berkongsi praktis pembangunan produk RISDA atau KRH di kesemua peringkat pembekal bagi memastikan keselamatan maklumat terjamin. d) Melaksanakan proses pemantauan rangkaian pembekal perkhidmatan ICT dan produk dengan kaedah yang berkesan bagi menjamin keperluan keselamatan maklumat sentiasa dipatuhi. e) Mendapatkan jaminan bahawa komponen produk yang kritikal boleh berfungsi mengikut spesifikasi dan dikesan sumbernya dari rangkaian pembekal yang pelbagai. f) Mewujudkan peraturan yang khusus bagi mengawal perkongsian maklumat dikalangan rangkaian pembekal. g) Mewujudkan mekanisma/proses khusus untuk mengurus rangkaian pembekal perkhidmatan ICT dan produk bagi memastikan keselamatan maklumat terjamin. Mekanisma yang diwujudkan wajar mampu untuk mengurus risiko sekiranya komponen produk yang dibekalkan tidak lagi boleh dibekalkan kerana perubahan trend dan teknologi yang berlaku.	
1102 Pengurusan Penyampaian Perkhidmatan Pembekal	
Objektif : Memastikan perkhidmatan yang diberikan oleh pembekal adalah pada tahap yang yang terbaik dan berkualiti.	
110201 Pemantauan dan Kajian Perkhidmatan Pembekal	
Pihak RISDA dan KRH hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal. Perkara-perkara yang perlu diambil kira adalah seperti berikut :- a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan. b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa. c) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pihak ketiga. d) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	ICTSO dan pembekal.
110202 Pengurusan Perubahan Perkhidmatan Pembekal	
Perkara yang perlu diambil kira adalah seperti berikut :- a) Perubahan dalam perjanjian dengan pembekal.	ICTSO

b) Perubahan yang dilakukan oleh jabatan bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur. c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	dan pembekal.
110203 Mekanisme Kawalan Peralatan Sewaan/Uji Cuba (*Proof of Concept*)	
Sebarang aktiviti *proof of concept* (POC) yang dijalankan perlu mendapat kelulusan Pengurus ICT dengan mengambil kita perkara-perkara yang berikut: a) Penerimaan i. Peralatan atau perisian yang diterima perlu bebas daripada sebarang *malware* (virus, *backdoor* dan *worm*) serta perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT jabatan. ii. Pembekal terlibat perlu memastikan semua syarat keselamatan dipatuhi melibatkan pematuhan kepada Polisi Keselamatan Siber RISDA, Perakuan Akta Rahsia Rasmi 1972 dan Hak Harta Intelek. b) Penyenggaraan i. Capaian melalui rangkaian luar RISDA atau KRH adalah tidak dibenarkan. ii. Aktiviti penyenggaraan adalah di bawah pengawasan pegawai RISDA dan KRH. c) Pemulangan i. Maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (*secured delete*). ii. Memastikan semua maklumat tidak tertinggal pada peralatan/perisian. d) Laporan dan keputusan Hasil penemuan atau laporan POC perlu diserahkan dan dibentangkan kepada pihak jabatan dan tidak dibenarkan untuk disebarkan atau dikongsi dengan mana-mana pihak luar.	Pentadbir Sistem dan pembekal.

BIDANG 12 PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

1201 Pengurusan dan Penambahbaikan Insiden Keselamatan Maklumat

120101 Tanggungjawab dan Prosedur

120102 Mekanisme Pelaporan Insiden

120103 Melaporkan Kelemahan Keselamatan ICT

120104 Penilaian dan Keputusan Mengenai Aktiviti Keselamatan Maklumat

120105 Pengurusan Maklumat Insiden Keselamatan ICT

120106 Pengalaman Insiden Keselamatan Maklumat

120107 Penilaian dan Keputusan Terhadap Insiden Keselamatan ICT

120108 Tindakbalas Terhadap Insiden Keselamatan ICT

1202 Pengurusan Insiden Keselamatan Aset Bukan ICT

BIDANG 12
PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

1201 Pengurusan dan Penambahbaikan Insiden Keselamatan Maklumat

Objektif : Memastikan insiden keselamatan maklumat dikendalikan dengan cepat, teratur dan berkesan bagi meminimumkan kesan insiden dan mengenal pasti komunikasi serta kelemahan apabila berlaku insiden.

120101 Tanggungjawab dan Prosedur

Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat.	Pengurus ICT dan ICTSO.

120102 Mekanisme Pelaporan Insiden

Insiden keselamatan ICT hendaklah dilaporkan kepada ICTSO atau peranan yang setara (KRH) dengan kadar segera. ICTSO boleh melaporkan kepada Pasukan Tindakbalas Kecemasan Komputer Kerajaan (GCERT) sekiranya perlu. Insiden keselamatan ICT adalah termasuk yang berikut :-

Pengurus ICT, ICTSO dan CSIRT RISDA.

a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa.
b) Sistem maklumat disyaki digunakan tanpa kebenaran atau disyaki sedemikian.
c) Kata laluan atau mekanisma kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang.
d) Berlaku kejadian sistem luar biasa seperti kehilangan fail, sistem kerap kali gagal digunakan dan maklumat tidak dapat dihantar.
e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.

Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan siber RISDA seperti di **Lampiran 4**. Prosedur pelaporan insiden keselamatan ICT adalah berdasarkan: -

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

120103 Melaporkan Kelemahan Keselamatan ICT	
Kakitangan dan pembekal yang menggunakan sistem dan perkhidmatan maklumat RISDA dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan ICT kepada ICTSO.	Pengurus ICT, ICTSO dan CSIRT RISDA.
120104 Penilaian dan Keputusan Mengenai Aktiviti Keselamatan Maklumat	
Sebarang aktiviti yang mengancam keselamatan maklumat hendaklah dinilai dan diputuskan sama ada untuk diklasifikasikan sebagai insiden keselamatan maklumat ataupun tidak.	ICTSO.
120105 Pengurusan Maklumat Insiden Keselamatan ICT	
Insiden keselamatan maklumat hendaklah dikendalikan mengikut prosedur yang telah ditetapkan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut :- a) Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti. b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan atau dikenali dengan sistem log. c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan. d) Menyediakan tindakan pemulihan segera. e) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	ICTSO.
120106 Pengalaman Insiden Keselamatan Maklumat	
a) Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. b) Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada jabatan. c) Setiap insiden keselamatan maklumat perlu direkodkan dan dibuat penilaian untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.	ICTSO dan CSIRT RISDA.

120107 Penilaian dan Keputusan Terhadap Insiden Keselamatan ICT	
Insiden keselamatan ICT perlu dinilai dan keputusan perlu dibuat jika pasti insiden tersebut boleh diklasifikasikan sebagai insiden keselamatan maklumat. a) Penilaian perlu dibuat berasaskan skim klasifikasi insiden yang dipersetujui. b) Insiden perlu disusun mengikut kepentingan dan implikasi kepada jabatan. c) Hasil daripada penilaian yang dibuat boleh dipanjangkan kepada GCERT supaya pengesahan atau penilaian semula dapat dilakukan. d) Hasil daripada penilaian juga perlu direkodkan dengan terperinci untuk rujukan masa depan dan penentusahan. e) Tindakan keatas insiden yang dilaporkan akan dibuat berasaskan tahap kritikal sesuatu insiden samada Keutamaan 1 atau Keutamaan 2. **Keutamaan 1 :** • Aktiviti yang berkemungkinan mengancam nyawa atau keselamatan negara. **Keutamaan 2 :** • Pencerobohan atau percubaan menceroboh melalui infrastruktur ICT. • Penyebaran penafian penyampaian perkhidmatan (*Distributed Denial of Service/*DDoS). • Pencerobohan melalui pemalsuan identiti. • Pengubahsuaian laman web, perisian atau mana-mana komponen sistem tanpa pengetahuan, arahan atau persetujuan pihak yang berkenaan. • Gangguan sistem untuk pemprosesan atau penyimpanan data. Sekiranya berlaku insiden di bawah Keutamaan 1, pihak yang perlu dihubungi adalah seperti berikut :- (a) Pasukan Tindakbalas Kecemasan Komputer Kerajaan (GCERT) National Cyber Coordination and Command Centre (NC4) Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara (MKN) Aras LG & G, Blok Barat, Bangunan Perdana Putra, Pusat Pentadbiran Kerajaan Persekutuan, 62502 Putrajaya. E-mel : cert@nc4.gov.my	ICTSO.

(b) *Malaysian Computer Emergency Response Team* (MyCERT) CyberSecurity Malaysia Level 7, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor Darul Ehsan. Cyber999 *Hotline* : 1-300-88-2999 (Waktu Pejabat) Telefon : 019 - 266 5850 (24x7) E-mel : cyber999@cybersecurity.my	
120108 Tindakbalas Terhadap Insiden Keselamatan ICT	
Insiden keselamatan maklumat perlu diberi tindakbalas sewajarnya oleh pihak yang bertanggungjawab mengikut prosedur yang berkaitan. Matlamat utama tindakbalas terhadap insiden keselamatan ICT adalah untuk mengembalikan tahap keselamatan ke paras normal dan seterusnya melaksanakan langkah-langkah perlu pemulihan. Pasukan tindakbalas wajar melaksanakan perkara berikut :- a) Mengumpul bukti secepat yang mungkin selepas kejadian. b) Melaksanakan kajian forensik sekiranya perlu. c) Insiden dimaklumkan kepada pihak yang berkaitan atau perlu tahu pada kadar segera. d) Pelaporan insiden keselamatan siber di jabatan perlu dilaporkan kepada pihak NACSA melalui kemudahan pelaporan insiden keselamatan siber yang disediakan secara atas talian di laman web Agensi Keselamatan Siber Negara di alamat www.nacsa.gov.my e) Semua aktiviti dalam memberi tindakbalas direkod secara sistematik untuk analisis selanjutnya. f) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan tersebut. g) Mengendalikan dengan efektif kelemahan-kelemahan keselamatan maklumat yang diketahui menjadi penyebab atau penyumbang kepada sesuatu insiden berlaku. h) Menyediakan pelan kontigensi/mengaktifkan pelan kesinambunganh perkhidmatan serta mengambil tindakan untuk pemulihan segera. i) Selepas sesuatu insiden ditangani dengan sempurna, penutupan kes secara rasmi perlu dilakukan dengan merekod semua perincian maklumat secara kemas dan teratur.	ICTSO dan CSIRT RISDA.

j) Memaklumkan atau mendapatkan nasihat daripada pihak berkuasa berkaitan sekiranya perlu. k) Analisa pasca insiden wajar dilakukan untuk mengenalpasti punca insiden. l) Dalam mempertingkatkan tahap keberkesanan tindakan tindak balas kecemasan ICT, anggota pasukan CSIRT RISDA digalakkan untuk sentiasa mendapatkan maklumat dan perkembangan tentang ancaman terkini keselamatan ICT dengan merujuk daripada sumber-sumber sokongan lain yang sah seperti Suruhanjaya Komunikasi dan Multimedia Malaysia, CyberSecurity Malaysia, Polis DiRaja Malaysia dan sebagainya.	
1202 Pengurusan Insiden Keselamatan Aset Bukan ICT	
Insiden keselamatan terhadap aset bukan ICT perlu dipantau kerana insiden tersebut boleh menjadi permulaan kepada insiden keselamatan aset ICT. Sekiranya ada berlaku insiden seumpama ini, pengguna yang terlibat harus melapor dan merekodkan kejadian dan kerosakan aset/peralatan bukan ICT kepada pihak pentadbiran jabatan.	Semua.

BIDANG 13 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1301 Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan

130101 Perancangan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan

130102 Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan

130103 Mengkaji, Mengesah dan Menilai Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan

1302 Pertindihan dan Duplikasi

130201 Ketersediaan Kemudahan Pemprosesan Maklumat

BIDANG 13
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1301 Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan

Objektif : Pengurusan kesinambungan perhidmatan adalah bertujuan bagi menjamin operasi perkhidmatan yang melibatkan infrastruktur ICT jabatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pengguna ICT dalaman dan orang awam yang berurusan dengan RISDA dan KRH.

130101 Perancangan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan

Pelan Kesinambungan Perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan bahagian-bahagian yang menggunakan infrastruktur ICT jabatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi RISDA dan KRH. Pelan ini mestilah diluluskan oleh JPICT RISDA dan perkara-perkara berikut perlu diberi perhatian :- a) Mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan. b) Mengenalpasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT di RISDA dan KRH. c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan. d) Mendokumentasikan proses dan prosedur yang telah dipersetujui. e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan. f) Membuat *backup* dan menguji data *backup* (*restore*). g) Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.	CDO, Pengurus ICT, ICTSO, Koordinator PKP dan Jawatankuasa PKP.

130102 Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan

Pelan Kesinambungan Perkhidmatan perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut :- a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan. b) Senarai kakitangan RISDA/KRH dan pembekal berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT.

c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan. d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh. e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh. Salinan Pelan Kesinambungan Perkhidmatan perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan Kesinambungan Perkhidmatan hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes dan pengoperasian untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan ia dibangunkan untuk ICT RISDA. Ujian Pelan Kesinambungan Perkhidmatan hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan kakitangan yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. RISDA dan KRH hendaklah memastikan salinan Pelan Kesinambungan Perkhidmatan sentiasa dikemaskini dan dilindungi seperti di lokasi utama.	
130103 Mengkaji, Mengesah dan Menilai Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
Pengurus ICT perlu mengesahkan Pelan Kesinambungan Perkhidmatan yang dibangunkan boleh digunapakai dan efektif semasa bencana. Pelan Kesinambungan Perkhidmatan perlu dikaji semula dari semasa ke semasa jika terdapat penambahan dalam organisasi, teknikal dan prosedur. Pengurus ICT perlu mengesahkan PKP dengan melaksanakan aktiviti berikut :- a) Membuat latihan dan menguji fungsi PKP, proses, prosedur dan kawalan agar konsisten dengan objektif pelan. b) Membuat latihan dan menguji pengetahuan dalam menguruskan proses, prosedur dan kawalan PKP agar prestasinya konsisten dengan objektif pelan. c) Mengkaji semula kesahihan dan keberkesanan pengukuran apabila terdapat perubahan dalam PKP.	Pengurus ICT, ICTSO, Koordinator PKP dan Pasukan PKP.

1302 Pertindihan dan Duplikasi	
Objektif : Untuk memastikan kebolehsediaan fasiliti prosesan maklumat.	
130201 Ketersediaan Kemudahan Pemprosesan Maklumat	
Untuk memastikan kebolehsediaan fasiliti pemprosesan maklumat ditahap yang tinggi, kaedah pemprosesan bertindan (lebih dari satu lokasi/platform pemprosesan) boleh diwujudkan. Untuk tujuan itu, perkara berikut wajar diberi tumpuan :- a) Pengurus ICT perlu mengenalpasti keperluan kebolehsediaan sistem maklumat (memahami sejauh mana kritikalnya kebolehsediaan sesuatu sistem maklumat). b) Jika kebolehsediaan sistem maklumat tidak dapat dipastikan dengan satu lokasi pemprosesan, maka fasiliti pemprosesan bertindan perlu dipertimbangkan. c) Fasiliti pemprosesan bertindan perlu diuji (*failover test*) bagi memastikan kesiapsediaan menjalankan operasi apabila pemprosesan utama gagal berfungsi. d) Kawalan kesinambungan keselamatan maklumat perlu disahkan berjaya dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan. e) Kewujudan pemprosesan bertindan boleh membawa risiko kepada kewibawaan dan kerahsiaan maklumat dan sistem maklumat. Hal ini perlu diambil kira semasa sesuatu sistem maklumat itu direkabentuk.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT.

BIDANG 14 PEMATUHAN

1401 Pematuhan Terhadap Keperluan Perundangan dan Perjanjian Kontrak

140101 Mengenalpasti Undang-Undang dan Perjanjian Kontrak

140102 Hak Harta Intelek (*Intellectual Property Right*)

140103 Perlindungan Rekod

140104 Privasi dan Perlindungan Maklumat Peribadi

140105 Kawalan Kriptografi

1402 Kajian Keselamatan Maklumat

140201 Kajian Bebas Pihak Ketiga Terhadap Keselamatan Maklumat

140202 Pematuhan Dasar dan Standard Piawaian

140203 Pematuhan Kajian Teknikal

1403 Pengecualian Dasar

BIDANG 14
PEMATUHAN

1401 Pematuhan Terhadap Keperluan Perundangan dan Perjanjian Kontrak

Objektif : Meningkat dan memantapkan tahap keselamatan ICT bagi mengelak daripada pelanggaran undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.

140101 Mengenalpasti Undang-Undang dan Perjanjian Kontrak

Semua keperluan undang-undang, peraturan dan kontrak yang berkaitan dengan RISDA dan KRH perlu ditakrifkan, didokumenkan dan disimpan sehingga tarikh yang sesuai bagi setiap sistem maklumat. Perkara berkaitan perundangan yang perlu diberi perhatian adalah seperti berikut :- a) Setiap pengguna RISDA dan KRH hendaklah membaca, memahami dan mematuhi Polisi Keselamatan Siber RISDA dan undang-undang atau peraturan-peraturan lain berkaitan yang berkuatkuasa. b) Semua perjanjian dan pekeliling berkaitan ICT termasuk maklumat yang disimpan di dalamnya adalah hakmilik kerajaan dan Ketua Jabatan berhak memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. c) Sebarang pengunaan aset ICT selain daripada maksud dan tujuan yang telah ditetapkan adalah merupakan satu penyalahgunaan sumber jabatan. d) Pelanggaran terhadap Polisi Keselamatan Siber RISDA boleh dikenakan tindakan tatatertib. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna ICT :- i. Arahan Keselamatan (Semakan dan Pindaan 2017). ii. Akta Rahsia Rasmi 1972. iii. Surat Pekeliling Perbendaharaan Bilangan 1 Tahun 1991 - Garis Panduan Pelupusan Peralatan Komputer. iv. Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender. v. Surat Pekeliling Perbendaharaan Bilangan 3Tahun 1995 - Peraturan Perolehan Perkhidmatan Perundingan. vi. Akta Tandatangan Digital 1997.	Semua.

vii. Akta Jenayah Komputer 1997.

viii. Akta Hak Cipta (Pindaan) Tahun 1997.

ix. Akta Komunikasi dan Multimedia 1998.

x. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan.

xi. Surat Pekeliling Am Bilangan 2 Tahun 2000 - Peranan Jawatankuasa-Jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK).

xii. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002.

xiii. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan.

xiv. Akta Arkib Negara 2003 (Akta 629).

xv. Garis Panduan Keselamatan MAMPU 2004.

xvi. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network)* di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006.

xvii. Garis Panduan *IT Outsourcing* Agensi-Agensi Sektor Awam, Oktober 2006.

xviii. Arahan Teknologi Maklumat 2007.

xix. Surat Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 - Tatacara Pengurusan Aset Alih Kerajaan.

xx. Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 dalam Sektor Awam.

xxi. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007.

xxv. Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 – Pengurusan Laman Web Agensi Sektor Awam

xxvi. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007.

xxvii. Surat Pekeliling Am Bilangan 3 Tahun 2009 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

xxviii. Perintah-Perintah Am.

xxix. Arahan Perbendaharaan.

xxx. Surat Arahan Ketua Pengarah MAMPU - Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.

xxxi. Dasar Pengurusan Rekod dan Arkib Elektronik, Arkib Negara Malaysia.

xxxii. Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam.

xxxiii. Standard ISO/IEC 27001:2013.

xxxiv. Garis Panduan Keselamatan Perlindungan RISDA.

xxxv. Tatacara Pengurusan Aset RISDA.

xxxvi. Keselamatan Rahsia Rasmi Dalam Persekitaran Teknologi Maklumat Dan Komunikasi (ICT).

xxxvii. Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Penilaian Risiko Keselamatan Maklumat Menggunakan MyRAM App 2.0 di Agensi Sektor Awam.

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

xxxix. Dasar Penerbitan Atas Talian RISDA 2012.

xl. Garis Panduan Sanitasi Media Elektronik Sektor Awam 2018.

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

xliv. Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam oleh NACSA bertarikh 28 Februari 2019. xlv. Surat Pekeliling Bahagian Pentadbiran Bilangan 2 Tahun 2019 – Larangan Penggunaan Telefon Bimbit dan Lain-Lain Peralatan Komunikasi Dalam Mesyuarat Kerajaan. xlvi. Panduan Pengurusan Projek ICT Sektor Awam (PPrISA). xlvii. Garis Panduan dan Pelaksanaan *Independent Verification and Validation (*IV&V*).* xlviii. Panduan Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA). xlix. MyPortfolio. l. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022 li. Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024 lii. Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024	
140102 Hak Harta Intelek (*Intellectual Property Right*)	
RISDA mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat. RISDA dan KRH perlu mematuhi perkara-perkara berikut :- a) Keperluan hakcipta yang berkaitan dengan bahan proprietari, perisian dan rekabentuk perisian atau aplikasi yang dibangunkan oleh RISDA dan KRH. b) Keperluan perlesenan menghadkan penggunaan produk, perisian, rekabentuk dan bahan-bahan lain yang diperolehi oleh RISDA dan KRH. c) Pihak RISDA dan KRH perlu memastikan pematuhan berterusan dengan sekatan hakcipta produk dan keperluan perlesenan. d) Pengguna tidak dibenarkan daripada menggunakan kemudahan pemprosesan maklumat bagi tujuan selain daripada tugas rasmi atau tugas yang diarahkan.	Semua.

140103 Perlindungan Rekod	
Rekod-rekod yang penting (fizikal atau media) hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, pelepasan yang tidak dibenarkan mengikut undang-undang, peraturan, kontrak dan keperluan perniagaan. Perkara yang perlu diberikan pertimbangan sewajarnya adalah :- a) Pengekalan, penyimpanan, pengendalian dan pelupusan rekod dan maklumat. b) Jadual penyimpanan rekod perlu dikenal pasti. c) Inventori rekod.	Semua.
140104 Privasi dan Perlindungan Maklumat Peribadi	
Pihak RISDA dan KRH perlu mengenal pasti privasi dan melindungi maklumat peribadi penguna seperti yang tertakluk dalam Undang-Undang Kerajaan Malaysia dan peraturan-peraturan yang berkenaan.	Semua.
140105 Kawalan Kriptografi	
Kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang dan peraturan-peraturan. Perkara yang perlu dipatuhi adalah seperti berikut :- a) Penggunaan enkripsi terhadap penghantaran dokumen dan maklumat terperingkat oleh semua pengguna yang berkaitan. b) Kaedah akses oleh RISDA dan KRH terhadap maklumat enkripsi bagi perkakasan dan perisian.	Semua.
1402 Kajian Keselamatan Maklumat	
Objektif : Bagi memastikan keselamatan maklumat dilaksanakan dan beroperasi bersama-sama polisi dan prosedur organisasi.	
140201 Kajian Bebas Pihak Ketiga Terhadap Keselamatan Maklumat	
a) Pelaksanaan keselamatan maklumat RISDA dab KRH hendaklah dikaji secara bebas atau oleh pihak ketiga secara berjadual berkala bagi mematuhi standard pelaksanaan keselamatan ICT. Pematuhan kepada keperluan audit juga perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. b) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	CDO.

140202 Pematuhan Dasar dan Standard Piawaian	
Pengurus ICT perlu membuat kajian semula pematuhan dan prosedur pemprosesan maklumat di bawah tanggungjawab mereka dengan polisi keselamatan siber sedia ada dan lain-lain piawaian yang berkenaan. Pengurus ICT perlu mengambil kira akan perkara-perkara berikut :- a) Mengenal pasti punca-punca ketidakpatuhan. b) Menilai keperluan tindakan untuk mencapai pematuhan. c) Melaksanakan tindakan pembetulan yang sewajarnya. d) Mengkaji semula tindakan pembetulan yang diambil untuk mengesahkan keberkesanannya dan mengenal pasti apa-apa kekurangan dan kelemahan.	Pengurus ICT.
140203 Pematuhan Kajian Teknikal	
Sistem maklumat hendaklah dikaji supaya selaras dengan pematuhan dasar dan standard keselamatan maklumat organisasi (Contohnya: *Security Posture Assessment*). Kajian teknikal perlu dilakukan setahun sekali atau mengikut kesesuaian.	Pengurus ICT dan ICTSO.
1403 Pengecualian Dasar	
Polisi Keselamatan Siber RISDA adalah terpakai kepada semua pengguna ICT RISDA, KRH, pembekal, perunding serta pelawat yang berurusan dengan RISDA dan KRH dan tiada pengecualian diberikan.	Semua.

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti cakera padat, pita magnetik, *optical disk, flash disk, CDROM*, *thumb drive* dan sebagainya untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Jalur Lebar
CDO	*Chief Digital Officer*
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
CSIRT	*Cyber Security Incident Response Team* atau Pasukan Tindakbalas Insiden Keselamatan Siber. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan siber di agensi.
COTS	*Commercial Off-The-Shelf*.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
ICT	*Information and Communication Technology (*Teknologi Maklumat dan Komunikasi*).*
ICTSO	*ICT Security Officer* iaitu pegawai yang bertanggungjawab terhadap keselamatan sistem keselamatan ICT.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.

GLOSARI	
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
ISMS	*Information Security Management System* (Sistem Pengurusan Keselamatan Maklumat)
*Intrusion Prevention System (*IPS*)*	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
ISP	*Internet Service Provider*
LAN	Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan *virus, trojan horse, worm, spyware* dan sebagainya.
MODEM	Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
NACSA	*National Cyber Security Agency* (Agensi Keselamatan Siber Negara).
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
PII	*Personal Identifiable Information* (Maklumat Pengenalan Peribadi)
PKP	Pelan Kesinambungan Perkhidmatan (*Business Continuity Management*)
Public-Key	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, *technology infrastructure* (PKI) enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer.

GLOSARI	
SPA	*Security Posture Assessment* (Penilaian tahap keselamatan untuk aset ICT).
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Telecommuting	Menjalankan tugas daripada rumah atau lain-lain lokasi secara *remote*, dimana ada kemudahan saluran komunikasi digital dan capaian maklumat antara kumpulan pegawai.
*Uninterruptible Power Supply (*UPS*)*	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Aturcara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

LAMPIRAN

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER RISDA

Nama (Huruf Besar) :.....

No. Kad Pengenalan :.....

Jawatan :.....

Bahagian/Jabatan :.....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber RISDA; dan

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

Tandatangan :.....

Tarikh :.....

Disahkan oleh,

.....
Pegawai Keselamatan ICT (ICTSO)
b.p. Timbalan Ketua Pengarah (Pengurusan) RISDA

Tarikh : .....

LAMPIRAN 2

NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (hereinafter referred to as "Agreement") is made on this _____day of _____, 20_____by and between :-

COMPANY NAME (Company No. _____), *full company address* (hereinafter referred to as **'the Contractor'**).

Company Name : ……..…..

Address : ……..……..

……...

Fax : ……..…..

And

PIHAK BERKUASA KEMAJUAN PEKEBUN KECIL PERUSAHAAN GETAH, Ibu Pejabat RISDA, Karung Berkunci 11067, Jalan Ampang, 50990 Kuala Lumpur (hereinafter referred to as **'RISDA'**)

Name : _____

Address : _____

: _____

Telephone : _____

Fax : _____

and shall become effective when executed by authorized representatives of both parties. The facts underlying the Agreement are as follows: -

1.0 Both parties wish to enter into discussions for the general purpose of evaluating each other's products, prototypes, designs, systems and/or exploring the potential application of their products, prototypes designs, systems to the various products systems and/or services the other has or will have for both parties' mutual benefit.

2.0 In order to protect the Confidential Information proprietary to each party, both during the term of the relationship and after the expiration or termination thereof, each party, in exchange for the mutual covenants contained herein, agrees as follows:

2.1 It is recognized and understood by both parties that such a relationship may require each to disclose and disseminate to the other various matters of a confidential nature, including reports and relevant data such as maps, diagrams, plans, drawings, statistics and supporting records or materials, but not limited to patents, manufacturing processes, product operations, research developments, trade secrets, business activities and operations, inventions, and engineering concepts, such matters being hereinafter referred to collectively as - '**Confidential Information'**. Confidential Information, in whatever form, shall be so identified as such at the time of disclosure. Any verbal communication believed to be confidential must be reduced to writing by the disclosing party within five (5) working days of the disclosure, notifying the recipient of the nature and extent of Confidential Information so disclosed.

2.2 Both parties shall maintain in strictest confidence and not disclose to any third party or use for any unauthorized purpose, any and all Confidential Information received from the other, or to which either party may have access, through any media of communication. Neither party shall have the right to duplicate, reproduce, copy, distribute, disclose, use or disseminate the other party's Confidential Information except to further the purpose expressed herein. Each document containing Confidential Information which is circulated to employees of the recipient shall not be disclosed to any other party.

2.3 Both parties represent and warrant to each other that they shall take all reasonable precautions to ensure against any breach of confidentiality and will advise their

employees who might have access to such Confidential Information of the confidential nature thereof. No Confidential Information shall be disclosed to any officer, employee or agent of either party who does not have a need for such information.

2.4 Notwithstanding the conclusion of termination of this relationship as described herein, due to cancellation by either party upon written notice to the other or otherwise, each party shall continue to maintain such confidentiality and covenants herein for a period of one (1) year thereafter. Upon termination, all Confidential Information represented in written for or any other media, including but not limited to, papers, documents, designs, manuals, specifications, prototypes, schematics, computer software, or any other materials or models, shall be returned to the party which furnished same, together with any reproductions or copies thereof, upon request.

2.5 Any attempted assignment by one of the parties to this Agreement without the written consent of the other party will be void except to a successor to its entire business.

2.6 Neither party shall be under any obligation to maintain in confidence any portion of the received Confidential Information which :-

2.6.1. is now, or which hereafter, becomes generally known or available; or

2.6.2. is known by either party at the time of receiving such information; or

2.6.3. is furnished to others by the disclosing party without restriction on disclosure; or

2.6.4. is hereafter furnished to either party by a third party, as a matter of right and without restriction on disclosure; or

2.6.5. is independently developed without any breach of this Agreement; or

2.6.6. is required to be disclosed by judicial action after all reasonable legal remedies to maintain such information in secret have been exhausted.

2.7 Both parties assure each other that they will not, without the prior written consent of the other, transmit, directly or indirectly, the Confidential Information received from the other hereunder or any portion thereof to any country outside of the Malaysia.

SIGNATURE SHEET

IN WITNESS WHEREOF, the parties have executed this Agreement as of the month, day and year first above written.

(Authorized representative for *company name*)

By (signature) : _____

Name (printed) : _____

Title : _____

Company : _____

Date : _____

(Authorized representative for RISDA)

By (signature) : _____

Name (printed) : _____

Title : _____

Company : _____

Date : _____

LAMPIRAN 3

TERHAD

LAMPIRAN C

PERAKUAN UNTUK DITANDATANGANI OLEH PEGAWAI AWAM BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [*AKTA 88*]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [*Akta 88*] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

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

Tandatangan : _____

Nama (huruf besar) : _____

No. Kad Pengenalan : _____

Jawatan : _____

Jabatan : _____

Tarikh : _____

Disaksikan oleh

_____

(Tandatangan)

Nama (huruf besar) : _____

No. Kad Pengenalan : _____

Jawatan : _____

Jabatan : _____

Tarikh : _____

Cap Jabatan

TERHAD

LAMPIRAN D

PERAKUAN UNTUK DITANDATANGANI OLEH PEGAWAI AWAM APABILA MENINGGALKAN PERKHIDMATAN KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [*AKTA 88*]

Perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [*Akta 88*] dan saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Dengan ini menjadi satu kesalahan di bawah Akta tersebut bagi saya menyampaikan dengan tiada kebenaran apa-apa rahsia rasmi atau suratan rasmi kepada mana-mana orang lain, sama ada atau tidak orang itu memegang jawatan dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau mana-mana Kerajaan Malaysia, dan sama ada di Malaysia atau di negara luar, sebelum dan selepas saya berhenti memegang jawatan dalam perkhidmatan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia.

Saya mengaku bahawa tidak lagi ada dalam milik saya atau kawalan saya apa-apa perkataan kod rasmi, isyarat timbal, atau kata laluan rasmi yang rahsia, atau apa-apa benda, suratan atau maklumat, anak kunci, lencana, alat meteri, atau cap bagi atau yang dipunyai, atau diguna, dibuat atau diadakan oleh mana-mana jabatan Kerajaan atau oleh mana-mana pihak berkuasa diplomat yang dilantik oleh atau yang bertindak di bawah kuasa Kerajaan Malaysia atau Seri Paduka Baginda Yang di-Pertuan Agong yang tidak dibenarkan berada dalam milikan atau kawalan saya.

Tandatangan :

Nama (huruf besar) :

No. Kad Pengenalan :

Jawatan :

Jabatan :

Tarikh :

Disaksikan oleh _____

(Tandatangan)

Nama (huruf besar) :

No. Kad Pengenalan :

Jawatan :

Jabatan :

Tarikh :

Cap Jabatan

Lampiran E

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Saya faham bahawa segala rahsia rasmi dan suratan rasmi yang saya peroleh semasa berurusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan, bertulis atau dengan cara elektronik kepada sesiapa jua dalam apa-apa bentuk, sama ada dalam masa atau selepas berurusan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila urusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia telah selesai.

Tandatangan : .....

Nama (huruf besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan/Organisasi : .....

Tarikh : .....

Disaksikan oleh

.....

(Tandatangan)

Nama (huruf besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan/Organisai : .....

Tarikh : .....

Cap Jabatan/Organisasi

Lampiran F

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN APABILA TAMAT KONTRAK PERKHIDMATAN DENGAN KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Dengan ini menjadi satu kesalahan di bawah Akta tersebut bagi saya menyampaikan dengan tiada kebenaran apa-apa rahsia rasmi atau suratan rasmi kepada mana-mana orang lain, sama ada atau tidak orang itu memegang jawatan dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau mana-mana Kerajaan Malaysia, dan sama ada di Malaysia atau di negara luar, sebelum dan selepas saya tamat kontrak perkhidmatan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana- mana Kerajaan dalam Malaysia.

Saya mengaku bahawa tidak lagi ada dalam milik saya atau kawalan saya apa-apa perkataan kod rasmi, isyarat timbal, atau kata laluan rasmi yang rahsia, atau apa-apa benda, suratan atau maklumat, anak kunci, lencana, alat meteri, atau cap bagi atau yang dipunyai, atau diguna, dibuat atau diadakan oleh mana-mana jabatan Kerajaan atau oleh mana-mana pihak berkuasa diplomat yang dilantik oleh atau yang bertindak di bawah kuasa Kerajaan Malaysia atau Seri Paduka Baginda Yang di-Pertuan Agong yang tidak dibenarkan berada dalam milikan atau kawalan saya.

Tandatangan :
_____

Nama (huruf besar) :
_____

No. Kad Pengenalan/Passport :
_____

Jawatan :
_____

Jabatan/Organisasi :
_____

Tarikh :
_____

Disaksikan oleh

_____
(Tandatangan)

Nama (huruf besar) :
_____

No. Kad Pengenalan/Passport :
_____

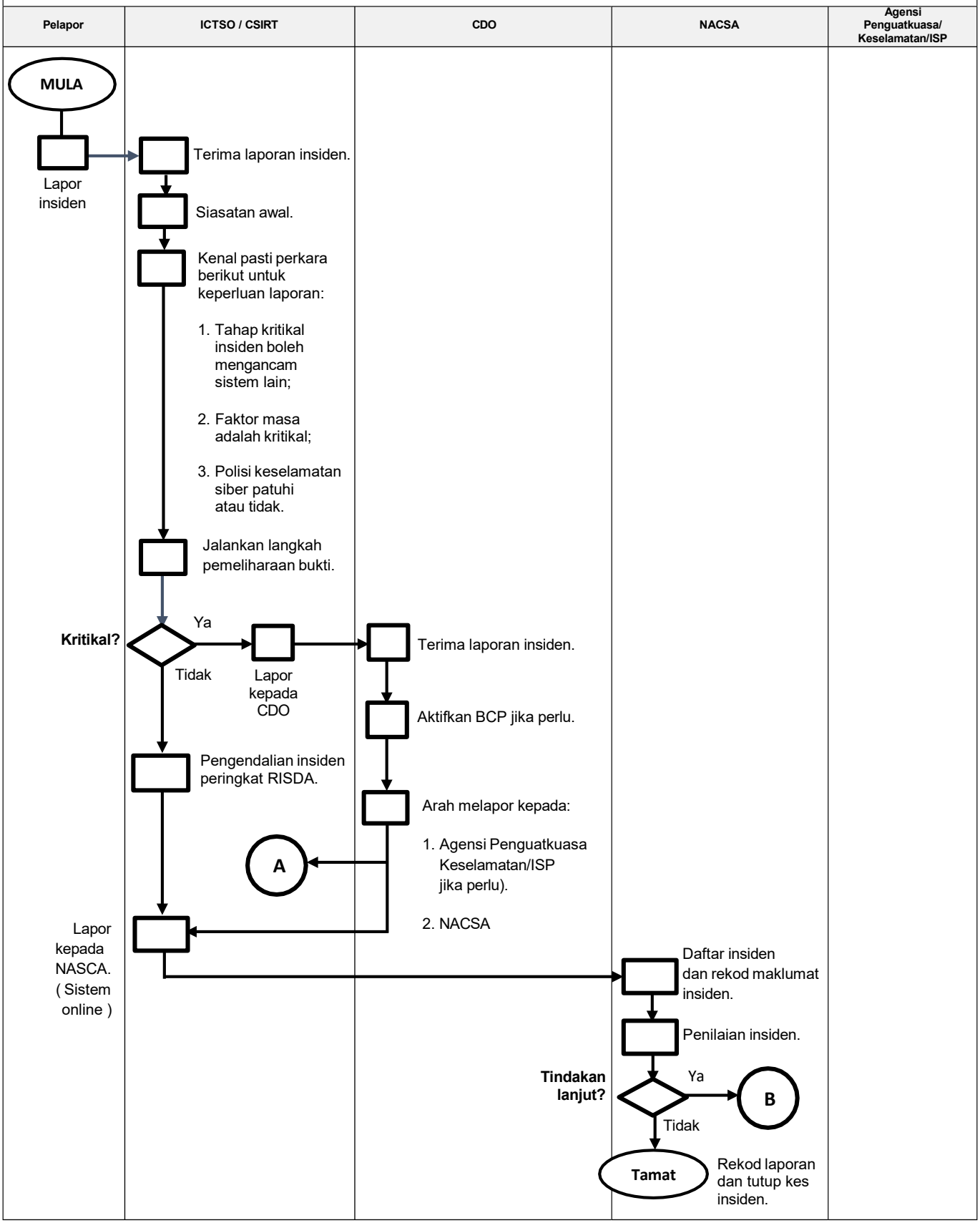
Jawatan :
_____

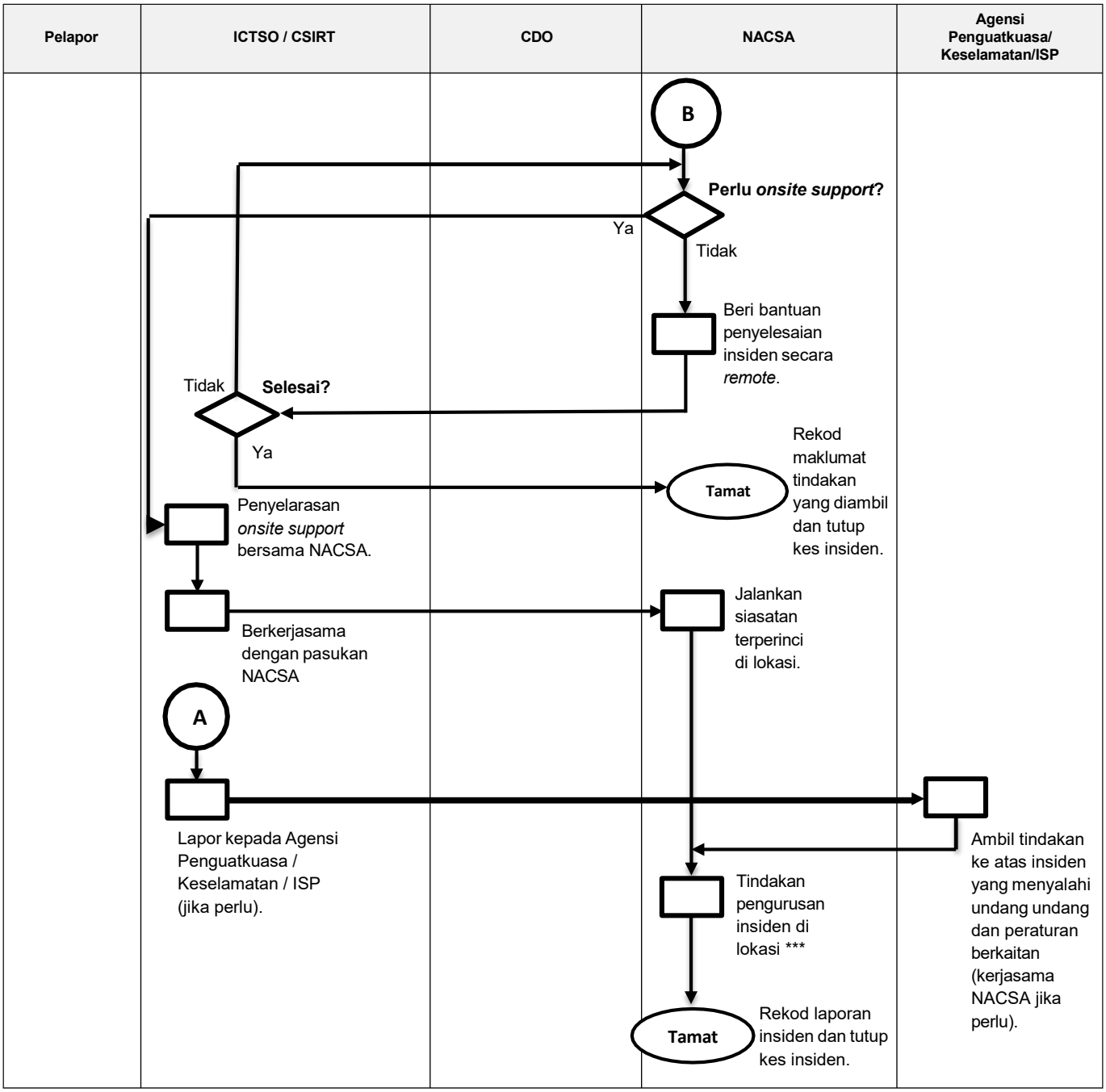
Jabatan/Organisasi :
_____

Tarikh :
_____

Cap Jabatan/Organisasi

RAJAH 1 : RINGKASAN PROSES KERJA PELAPORAN INSIDEN KESELAMATAN SIBER RISDA (LAMPIRAN 4)





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

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


AMALAN BERISIKO BOLEH
MENYEBABKAN KETIRISAN MAKLUMAT
CLOUD
AKSES KE INTERNET MENERUSI RANGKAIAN
WIRELESS YANG TIDAK SELAMAT
Bersama
Hentikan
Wabak
COVID-19
REKABENTUK OLEH BAHAGIAN TEKNOLOGI MAKLUMAT


AMALAN BERISIKO BOLEH
MENYEBABKAN KETIRISAN MAKLUMAT
KEGAGALAN UNTUK MEMADAM MAKLUMAT
SENSITIF ATAU MAKLUMAT TERPERINGKAT
YANG TIDAK PERLU DALAM KOMPUTER
RISDA
Bersama
Hentikan
Wabak
COVID-19
REKABENTUK OLEH BAHAGIAN TEKNOLOGI MAKLUMAT


AMALAN BERISIKO BOLEH
MENYEBABKAN KETIRISAN MAKLUMAT
SHARING
PASSWORD
****
BERKONGSI MAKLUMAT KATALALUAN
DENGAN PIHAK YANG LAIN
Bersama
Hentikan
Wabak
COVID-19
REKABENTUK OLEH BAHAGIAN TEKNOLOGI MAKLUMAT


AMALAN BERISIKO BOLEH
MENYEBABKAN KETIRISAN MAKLUMAT
USERNAME
PASSWORD
MENGGUNAKAN NAMA PENGGUNA DAN KATALALUAN YANG SAMA UNTUK BEBERAPA LAMAN WEB ATAU AKAUN ONLINE YANG SAMA
Bersama Hentikan Wabak COVID-19
REKABENTUK OLEH BAHAGIAN TEKNOLOGI MAKLUMAT


AMALAN BERISIKO BOLEH
MENYEBABKAN KETIRISAN MAKLUMAT
MENGGUNAKAN USB DRIVE TANPA
MEMASANG CIRI ENKRIPSI SEMASA
MENYIMPAN ATAU MEMINDAHKAN
MAKLUMAT TERPERINGKAT
Bersama
Hentikan
Wabak
COVID-19
REKABENTUK OLEH BAHAGIAN TEKNOLOGI MAKLUMAT


AMALAN BERISIKO BOLEH
MENYEBABKAN KETIRISAN MAKLUMAT
MEMBIARKAN KOMPUTER ATAU LAPTOP
TERBIAR APABILA MENINGGALKAN
RUANG KERJA
Bersama
Hentikan
Wabak
COVID-19
REKABENTUK OLEH BAHAGIAN TEKNOLOGI MAKLUMAT

Dokumen Tamat


BAHAGIAN TEKNOLOGI MAKLUMAT