POLISI KESELAMATAN SIBER VERSI 2.0

PIHAK BERKUASA KEMAJUAN PEKEBUN KECIL PERUSAHAAN GETAH

1 FEBRUARI 2026

POLISI KESELAMATAN SIBER

SEJARAH DOKUMEN

TARIKH	VERSI	PEKELILING	TARIKH KUAT KUASA
11 Disember 2023	1.0	Surat Pekeliling Bahagian Teknologi Maklumat Bilangan 3 Tahun 2024	22 April 2024
1 Februari 2026	2.0	Surat Pekeliling Bahagian Teknologi Maklumat Bilangan 1 Tahun 2026	19 Februari 2026

ISI KANDUNGAN

PENGENALAN

Polisi Keselamatan Siber Pihak Berkuasa Kemajuan Pekebun Kecil Perusahaan Getah (RISDA) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) RISDA. Dasar ini juga menerangkan kepada semua pengguna di RISDA mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT RISDA.

OBJEKTIF

Polisi Keselamatan Siber RISDA diwujudkan untuk menjamin kesinambungan urusan RISDA dengan meminimumkan kesan insiden keselamatan ICT.

Polisi ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi RISDA. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Objektif utama Keselamatan ICT RISDA ialah seperti berikut:

(a) Memastikan kelancaran operasi RISDA dan meminimumkan kerosakan atau kemusnahan;
(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;
(c) Mencegah salah guna atau kecurian aset ICT;
(d) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan; dan
(e) Memperkemaskan pengurusan keselamatan ICT RISDA.

PENYATAAN 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 ICT yang bersifat dinamik.

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. Terdapat empat (4) 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; dan
(d) Memastikan akses hanya kepada 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; dan
(e) **Ketersediaan** - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

Aset ICT RISDA 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; dan

(b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan 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 RISDA. Contoh 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 disediakan bagi kemudahan pemprosesan maklumat kepada RISDA;

(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 kawalan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

(d) Data atau Maklumat

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

(e) Manusia

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

(f) Premis Komputer Dan Komunikasi

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

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran maklumat rasmi 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 untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

(b) Hak akses minimum

Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

(c) Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT;

(d) Pengasingan

Tugas mewujud, memadam, mengemas 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;

(e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti 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 penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan; dan

(h) Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

RISDA hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat daripada ancaman dan kerentanan (*vulnerability*) yang semakin meningkat hari ini. Justeru itu RISDA 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.

RISDA 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 RISDA termasuklah aplikasi, perisian, perkakasan, 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 media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

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. RISDA 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 agensi;

(c) Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan

(d) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

PEMBATALAN

Dengan berkuatkuasanya Polisi Keselamatan Siber ini, PKS versi 1.0 bertarikh 11 Disember 2023 adalah dibatalkan.

BIDANG 01: KAWALAN ORGANISASI

0101 Polisi Keselamatan Maklumat

Objektif:

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan RISDA dan perundangan yang berkaitan.

010101 Pelaksanaan Polisi	Tanggungjawab
Pelaksanaan polisi ini akan dipacu oleh Ketua Pengarah RISDA dan diselaras oleh ahli Jawatankuasa Pemandu ICT (JPICT) RISDA yang terdiri daripada Timbalan Ketua Pengarah (Pengurusan) selaku Ketua Pegawai Digital (CDO), Timbalan Ketua Pengarah (Pembangunan), Pengurus ICT, semua Pengarah Bahagian, Pegawai Undang-Undang, Pegawai Keselamatan ICT (ICTSO), dan seorang wakil Kumpulan RISDA Holdings (KRH).	Ketua Pengarah RISDA
010102 Penyebaran Polisi	**Tanggungjawab**
Polisi ini perlu disebar kepada semua pengguna RISDA (termasuk kakitangan, pihak ketiga dan lain-lain).	ICTSO
010103 Penyelenggaraan Polisi	**Tanggungjawab**
Piawaian berhubung dengan penyelenggaraan Polisi Keselamatan Siber RISDA adalah seperti berikut: a. Polisi ini hendaklah dikaji semula sekurang-kurangnya tiga tahun sekali atau mengikut keperluan semasa bagi memastikan dokumen sentiasa dipatuhi; b. Mengemukakan cadangan pindaan secara bertulis, membuat pembentangan dan mendapatkan kelulusan pindaan daripada JPICT RISDA; dan c. Memaklumkan perubahan yang telah dipersetujui oleh JPICT RISDA kepada semua pengguna.	ICTSO
010104 Pengecualian Polisi	**Tanggungjawab**
Polisi Keselamatan Siber RISDA adalah terpakai kepada semua pihak yang terlibat dalam urusan ICT di RISDA dan tiada sebarang pengecualian diberikan.	Warga RISDA dan Pihak Ketiga

0102 Peranan Dan Tanggungjawab Dalam Keselamatan Maklumat	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber RISDA.	
010201 Ketua Pengarah RISDA	**Tanggungjawab**
Peranan dan tanggungjawab Ketua Pengarah RISDA adalah seperti berikut: a. Menetapkan arah tuju dan strategi untuk pelaksanaan keselamatan siber di RISDA; b. Memperuntukkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju dan strategi keselamatan Siber di RISDA; c. Memastikan semua warga RISDA mematuhi Polisi Keselamatan Siber RISDA; d. Memperakui proses pengambilan tindakan tatatertib ke atas warga RISDA yang melanggar Polisi Keselamatan Siber RISDA; e. Melantik CDO dan ICTSO serta memaklumkan pelantikan kepada Ketua Pengarah Jabatan Digital Negara; dan f. Meluluskan dokumen Polisi Keselamatan Siber RISDA.	Ketua Pengarah RISDA
010202 Ketua Pegawai Digital (CDO)	**Tanggungjawab**
Timbalan Ketua Pengarah (Pengurusan) RISDA adalah merupakan Ketua Pegawai Digital (CDO). Peranan dan tanggungjawab CDO adalah seperti berikut: a. Membantu Ketua Pengarah RISDA dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Memperakukan dokumen Polisi Keselamatan Siber RISDA; c. Menentukan keperluan keselamatan ICT;	CDO

d. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; dan e. Bertanggungjawab ke atas perkara-perkara yang berkaitan keselamatan ICT RISDA.	
010203 Pegawai Keselamatan ICT (ICTSO)	**Tanggungjawab**
ICTSO yang dilantik adalah berperanan dan bertanggungjawab seperti berikut: a. Memastikan kajian semula dan pelaksanaan kawalan keselamatan ICT selaras dengan keperluan RISDA; b. Mengurus keseluruhan program-program keselamatan ICT RISDA; c. Menguatkuasakan dan memantau pelaksanaan Polisi Keselamatan Siber RISDA; d. Memberi penerangan dan pendedahan berkenaan Polisi Keselamatan Siber RISDA kepada semua warga RISDA; e. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber RISDA; f. Menjalankan tugas pengurusan risiko; g. Menjalankan audit, kajian semula, merumus tindak balas pengurusan RISDA berdasarkan hasil penemuan dan menyediakan laporan mengenainya; h. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; i. Melaporkan insiden keselamatan ICT kepada Agensi Keselamatan Siber Negara (NACSA) dan memaklumkan kepada CDO; j. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;	ICTSO

k. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; l. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; dan m. Koordinator Pelan Pengurusan Pemulihan Bencana (*DR Coordinator*) RISDA.	
010204 Pentadbir Sistem ICT	**Tanggungjawab**
Pentadbir Sistem ICT adalah terdiri daripada peranan berikut: a. Pengurus ICT b. Pentadbir Sistem Aplikasi c. Pentadbir Pusat Data d. Pentadbir Keselamatan ICT e. Pentadbir Rangkaian ICT f. Pentadbir Pangkalan Data g. Pentadbir Portal (*Webmaster*) h. Pentadbir Media Sosial i. Pentadbir Peralatan ICT j. Pegawai Aset k. *Cybersecurity Incidents Response Team* (CSIRT)	Pentadbir Sistem ICT
010205 Pengurus ICT	**Tanggungjawab**
Pengurus ICT RISDA adalah berperanan dan bertanggungjawab seperti berikut: a. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan PKS; b. Menentukan kawalan akses peralatan dan perisian semua pengguna di RISDA terhadap aset ICT RISDA; dan	Pengurus ICT

c. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT RISDA.	
010206 Pentadbir Sistem Aplikasi	**Tanggungjawab**
Pentadbir Sistem Aplikasi adalah berperanan dan bertanggungjawab seperti berikut: a. Mengkaji cadangan pembangunan, penambahbaikan, pembaikan, penyelarasan, pelaksanaan, pemantauan dan penyelenggaraan sistem di RISDA; b. Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; c. Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya; d. Memastikan bahawa pembangunan sistem aplikasi adalah berpandukan Buku Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA) dan Polisi Keselamatan Siber RISDA; e. Menyediakan dokumentasi sistem dan manual pengguna; f. Menghadkan capaian ke atas dokumentasi sistem bagi mengelakkan dari penyalahgunaannya; dan g. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi Keselamatan Siber RISDA.	Pentadbir Sistem Aplikasi
010207 Pentadbir Pusat Data	**Tanggungjawab**
Pentadbir Pusat Data RISDA adalah berperanan dan bertanggungjawab seperti berikut: a. Memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat; b. Memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data; c. Menjadualkan dan melaksanakan proses *backup* dan *restoration* ke atas pangkalan data dan sistem secara	Pentadbir Pusat Data

berkala; d. Menyediakan perancangan Pelan Pemulihan Bencana; e. Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan; f. Memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa g. Merangka, melaksana dan menguatkuasakan polisi keselamatan ICT seperti perlindungan dan perkongsian data; h. Melaksanakan polisi ancaman keselamatan ICT; dan i. Melaporkan sebarang insiden pelanggaran dasar keselamatan pusat data kepada ICTSO.	
010208 Pentadbir Keselamatan ICT	**Tanggungjawab**
Pentadbir Keselamatan ICT RISDA adalah berperanan dan bertanggungjawab seperti berikut: a. Merangka dan menetapkan polisi berkaitan keselamatan ICT; b. Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT RISDA secara berkala; c. Memastikan konfigurasi peralatan keselamatan ICT dibuat dengan amalan keselamatan terbaik (*security best practices);* d. Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam atau menceroboh; e. Memantau aktiviti capaian warga RISDA secara berkala; f. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta; g. Melaksanakan program dan kempen kesedaran keselamatan ICT untuk pengguna RISDA;	Pentadbir Keselamatan ICT

h. Melaksanakan polisi ancaman keselamatan ICT; dan i. Melaporkan sebarang insiden pelanggaran dasar keselamatan pusat data kepada ICTSO.	
010209 Pentadbir Rangkaian ICT	**Tanggungjawab**
Pentadbir Rangkaian ICT adalah berperanan dan bertanggungjawab seperti berikut: a. Memastikan kerahsiaan akaun pentadbir; b. Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di RISDA beroperasi sepanjang masa; c. Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; d. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; e. Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian JPA secara tidak sah; f. Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian; g. Melaksanakan polisi ancaman keselamatan ICT; dan h. Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian.	Pentadbir Rangkaian ICT
010210 Pentadbir Pangkalan Data	**Tanggungjawab**
Pentadbir pangkalan data bertanggungjawab menentukan keselamatan pangkalan data dengan memastikan: a. Perisian pangkalan data dikemaskini dengan *patches* terkini (bergantung kepada keperluan, kesesuaian dan kelulusan); b. Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur; dan c. Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.	Pentadbir Pangkalan Data

010211 Pentadbir Portal (*Webmaster*)	**Tanggungjawab**
Peranan dan tanggungjawab Pentadbir Portal (*Webmaster*) adalah seperti berikut: a. Menerima kandungan portal yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b. Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar; c. Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai antara muka portal; d. Memastikan reka bentuk portal dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; dan e. Melaporkan sebarang pelanggaran keselamatan portal kepada ICTSO.	Pentadbir Portal (*Webmaster*)
010212 Pentadbir Media Sosial	**Tanggungjawab**
Peranan dan tanggungjawab Pentadbir Media Sosial adalah seperti berikut: a. Mematuhi segala peraturan atau syarat-syarat yang digariskan oleh penyedia platform media sosial; dan b. Mentadbir dan menyemak ketepatan serta sensitiviti maklumat dalam pengurusan kandungan (video, audio, gambar dan dokumen) dan komen mengikut etika media sosial semasa.	Pentadbir Media Sosial
010213 Pentadbir Peralatan ICT	**Tanggungjawab**
Peranan dan tanggungjawab Pentadbir Peralatan ICT adalah seperti berikut: a. Merancang, melaksana dan memastikan pembekalan aset ICT dilaksanakan; dan b. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada warga RISDA seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	Pentadbir Peralatan ICT

010214 Pegawai Aset	Tanggungjawab
Pegawai Aset RISDA ialah pegawai yang dilantik oleh Pegawai Pengawal. Peranan dan tanggungjawab Pegawai Aset adalah seperti berikut: a. Memastikan pengurusan aset ICT dijalankan selaras dengan peraturan yang ditetapkan; b. Memastikan penerimaan aset ICT dilaksanakan oleh pegawai yang dilantik secara bertulis oleh Ketua Jabatan/ Bahagian; c. Memastikan semua aset ICT yang diterima, didaftarkan menggunakan Sistem Pemantauan Pengurusan Aset (SPA) dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset; d. Memastikan semua aset ICT yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan bertulis daripada Ketua Jabatan/Bahagian; e. Memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/ penggantian/ penaiktarafan aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira; f. Memastikan semua aset ICT diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia dan nama RISDA berkenaan 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 mengikut lokasi dan format Senarai Aset ICT dalam dua (2) salinan. Satu (1) senarai berkenaan perlu disimpan oleh Pegawai Aset dan satu (1) salinan perlu dipaparkan oleh pegawai yang bertanggungjawab di lokasi;	Pegawai Aset

j. Memastikan setiap kerosakan aset ICT dilaporkan; k. Bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT; l. Merancang, memantau dan memastikan pemeriksaan asset dilaksanakan ke atas keseluruhan aset ICT sekurang-kurangnya sekali setahun; dan m. Memastikan setiap kes kehilangan aset ICT dilaporkan dan diuruskan dengan teratur.	
010215 CSIRT RISDA	**Tanggungjawab**
Tanggungjawab CSIRT RISDA meliputi semua bidang tugas pengurusan pengendalian insiden keselamatan siber yang dialami oleh RISDA seperti berikut: a. Memantau, mengesan insiden, menerima dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber; b. Merekod dan menjalankan siasatan awal tehadap insiden yang diterima; c. Melaksanakan pengurusan dan pengendalian insiden keselamatan siber serta mengambil tindakan awal pemulihan; d. Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden baharu dapat dielakkan; e. Melaporkan insiden keselamatan siber kepada agensi yang menyelianya dan *National Cyber Coordination and Command Centre* (NC4); f. Menasihat Pengurusan RISDA bagi mengambil tindakan pemulihan dan pengukuhan; g. Menyebarkan makluman/amaran berkaitan insiden kepada semua pihak yang terlibat/berkepentingan; dan h. Memastikan fail log disimpan sekurang-kurangnya bagi tempoh 2 minggu terkini di tempat yang selamat.	CSIRT RISDA

010216 Pegawai Pengelas	**Tanggungjawab**
Tanggungjawab Pegawai Pengelas meliputi: a. Mendaftar dokumen rahsia rasmi kerajaan. b. Mengelas rahsia rasmi kerajaan. c. Pengelasan semula rahsia rasmi kerajaan. d. Memastikan buku daftar rahsia rasmi kerajaan dikawal dan disimpan dengan selamat. e. Memastikan dokumen rahsia rasmi kerajaan yang telah diturun taraf hendaklah dimusnahkan mengikut prosedur.	Pegawai Pengelas
010217 Warga RISDA	**Tanggungjawab**
Warga RISDA mempunyai peranan dan tanggungjawab seperti berikut: a. Membaca, memahami, dan mematuhi Polisi Keselamatan Siber RISDA; b. Mengetahui dan memahami implikasi keselamatan ICT akibat daripada tindakannya; c. Menjalani tapisan keselamatan seperti yang diarahkan (sekiranya berkaitan); d. Melaksanakan dan mematuhi prinsip-prinsip Polisi Keselamatan Siber RISDA serta menjaga kerahsiaan maklumat RISDA; e. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; f. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan g. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber RISDA sebagaimana di Lampiran B dan Perakuan Akta Rahsia Rasmi 1972 sebagaimana di Lampiran C.	Warga RISDA

0103 Pengasingan Tugas dan Tanggungjawab

Objektif:

Mengurangkan risiko penipuan, kesilapan dan pemintasan dalam kawalan keselamatan maklumat.

010301 Keperluan Keselamatan Dalam Pengasingan Tugas	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesah data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan c. Aset ICT yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari aset ICT yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pengurus/ Penyelaras ICT dan Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT, Pentadbir Pangkalan Data

0104 Tanggungjawab Pengurusan

Objektif:

Memastikan pengurusan memahami peranan mereka dalam keselamatan maklumat dan mengambil tindakan yang bertujuan untuk memastikan semua kakitangan menyedari dan memenuhi tanggungjawab dalam keselamatan maklumat RISDA.

010401 Tanggungjawab Pengurusan Terhadap Kakitangan	Tanggungjawab
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan Dasar Keselamatan Maklumat dan Objektif Keselamatan Maklumat dibangunkan dan selaras	Pihak Pengurusan

dengan hala tuju strategik organisasi; b. Memastikan pegawai dan kakitangan RISDA serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan undang-undang dan peraturan yang ditetapkan oleh RISDA; c. Memastikan sumber yang diperlukan untuk pengurusan keselamatan maklumat tersedia; dan d. Menyampaikan kepentingan tentang pengurusan keselamatan maklumat yang berkesan.	

0105 Hubungan Dengan Pihak Berautoriti	
Objektif: Memastikan aliran maklumat berkaitan keselamatan berlaku dengan sewajarnya di antara RISDA dan pihak berautoriti.	
010501 Hubungan Dengan Pihak Berautoriti	**Tanggungjawab**
Perkara-perkara yang perlu dilaksanakan ialah mewujudkan dan mengemaskini senarai pihak berautoriti/pihak yang dihubungi semasa kecemasan yang terdiri daripada: a. Pihak berautoriti termasuklah Polis Diraja Malaysia (PDRM) dan Suruhanjaya Komunikasi dan Multimedia (SKMM). b. Pihak yang dihubungi semasa kecemasan termasuklah tetapi tidak terhad kepada pihak penyedia utiliti, pembekal elektrik, pembekal perkhidmatan dan lain-lain.	CDO, ICTSO, Penyelaras ICT dan Pentadbir Sistem ICT

0106 Hubungan Dengan Pihak Berkepentingan Yang Khusus	
Objektif: Memastikan aliran maklumat berkaitan keselamatan berlaku dengan sewajarnya.	
010601 Hubungan Dengan Pihak Berkepentingan Yang Khusus	**Tanggungjawab**
Hubungan dengan kumpulan berkepentingan yang khusus atau	ICTSO, Pengurus

forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan seperti Agensi Keselamatan Siber Negara (NACSA), Pejabat Ketua Keselamatan Kerajaan (CGSO), Cybersecurity Malaysia dan lain-lain.	ICT dan Pentadbir Sistem ICT

0107 Risikan Ancaman (*Threat Intelligence*)

Objektif:

Memberi kesedaran tentang persekitaran ancaman organisasi supaya tindakan mitigasi yang sewajarnya dapat diambil.

010701 Keperluan Risikan Ancaman	Tanggungjawab
Maklumat mengenai ancaman sedia ada atau baharu hendaklah dikumpulkan daripada sumber luaran dan dalaman, dan dianalisis untuk: a. Memudahkan tindakan sewajarnya diambil untuk mencegah ancaman daripada menyebabkan kemudaratan kepada organisasi; dan b. Mengurangkan kesan ancaman tersebut. Aktiviti perisikan ancaman hendaklah termasuk: a. Mengenal pasti, memeriksa dan memilih sumber maklumat dalaman dan luaran yang diperlukan dan sesuai untuk melaksanakan tindakan yang diperlukan berdasarkan maklumat perisikan ancaman; b. Memproses dan menganalisis maklumat untuk memahami bagaimana ia berkaitan dan bermakna kepada organisasi; dan c. Berkomunikasi dan berkongsi kepada individu yang berkaitan dalam format yang boleh difahami. Perisikan ancaman hendaklah dianalisis dan kemudian digunakan: a. Dengan melaksanakan proses untuk memasukkan maklumat yang dikumpulkan dari sumber perisikan ancaman ke dalam proses pengurusan risiko	ICTSO dan CSIRT RISDA

keselamatan maklumat organisasi; b. Sebagai input tambahan kepada kawalan pencegahan dan pengesanan teknikal seperti firewall, intrusion detection system, atau penyelesaian anti perisian hasad; dan c. Sebagai input kepada proses dan teknik Penilaian Tahap Keselamatan.	

0108 Keselamatan Maklumat Dalam Pengurusan Projek	
Objektif: Memastikan risiko keselamatan maklumat berkaitan projek dan serahan ditangani dengan berkesan dalam pengurusan projek sepanjang kitaran hayat projek.	
010801 Keselamatan Maklumat Dalam Pengurusan Projek	**Tanggungjawab**
Aspek keselamatan secara keseluruhan iaitu fizikal, infrastruktur ICT, aplikasi dan data perlu diambil kira dalam menentukan pendekatan projek.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

0109 Pengurusan Aset ICT	
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas pengguna aset ICT RISDA.	
010901 Inventori Aset ICT	**Tanggungjawab**
Bertujuan memastikan aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik/ pengguna aset masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan pengguna aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan aset bernilai rendah sentiasa dikemas kini; b. Memastikan aset ICT mempunyai pemilik dan dikendalikan oleh warga RISDA yang dibenarkan sahaja;	Pegawai Aset dan Warga RISDA

c. Mengenal pasti lokasi pengguna aset ICT yang telah ditempatkan di RISDA; d. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan e. Setiap warga RISDA adalah bertanggungjawab ke atas aset ICT di bawah kawalannya.	

0110 Penggunaan Maklumat Dan Aset ICT	
Objektif: Memastikan maklumat dan aset ICT dilindungi, diguna dan dikendali sewajarnya.	
011001 Penggunaan Aset ICT	**Tanggungjawab**
Memastikan semua peraturan pengendalian aset ICT dikenal pasti, didokumenkan dan dilaksanakan.	Pegawai Aset dan Warga RISDA
011002 Pengendalian Maklumat	Tanggungjawab
Aktiviti seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah maklumat hendaklah mengambil kira langkah keselamatan berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, pengantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Warga RISDA

0111 Pemulangan Aset ICT	
Objektif: Melindungi aset RISDA susulan daripada proses pertukaran perkhidmatan kakitangan, atau penamatan perjanjian.	
011101 Pemulangan Aset ICT	**Tanggungjawab**
Memastikan semua aset ICT dikembalikan kepada RISDA mengikut peraturan dan terma perkhidmatan yang ditetapkan.	Warga RISDA dan Pegawai Aset

0112 Pengelasan Maklumat	
Objektif: Memastikan pengenalpastian dan pemahaman terhadap keperluan perlindungan maklumat berdasarkan kepentingan RISDA.	
011201 Pengelasan Maklumat	**Tanggungjawab**
Maklumat hendaklah dilabelkan sewajarnya berdasarkan pengelasan oleh pegawai pengelas yang dilantik. Setiap maklumat yang dilabelkan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan (Semakan dan Pindaan 2017) seperti berikut: a. Rahsia besar; b. Rahsia; c. Sulit; atau d. Terhad.	Pegawai Pengelas

0113 Pelabelan Maklumat	
Objektif: Memudahkan komunikasi dalam pengelasan maklumat dan menyokong automasi pemprosesan dan pengurusan maklumat.	
011301 Pelabelan Maklumat	**Tanggungjawab**
a. Maklumat hendaklah dilabel dan dikendali berasaskan peringkat keselamatan yang dikenal pasti selaras dengan Arahan Keselamatan (Semakan dan Pindaan 2017); dan b. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat.	Warga RISDA

0114 Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat antara RISDA dan pihak luar terjamin.	
011401 Pengurusan Pertukaran Maklumat	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mematuhi prosedur kawalan pertukaran maklumat untuk melindungi maklumat semasa pertukaran maklumat dilaksanakan melalui penggunaan pelbagai jenis kemudahan komunikasi; b. Melindungi media yang mengandungi maklumat daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari RISDA; dan c. Melindungi sebaik-baiknya maklumat yang terdapat di dalam sebarang media.	Warga RISDA

011402 Pengurusan Mel Elektronik	Tanggungjawab
Penggunaan e-mel di RISDA hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel 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 yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh RISDA sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh RISDA; c. Warga RISDA hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; d. Warga RISDA hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; e. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; f. Warga RISDA hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; g. Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat serta mengambil tindakan segera; dan h. Warga RISDA hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.	Pentadbir Sistem ICT, Warga RISDA

011403 Perkhidmatan Dalam Talian (*Online*)	**Tanggungjawab**
Bagi menggalakkan pertumbuhan perkhidmatan dalam talian serta sebagai menyokong hasrat kerajaan mengoptimumkan penyampaian perkhidmatan melalui media elektronik, warga RISDA boleh menggunakan kemudahan Internet yang disediakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Maklumat yang terlibat dalam transaksi dalam talian perlu dilindungi daripada aktiviti penipuan, pendedahan dan pengubahsuaian yang tidak dibenarkan; b. Maklumat yang terlibat pada 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; dan d. Pelaksanaan sidang video/*video conference* dengan i. Memastikan perisian yang digunakan adalah selamat dan sah. ii. Warga RISDA hendaklah menjaga etika semasa sidang video dijalankan. iii. Penganjur (*host*) dan ahli sidang video perlulah menjaga sensitiviti maklumat agar tidak berlaku kebocoran.	Warga RISDA
011404 Maklumat Umum	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: a. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b. Memastikan semua sistem diuji terlebih dahulu; dan	Pentadbir Sistem ICT, Warga RISDA

c. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	
011405 Media Sosial	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi di dalam memastikan keselamatan dan kawalan penyebaran maklumat yang dikongsi dan disebarkan melalui media sosial adalah seperti berikut: a. Tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara; b. Tidak melibatkan penyebaran maklumat dan dokumen terperingkat; c. Tidak memaparkan kenyataan yang boleh menjejaskan imej Kerajaan; d. Tidak menyentuh isu sensitif seperti agama, politik dan perkauman; e. Tidak memaparkan kenyataan yang berunsur fitnah atau hasutan; f. Tidak memuat naik atau membuat *live streaming* bagi maklumat sensitif dan dokumen terperingkat; g. Mempertimbangkan untuk mengeluarkan atau menyekat mereka yang terus membuat *posting* atau komen jelik; dan h. Melaporkan sebarang pelanggaran polisi penggunaan yang sedang berkuat kuasa.	Pentadbir Media Sosial, Warga RISDA
011406 Keselamatan Media Sosial	**Tanggungjawab**
Pentadbir Media Sosial yang bertanggungjawab mengendalikan media sosial rasmi perlulah memastikan keselamatan media sosial tidak menjejaskan kepentingan RISDA. Sekiranya terdapat pelanggaran, hendaklah dilaporkan kepada Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM).	Pentadbir Media Sosial, Pengurus ICT, Warga RISDA

0115 Kawalan Capaian	
Objektif: Memastikan hanya capaian yang disahkan dan mengelakkan capaian yang tidak sah kepada maklumat dan aset ICT.	
011501 Dasar Kawalan Capaian	**Tanggungjawab**
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d. Kawalan ke atas kemudahan pemprosesan maklumat.	ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT.
011502 Capaian Rangkaian	**Tanggungjawab**
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian RISDA, rangkaian agensi lain dan rangkaian awam; b. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

011503 Capaian Internet	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan Internet di RISDA hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian ICT 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; b. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; c. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan/ pegawai yang diberi kuasa; d. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; e. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet; f. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; g. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh RISDA; dan h. 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,	Pengurus ICT, Pentadbir Rangkaian ICT dan Warga RISDA

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, perjudian atau keganasan.	

0116 Pengurusan Identiti	
Objektif: Membenarkan individu dan sistem yang menggunakan identiti unik bagi membuat capaian kepada maklumat RISDA dan aset ICT serta melaksanakan tugasan berdasarkan hak capaian.	
011601 Pendaftaran Dan Penamatan Pengguna	**Tanggungjawab**
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi mengawal hak capaian Warga RISDA dan pihak ketiga supaya mereka dipertanggungjawabkan ke atas sistem ICT yang digunakan. Perkara-perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh RISDA sahaja boleh digunakan; b. Akaun warga RISDA dan pihak ketiga mestilah unik dan mencerminkan identiti pengguna; c. Pemilikan akaun warga RISDA dan pihak ketiga bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan RISDA. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; d. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan e. Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Bertukar bidang tugas kerja; ii. Bertukar ke unit / pusat tanggungjawab / agensi lain;	Pentadbir Sistem ICT, Pentadbir Pusat Data, Pentadbir Rangkaian ICT dan Warga RISDA

iii. Bersara; atau iv. Ditamatkan perkhidmatan.	

0117 Pengesahan Maklumat	
Objektif: Memastikan pengesahan entiti yang betul dan mengelakkan kegagalan ketika proses pengesahan.	
011701 Pengurusan Maklumat Pengesahan Rahsia Pengguna	**Tanggungjawab**
Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal dan diselia melalui proses pengurusan yang formal.	ICTSO dan Pentadbir Sistem ICT
011702 Penggunaan Maklumat Pengesahan Rahsia Pengguna	**Tanggungjawab**
Melaksanakan langkah-langkah perlindungan seperti berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan; f. Melaksanakan peraturan berkaitan maklumat rahsia rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan berdasarkan Arahan Keselamatan (Semakan dan Pindaan 2017); g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum; dan h. Mengawal aktiviti penggunaan media sosial seperti	Warga RISDA

dibawah: i. Mengelakkan ketirisan maklumat; ii. Tidak memberi atau mendedahkan sebarang komen atau pernyataan atau isu yang menyentuh perkara-perkara yang boleh menjejaskan imej dan dasar kerajaan; iii. Tidak menyebarkan maklumat yang berbentuk fitnah, hasutan dan lucah atau cuba memprovokasikan sesuatu isu yang menyalahi undang-undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan iv. Tidak menggunakan saluran media sosial hingga mengganggu fokus dalam urusan kerja.	
011703 Pengurusan Kata Laluan	**Tanggungjawab**
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh RISDA seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c. Kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun; d. Kata laluan Sistem Pengoperasian dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; e. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; f. Kuatkuasakan pertukaran kata laluan semasa log masuk kali pertama atau selepas log masuk kali pertama atau selepas kata laluan diset semula;	Pentadbir Sistem ICT, Pentadbir Pusat Data, Pentadbir Rangkaian ICT dan Warga RISDA

g. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; h. Mengelakkan penggunaan semula kata laluan yang baru digunakan; dan i. Penetapan kata laluan hendaklah mematuhi kombinasi panjang kata laluan sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara huruf besar dan kecil, aksara khas dan nombor (*alphanumeric*) KECUALI bagi perkakasan, perisian dan aplikasi yang mempunyai pengurusan kata laluan yang terhad.	

0118 Hak Capaian	
Objektif: Memastikan capaian kepada maklumat dan aset ICT ditakrifkan dan disahkan mengikut keperluan perkhidmatan RISDA.	
011801 Peruntukan Capaian Pengguna	**Tanggungjawab**
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas. Proses penyediaan capaian pengguna untuk kebenaran dan pembatalan capaian pengguna ke atas semua aplikasi dan perkhidmatan ICT perlu dilaksanakan.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT
011802 Semakan Semula Hak Capaian	**Tanggungjawab**
a. Mewujudkan prosedur penetapan dan penggunaan hak capaian pengguna kepada perkhidmatan ICT berdasarkan skop tugas yang dikawal dan diselia. b. Bagi akaun pengguna yang tidak aktif, pentadbir sistem perlu menyemak status semasa pengguna sebelum sebarang tindakan yang bersesuaian diambil. c. Semakan semula hak capaian perlu dilakukan sekurang- kurangnya sekali setahun. d. Hak capaian juga tertakluk kepada kebenaran daripada pemilik sistem/aplikasi/ lesen/data dan juga peraturan-peraturan lain yang berkenaan.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

011803 Pembatalan Atau Pelarasan Hak Capaian	Tanggungjawab
Hak capaian pengguna dan pihak luaran/ketiga untuk maklumat atau pemprosesan maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan tugas, perjanjian atau diselaraskan apabila berlaku perubahan dalam RISDA.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

0119 Keselamatan Maklumat Berhubung Dengan Pembekal	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).	
011901 Pemilihan Syarikat Pembekal	**Tanggungjawab**
Pemilihan syarikat pembekal hendaklah mengikut peraturan seperti berikut: a. Memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; b. Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; c. Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan seperti *e-Vetting* daripada agensi berkaitan; dan d. Jawatankuasa penilaian teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal.	Warga RISDA, Pihak Ketiga
011902 Polisi Keselamatan Maklumat Ke Atas Pembekal	**Tanggungjawab**
Semua pembekal adalah tertakluk kepada Dasar Keselamatan Kerajaan yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pengurus/ Penyelaras ICT dan Pihak Ketiga

a. Pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas; b. Pengurusan pembekal adalah tertakluk kepada peraturan yang sedang berkuat kuasa; c. Pengawalan dan pemantauan akses pembekal; dan d. Keperluan minimum keselamatan maklumat bagi setiap pembekal seperti keperluan perundangan atau pekeliling berkaitan hendaklah dinyatakan dalam perjanjian.	
011903 Keperluan Keselamatan Maklumat Berhubung Dengan Pembekal	**Tanggungjawab**
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk perkara-perkara seperti 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 perlu berlandaskan kepada peruntukan klausa dalam perjanjian; e. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai: i. Polisi Keselamatan Siber RISDA; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek.	CDO, ICTSO, Pengurus/ Penyelaras ICT, Pentadbir Pusat Data, Pentadbir Sistem ICT, Pentadbir Rangkaian ICT, Pemilik Projek dan Pihak Pembekal

f. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber RISDA sebagaimana **Lampiran B-1**.	

0120 Menangani Keselamatan Maklumat Dalam Perjanjian Dengan Pembekal	
Objektif: Mengekalkan tahap persetujuan bagi keselamatan maklumat dalam perjanjian dengan pembekal.	
012001 Perjanjian	**Tanggungjawab**
Menyedia dan menyemak Perjanjian dengan memastikan terma dan syarat yang bersesuaian untuk memastikan aktiviti pemprosesan maklumat di RISDA dilaksanakan mengikut undang-undang dan peraturan.	Pemilik Projek dan Penasihat Undang-undang
012002 Menangani Keselamatan Maklumat Dalam Perjanjian Dengan Pembekal	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; b. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mencapai, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan RISDA; c. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh RISDA; d. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal; dan e. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal perlu sentiasa dipantau, disemak semula dan diaudit secara berkala.	CDO, ICTSO, Pengurus/ Penyelaras ICT, Pentadbir Pusat Data, Pentadbir Sistem ICT, Pentadbir Rangkaian ICT, Pemilik Projek dan Pihak Pembekal

0121 Pengurusan Keselamatan Maklumat Dalam Rantaian Bekalan Teknologi Maklumat Dan Komunikasi	
Objektif: Mengekalkan tahap persetujuan bagi keselamatan maklumat dalam hubungan pembekal.	
012101 Pengurusan Keselamatan Maklumat Dalam Rantaian Bekalan ICT	**Tanggungjawab**
Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk/perkhidmatan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan c. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	CDO, ICTSO, Pengurus/ Penyelaras ICT, Pentadbir Pusat Data, Pentadbir Sistem ICT, Pentadbir Rangkaian ICT, Pemilik Projek dan Pihak Pembekal

0122 Pengurusan Pemantauan, Kajian Semula Dan Perubahan Perkhidmatan Pembekal	
Objektif: Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan penyampaian perkhidmatan adalah sama seperti mana dinyatakan dalam perjanjian oleh pembekal.	
012201 Pemantauan dan Kajian Perkhidmatan Pembekal	**Tanggungjawab**
RISDA hendaklah sentiasa memantau, mengkaji semula dan	Pemilik Projek,

mengaudit penyampaian perkhidmatan pembekal. Perkara-perkara berikut hendaklah dipatuhi: a. Pemantauan tahap prestasi perkhidmatan bagi mengesahkan pembekal mematuhi perjanjian perkhidmatan; dan b. Laporan perkhidmatan yang dihasilkan oleh pembekal hendaklah dipantau dan status kemajuan dikemukakan kepada RISDA.	Pengurus/ Penyelaras ICT
012202 Pengurusan Perubahan Perkhidmatan Pembekal	**Tanggungjawab**
Semua perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut SOP yang ditetapkan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. Perubahan dalam perjanjian dengan pembekal; b. Perubahan yang dilakukan oleh RISDA bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c. Perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	Pemilik Projek, Pentadbir Sistem ICT

0123 Perkhidmatan Awan (*Cloud Services*)	
Objektif: Memastikan keselamatan dan kawalan maklumat bagi perolehan, penggunaan, pengurusan dan penamatan/pelucutan daripada perkhidmatan awan yang bergantung kepada sumber pengkomputeran seperti pelayan, storan, pangkalan data, rangkaian dan perisian yang boleh dicapai menerusi Internet.	
012301 Kawalan Keselamatan Pengkomputeran Awan	**Tanggungjawab**
Penggunaan aplikasi dan kemudahan infrastruktur pengkomputeran awan (*cloud computing*) tidak dibenarkan	Pengurus/ Penyelaras ICT dan

sama sekali kecuali pengkomputeran awan yang dibangunkan, dilanggan dan dibenarkan oleh pihak Kerajaan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa. Secara asasnya maksud pengkomputeran awan yang dibangunkan dan dibenarkan oleh pihak Kerajaan adalah perkhidmatan pengkomputeran awan yang dimiliki, diuruskan atau dikendalikan oleh pihak Kerajaan sendiri berdasarkan kepada prinsip, penilaian dan keperluan keselamatan siber secara komprehensif dan strategik melibatkan teknologi, manusia dan proses. Ia bertujuan agar perkhidmatan pengkomputeran awan tersebut memenuhi objektif keselamatan, hala tuju bisnes serta keperluan peraturan dan undangundang yang berkuat kuasa.	Warga RISDA
012302 Penstoran Awan (*Cloud Storage*)	**Tanggungjawab**
Maklumat yang terlibat dalam transaksi dalam pengkomputeran awan perlu dilindungi daripada aktiviti penipuan dan pendedahan serta pengubahsuaian yang tidak dibenarkan. Penstoran awan ini tertakluk kepada perkhidmatan awan yang dilanggan dan dibenarkan oleh pihak Kerajaan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Dokumen terperingkat yang disimpan di *public cloud storage* hendaklah menggunakan kaedah enkripsi terlebih dahulu sebelum dimuat naik; b. Setiap dokumen yang disimpan di atas talian perlu ditetapkan kata laluan untuk membuka dokumen; dan c. Bahan rasmi perlu mendapat kelulusan Ketua Jabatan sebelum dimuat naik ke penstoran awan.	Warga RISDA

0124 Perancangan Dan Persediaan Pengurusan Insiden Keselamatan Maklumat	
Objektif: Memastikan tindak balas yang cepat, berkesan, konsisten dan teratur kepada insiden keselamatan maklumat termasuk komunikasi pada kejadian keselamatan maklumat.	
012401 Tanggungjawab Dan Prosedur	**Tanggungjawab**
RISDA menubuhkan pasukan CSIRT RISDA yang bertindak dalam mengendalikan insiden keselamatan siber. Tanggungjawab CSIRT RISDA meliputi semua bidang tugas pengurusan pengendalian insiden keselamatan siber RISDA.	ICTSO dan CSIRT RISDA

0125 Penilaian Dan Keputusan Dalam Kejadian Keselamatan Maklumat	
Objektif: Memastikan kategori dan keutamaan yang efektif dalam kejadian keselamatan maklumat.	
012501 Penilaian Dan Keputusan Dalam Kejadian Keselamatan Maklumat	**Tanggungjawab**
Insiden keselamatan siber ialah kejadian siber yang tidak diingini di mana berlakunya kehilangan kerahsiaan maklumat, gangguan terhadap integriti data atau sistem, atau gangguan yang menyebabkan kegagalan dalam memperoleh maklumat daripada sistem komputer dan kemungkinan berlakunya kesalahan perlanggaran peraturan keselamatan maklumat, dasar-dasar tertentu atau amalan piawai keselamatan siber. Jenis-jenis insiden keselamatan siber ialah: a. Penafian Perkhidmatan (*Denial of Service,* DoS) atau Penafian Perkhidmatan Teragih) *Distributed Denial of Service*, DDoS); b. Pencerobohan (*Intrusion*); c. Jangkitan Perisian Hasad (*Malicious Software Malware*); d. Pengehosan Perisian Hasad (*Malware Hosting*);	ICTSO dan CSIRT RISDA

e. Percubaan Pencerobohan (*Intrusion Attempt*); dan

f. Potensi Serangan (*Potential Attack*).

Insiden Dalaman Pusat Data adalah insiden yang berkaitan dengan jenis kerosakan yang berlaku ke atas aset fizikal Pusat Data yang tidak melibatkan gangguan terhadap pengoperasian di Pusat Data secara terus. Contoh insiden Pusat Data adalah seperti kerosakan atau gangguan pada ketersediaan peralatan seperti server, peralatan rangkaian, penghawa dingin dan lain-lain, kegagalan bekalan elektrik di Pusat Data, penggera alarm keselamatan tidak berfungsi, CCTV tidak berfungsi dan lain-lain.

Tindakan ke atas insiden yang berlaku hendaklah dibuat berasaskan kepada keseriusan sesuatu insiden. Tahap keutamaan tindakan ke atas insiden akan ditentukan seperti berikut:

a. Keutamaan 1

Insiden keselamatan siber yang memberi impak tinggi terhadap pertahanan dan keselamatan negara, kestabilan ekonomi negara, imej negara, keupayaan RISDA untuk berfungsi, kesihatan dan keselamatan awam serta privasi individu.

b. Keutamaan 2

Insiden keselamatan siber yang tidak memberi impak seperti mana yang dinyatakan dalam Keutamaan 1.

Bagi insiden yang dinilai dalam kategori tahap keutamaan 1, insiden perlu dimaklumkan kepada ICTSO dan CDO untuk tindakan berikut:

a. Mengurus dan mengambil tindakan ke atas insiden yang berlaku sehingga keadaan pulih;

b. Mengaktifkan Pelan Pemulihan Perkhidmatan (PKP) jika perlu; dan

c. Menentukan samada insiden ini perlu dilaporkan kepada agensi penguatkuasaan undang- undang/keselamatan (NACSA, PDRM, SKMM dan lain-lain).

Sekiranya insiden yang dinilai berada di dalam tahap keutamaan 2, insiden tersebut hanya perlu diselesaikan di peringkat dalaman atau/dan makluman kepada CDO (jika perlu).	

0126 Tindak Balas Terhadap Insiden Keselamatan Maklumat	
Objektif: Memastikan tindak balas yang efisien dan efektif kepada insiden keselamatan maklumat.	
012601 Tindak Balas Terhadap Insiden Keselamatan Maklumat	**Tanggungjawab**
Insiden keselamatan maklumat hendaklah dikendalikan menurut prosedur yang didokumenkan. Tindak balas yang dirancang dan yang diambil perlu direkodkan.	ICTSO dan CSIRT RISDA

0127 Pembelajaran Insiden Keselamatan Maklumat	
Objektif: Mengurangkan kebarangkalian atau kesan daripada insiden akan datang.	
012701 Pembelajaran Insiden Keselamatan Maklumat	**Tanggungjawab**
Setiap insiden keselamatan maklumat direkodkan dan dinilai untuk memastikan kawalan dan tindakan yang diambil adalah mencukupi atau perlu ditambah.	ICTSO dan CSIRT RISDA

0128 Pengumpulan Bahan Bukti
Objektif: Memastikan pengurusan bukti yang konsisten dan efektif berkaitan dengan insiden keselamatan maklumat bagi tujuan tindakan disiplin dan undang-undang.

012801 Pengumpulan Bahan Bukti	Tanggungjawab
RISDA hendaklah menentukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti.	ICTSO dan CSIRT RISDA

0129 Kesinambungan Keselamatan Maklumat	
Objektif: Melindungi keselamatan maklumat dan aset ICT ketika berlakunya gangguan.	
012901 Keperluan Kesinambungan Keselamatan Maklumat	**Tanggungjawab**
RISDA hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan penyampaian perkhidmatan dalam situasi kecemasan. RISDA perlu mengambil kira keperluan dan jangkaan pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan terpakai. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Melantik pasukan tadbir urus PKP RISDA; b. Menetapkan polisi PKP; c. Mengenal pasti perkhidmatan kritikal; d. Melaksanakan Kajian Impak Perkhidmatan dan Penilaian Risiko terhadap perkhidmatan kritikal; e. Membangunkan Pelan Induk PKP, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana (DRP) ICT; f. Melaksanakan program kesedaran dan latihan pasukan PKP dan RISDA; g. Melaksanakan simulasi; dan h. Melaksanakan penyelenggaraan ke atas pelan.	Koordinator PKP RISDA

0130 Persediaan ICT Untuk Kesinambungan Perkhidmatan	
Objektif: Memastikan maklumat dan aset ICT RISDA tersedia apabila berlaku gangguan.	
013001 Menentusahkan, Mengkaji Semula Dan Menilai Kesinambungan Keselamatan Maklumat	**Tanggungjawab**
PKP termasuk Pelan Pemulihan Bencana (DRP) hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi perkhidmatan RISDA untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian ini hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan pegawai yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.	Koordinator PKP RISDA

0131 Perlindungan Rekod	
Objektif: Memastikan pematuhan kepada keperluan undang-undang, peraturan dan perjanjian serta jangkaan masyarakat atau sosial berkaitan perlindungan dan ketersediaan rekod.	
013101 Kawalan Perlindungan Rekod	**Tanggungjawab**
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas pihak yang tidak berkenaan seperti yang terkandung di dalam keperluan undang-undang, peraturan dan perjanjian.	Warga RISDA, Pihak Pembekal dan Pihak Ketiga

0132 Privasi Dan Perlindungan Maklumat Pengecaman Individu (PII)	
Objektif: Memastikan pematuhan kepada keperluan undang-undang dan peraturan berkaitan aspek keselamatan maklumat dalam perlindungan maklumat pengecaman individu (PII).	
013201 Kawalan Privasi Dan Perlindungan Maklumat Pengecaman Individu (PII)	**Tanggungjawab**
RISDA hendaklah mengenal pasti privasi dan perlindungan maklumat peribadi pengguna dijamin seperti yang tertakluk dalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkenaan.	Warga RISDA dan Pihak Ketiga

0133 Kajian Semula Keselamatan Maklumat Secara Berkecuali	
Objektif: Memastikan kesesuaian, kecekapan dan keberkesanan yang berterusan dalam pendekatan RISDA untuk menguruskan keselamatan maklumat.	
013301 Keperluan Kajian Semula Keselamatan Maklumat Secara Berkecuali	**Tanggungjawab**
Penilaian keselamatan yang dilaksanakan oleh pihak ketiga boleh dilaksanakan secara terancang apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	ICTSO dan Pentadbir Sistem

0134 Keperluan Undang-Undang dan Peraturan	
Objektif: Memastikan pematuhan kepada keperluan undang-undang dan peraturan yang berkaitan dengan keselamatan maklumat.	
013401 Kenal Pasti Keperluan Undang-Undang dan Peraturan Yang Terpakai	**Tanggungjawab**
a. Setiap warga RISDA hendaklah membaca, memahami dan mematuhi Polisi Keselamatan Siber RISDA dan undang-undang atau peraturan-peraturan	Warga RISDA dan Pihak Ketiga

lain yang berkaitan, yang sedang berkuat kuasa. Pelanggaran Polisi Keselamatan Siber RISDA boleh dikenakan tindakan tatatertib. Sekiranya disyaki berlaku perlanggaran dasar Polisi Keselamatan Siber RISDA, Pengurus ICT perlulah melaporkan kepada ICTSO; b. Semua aset ICT di RISDA termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan; c. Sebarang penggunaan aset ICT RISDA selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber RISDA; dan d. Tertakluk kepada pematuhan dasar yang dinyatakan ia hendaklah berasaskan keupayaan sebenar persekitaran yang boleh dilaksanakan melalui analisa jurang (*gap analysis*) tanpa menjejaskan objektif polisi. Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua Warga RISDA adalah seperti di **Lampiran A**.	
013402 Peraturan Kawalan Kriptografi	**Tanggungjawab**
Kawalan kriptografi perlu digunakan bagi tujuan pematuhan kepada undang-undang dan peraturan yang diguna pakai.	Warga RISDA, Pihak Pembekal dan Pihak Ketiga

0135 Hak Harta Intelek	
Objektif: Memastikan pematuhan kepada keperluan undang-undang, peraturan dan perjanjian yang berkaitan dengan Hak Harta intelek dan pengunaan Hak Milik produk.	
013501 Kawalan Hak Harta Intelek	**Tanggungjawab**
Prosedur-prosedur yang sesuai akan dilaksanakan untuk memastikan keselarasan dengan perundangan, peraturan dan juga keperluan perjanjian yang berkaitan dengan IPR dan juga	Pemilik Projek, Pentadbir Sistem ICT, Warga RISDA,

pelesenan perisian. RISDA akan mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat. Perkara-perkara berikut hendaklah dipatuhi: a. Pematuhan terhadap hak cipta yang berkaitan dengan perisian proprietari, dan reka bentuk yang diperoleh daripada RISDA; b. Pematuhan terhadap perlesenan menghadkan penggunaan produk, perisian, reka bentuk dan bahan-bahan lain yang diperoleh daripada RISDA; dan c. Pematuhan terhadap hakcipta produk dan keperluan perlesenan.	Pihak Ketiga

0136 Pematuhan Kepada Polisi, Peraturan Dan Piawaian Keselamatan Maklumat	
Objektif: Memastikan keselamatan maklumat yang dilaksanakan dan beroperasi sesuai dengan polisi keselamatan, polisi tajuk khusus, peraturan dan piawaian yang dikaji semula secara berkala.	
013601 Pematuhan Polisi Dan Piawaian Keselamatan Maklumat	**Tanggungjawab**
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
013602 Kajian Semula Pematuhan Teknikal	**Tanggungjawab**
a. Dalam pelaksanaan keselamatan maklumat RISDA, kesemua prosedur, polisi dan proses keselamatan maklumat hendaklah disemak apabila terdapat perubahan ketara berlaku dalam pelaksanaannya; dan b. Sistem maklumat hendaklah sentiasa dikaji supaya selaras dengan pematuhan polisi dan standard keselamatan maklumat RISDA (seperti *Security Posture Assessment* – SPA).	ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT,

0137 Mendokumenkan Prosedur Operasi	
Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.	
013701 Keperluan Mendokumenkan Prosedur Operasi	**Tanggungjawab**
a. Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan; dan d. Warga RISDA hendaklah mematuhi prosedur yang telah ditetapkan.	Pentadbir Sistem ICT, Pentadbir Rangkaian ICT, Pentadbir Pusat Data, Warga RISDA

BIDANG 02: KAWALAN MANUSIA

0201 Saringan

Objektif:

Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan RISDA, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

020101 Saringan Sebelum Perkhidmatan	Tanggungjawab
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga RISDA serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan b. Menjalankan tapisan keselamatan untuk warga RISDA serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Warga RISDA dan Bahagian Pengurusan Sumber Manusia

0202 Terma Dan Syarat Sebelum Perkhidmatan

Objektif:

Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

020201 Terma Dan Syarat Sebelum Perkhidmatan	Tanggungjawab
Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Warga RISDA dan Bahagian Pengurusan Sumber Manusia

0203 Kesedaran, Pendidikan Dan Latihan Keselamatan Maklumat	
Objektif: Memastikan kakitangan dan pihak yang berkepentingan sedar dan memenuhi tanggungjawab keselamatan maklumat.	
020301 Kesedaran, Pendidikan Dan Latihan Keselamatan Maklumat	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan latihan kesedaran yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada warga RISDA secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan b. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	Warga RISDA dan Bahagian Pengurusan Sumber Manusia

0204 Proses Tindakan Disiplin	
Objektif: Memastikan kakitangan dan pihak yang berkepentingan faham ke atas kesan perlanggaran polisi keselamatan, menghalang serta berurusan dengan kakitangan dan pihak yang berkepentingan yang terlibat dengan perlanggaran.	
020401 Kesedaran, Pendidikan Dan Latihan Keselamatan Maklumat	**Tanggungjawab**
Memastikan adanya proses tindakan tatatertib dan/ atau undang-undang ke atas pegawai dan kakitangan RISDA serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh RISDA.	Warga RISDA, Bahagian Pengurusan Sumber Manusia dan Unit Integriti

0205 Tanggungjawab Selepas Pertukaran Atau Penamatan Perkhidmatan	
Objektif: Melindungi pihak berkepentingan RISDA sebagai sebahagian proses pertukaran atau penamatan kakitangan atau Perjanjian.	
020501 Tindakan Selepas Bertukar Atau Tamat Perkhidmatan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan semua aset ICT dikembalikan kepada RISDA mengikut peraturan dan/ atau terma perkhidmatan yang ditetapkan; dan b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh RISDA.	Warga RISDA dan Bahagian Pengurusan Sumber Manusia

0206 Perjanjian Kerahsiaan Maklumat	
Objektif: Mengekalkan kerahsiaan maklumat yang boleh dicapai oleh kakitangan dan pihak luaran/ketiga.	
020601 Keperluan Perjanjian Kerahsiaan Maklumat	**Tanggungjawab**
Syarat-syarat dan terma perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan RISDA dan hendaklah disemak dan didokumentasi. Pembekal/pihak luaran/pihak ketiga hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan	ICTSO, Warga RISDA, Pihak Ketiga dan Pihak Pembekal

0207 Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat bagi kakitangan yang bekerja jarak jauh (*remote*).	
020701 Kawalan Kerja Jarak Jauh	**Tanggungjawab**
Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Warga RISDA

0208 Pelaporan Kejadian Keselamatan Maklumat	
Objektif: Menyokong pelaporan bagi kejadian keselamatan maklumat yang boleh dikenalpasti oleh kakitangan tepat pada masanya, konsisten dan berkesan.	
020801 Mekanisme Pelaporan	**Tanggungjawab**
Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar Polisi Keselamatan Siber sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO RISDA dan Pasukan CSIRT RISDA dengan kadar segera: a. Maklumat didapati hilang atau didedahkan kepada pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan	ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data, Pentadbir Rangkaian ICT, Pentadbir Pangkalan Data, Pentadbir Media Sosial, Pentadbir Peralatan ICT dan CSIRT RISDA

e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Pelaporan insiden keselamatan ICT di RISDA sepertimana Prosedur Pelaporan iInsiden Keselamatan ICT berdasarkan Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam.	

0209 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
020901 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	**Tanggungjawab**
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. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada RISDA. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. 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; c. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; d. Menyediakan tindakan pemulihan segera; dan e. Memaklumkan/mendapatkan nasihat pihak berautoriti, jika perlu.	CSIRT RISDA

BIDANG 03: KAWALAN FIZIKAL

0301 Perimeter Keselamatan Fizikal

Objektif:

Melindungi premis dan aset ICT daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

030101 Kawalan Perimeter Keselamatan Fizikal	Tanggungjawab
Bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi 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. Memasang alat penggera atau kamera; d. Menghadkan laluan keluar masuk; e. Mengadakan kaunter kawalan; f. Menyediakan tempat atau bilik khas untuk pelawat; g. Mewujudkan perkhidmatan kawalan keselamatan; h. Melindungi kawasan terhad melalui kawalan pintu masuk yang sesuai bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; i. Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan yang disediakan; j. Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; dan	Pegawai Keselamatan dan Bahagian Pentadbiran

k. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad.	

0302 Laluan Masuk Fizikal	
Objektif: Memastikan penggunaan laluan masuk fizikal kepada maklumat dan aset ICT RISDA yang disahkan sahaja.	
030201 Kawalan Masuk Fizikal	**Tanggungjawab**
a. Setiap warga RISDA hendaklah memakai atau mengenakan kad ID Jabatan sepanjang waktu bertugas; b. Semua kad ID Jabatan hendaklah diserahkan balik kepada RISDA apabila pengguna berhenti, berpindah atau bersara; c. Setiap pelawat perlu mendaftar dan mendapatkan pas pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; d. Kehilangan pas pelawat mestilah dilaporkan dengan segera kepada Pengawal Keselamatan; dan e. Hanya warga RISDA dan pelawat yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT tertentu RISDA.	Bahagian Pentadbiran, Warga RISDA dan Pelawat
030202 Kawasan Penghantaran Dan Pemunggahan	**Tanggungjawab**
Memastikan kawasan penghantaran, pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Bahagian Pentadbiran
030203 Kawasan Terperingkat	**Tanggungjawab**
Kawasan terperingkat ditakrifkan sebagai kawasan yang menempatkan aset ICT berisiko tinggi dan meliputi kawasan premis atau sebahagian daripada premis di mana rahsia rasmi disimpan, diuruskan atau di mana kerja terperingkat	Pengurus ICT, Pentadbir Pusat Data dan Pentadbir

dijalankan. Akses ke kawasan terperingkat adalah dihadkan dengan kebenaran. a. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan b. Semua penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	Rangkaian ICT

0303 Keselamatan Pejabat, Bilik dan Kemudahan	
Objektif: Mencegah dari akses fizikal yang tidak sah, kerosakan dan gangguan terhadap maklumat dan aset ICT RISDA di pejabat, bilik dan kemudahan.	
030301 Kawalan Keselamatan Pejabat, Bilik dan Kemudahan	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a. Kawasan tempat kerja, bilik mesyuarat, bilik perbincangan, bilik fail, bilik kawalan CCTV, pusat data dan bilik server perlu dihadkan daripada diakses tanpa kebenaran; b. Kawasan tempat kerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh pihak luar; c. Petunjuk lokasi bilik operasi dan Kawasan larangan hendaklah mematuhi arahan keselamatan; dan d. Fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk KECUALI dengan kebenaran CDO, ICTSO atau Pegawai Pengawal.	CDO, ICTSO dan Bahagian Pentadbiran

0304 Pemantauan Keselamatan Fizikal	
Objektif: Mengesan dan menghalang akses fizikal yang tidak sah.	
030301 Kawalan Pemantauan Keselamatan Fizikal	**Tanggungjawab**
Premis fizikal perlu dipantau menggunakan sistem pengawasan (contoh: pengawal, penggera pencerobohan, sistem pemantauan video seperti CCTV, sistem aplikasi pengurusan maklumat keselamatan fizikal atau mana-mana yang bersesuaian.) Akses ke lokasi kritikal perlu dipantau secara berterusan bagi mengesan akses yang tidak sah atau tingkah laku yang mencurigakan.	Bahagian Pentadbiran

0305 Perlindungan Daripada Ancaman Fizikal Dan Persekitaran	
Objektif: Mencegah atau mengurangkan kesan dari kejadian yang berpunca dari ancaman fizikal dan persekitaran	
030501 Keperluan Perlindungan Daripada Ancaman Fizikal Dan Persekitaran	**Tanggungjawab**
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubah suai, pembelian hendaklah mematuhi garis panduan, tatacara dan prosedur yang sedang berkuatkuasa. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: 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	CDO, ICTSO, Bahagian Pentadbiran dan Bahagian Teknikal

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; i. Setiap warga RISDA hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan yang sedang berkuatkuasa; dan j. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan.	

0306 Bekerja Di Kawasan Selamat	
Objektif: Mencegah maklumat dan aset ICT di dalam kawasan yang selamat dari kerosakan dan gangguan oleh kakitangan yang tidak sah yang bekerja di kawasan tersebut.	
030601 Bekerja Di Kawasan Selamat	**Tanggungjawab**
Menyediakan garis panduan untuk keperluan bekerja di dalam kawasan yang dihadkan kepada pihak tertentu sahaja.	Bahagian Pentadbiran

0307 *Clear Desk* dan *Clear Screen*	
Objektif: Mengurangkan risiko capaian tidak sah, kehilangan dan kerosakan kepada maklumat di meja, skrin dan mana- mana lokasi yang boleh dimasuki sewaktu dan selepas waktu bekerja.	
030701 Kawalan *Clear Desk* dan *Clear Screen*	Tanggungjawab
Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; b. Dokumen terperingkat hendaklah disimpan dalam laci atau kabinet fail yang berkunci; dan c. Memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Warga RISDA

0308 Penempatan Dan Perlindungan Peralatan	
Objektif: Melindungi peralatan ICT RISDA daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
030801 Penempatan Dan Perlindungan Peralatan ICT	Tanggungjawab
a. Warga RISDA hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Warga RISDA bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan	Warga RISDA

konfigurasi yang telah ditetapkan; c. Warga RISDA dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d. Warga RISDA dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e. Warga RISDA adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f. Warga RISDA mesti memastikan perisian antivirus di komputer yang dipertanggungjawabkan kepada pengguna sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan luaran yang digunakan; g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h. Peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); i. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti router dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; j. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; k. Peralatan ICT yang hendak dibawa keluar dari premis RISDA, perlulah mendapat kebenaran bertulis dari Pentadbir Sistem ICT dan direkodkan seperti yang dinyatakan dalam pekeliling perbendaharaan sedia ada bagi tujuan pemantauan; l. Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera mengikut pekeliling perbendaharaan sedia ada; m. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa;	

n. Warga RISDA tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset; o. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Meja Bantuan ICT (ICT Service Desk) untuk dibaik pulih; p. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; q. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang telah ditetapkan; r. Warga RISDA dilarang sama sekali mengguna dan mengubah kata laluan akaun pentadbir (*administrator password*) pada komputer yang dipertanggungjawabkan dan telah ditetapkan; s. Warga RISDA bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; t. Warga RISDA hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan “OFF” apabila meninggalkan pejabat; u. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan v. Semua pergerakan aset ICT RISDA hendaklah direkodkan. w. Tidak memuat turun dan memasang perisian tanpa lesen yang sah dan kebenaran pentadbir ICT.	

0309 Keselamatan Aset Di Luar Premis

Objektif:

Mencegah maklumat dan aset ICT di dalam kawasan yang selamat dari kerosakan dan gangguan oleh kakitangan yang tidak sah yang bekerja di kawasan tersebut.

030901 Peminjaman Peralatan Untuk Kegunaan Di Luar Pejabat	Tanggungjawab
Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan: a. Peralatan yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai yang mengurus aset ICT/ Pentadbir Peralatan ICT dan tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	Pegawai Aset, Pentadbir Peralatan ICT, Warga RISDA
030902 Peralatan di Luar Premis	**Tanggungjawab**
Bagi perkakasan yang dibawa keluar dari premis RISDA, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan RISDA: a. Peralatan perlu dilindungi dan dikawal sepanjang masa; b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan; dan c. Kehilangan peralatan ICT perlu dilaporkan mengikutperaturan semasa yang ditetapkan.	Pentadbir Peralatan ICT, Warga RISDA

0310 Media Storan	
Objektif: Memastikan pendedahan, pengubahsuaian, penghapusan dan pemusnahan yang sah pada media storan.	
031001 Media Storan	**Tanggungjawab**
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti *thumb drive* dan media storan lain.	Warga RISDA

Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat: a. Pemerolehan bagi media storan hendaklah mematuhi garis panduan berkaitan perolehan yang sedang berkuatkuasa; b. Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; c. Akses untuk memasuki kawasan penyimpanan media adalah terhad kepada pegawai yang dibenarkan sahaja; d. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; e. Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan; f. Pergerakan media storan hendaklah direkodkan; g. Perkakasan backup hendaklah diletakkan di tempat yang terkawal; h. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; i. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; j. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; k. Menghadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja; dan l. Kitaran hayat data hendaklah diuruskan mengikut Akta Arkib Negara (Akta 629).	

031002 Pengurusan Media	Tanggungjawab
a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat terperingkat hendaklah dihapus atau dimusnahkan mengikut prosedur yang ditetapkan.	Warga RISDA
031003 Penghantaran dan Pemindahan	**Tanggungjawab**
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	Warga RISDA
031004 Pelupusan Media Storan	**Tanggungjawab**
Pelupusan media storan adalah tertakluk kepada keperluan berdasarkan kepada klasifikasi maklumat dan tatacara pelupusan semasa yang berkuat kuasa.	Pegawai Aset,Pentadbir Peralatan ICT, Warga RISDA

0311 Utiliti Sokongan	
Objektif: Mencegah maklumat dan aset ICT dari hilang, rosak dan dikompromi atau gangguan kepada operasi RISDA akibat dari kegagalan dan gangguan utiliti sokongan.	
031101 Kawalan Utiliti Sokongan	**Tanggungjawab**
Peralatan ICT perlu dilindungi daripada kegagalan bekalan	Pentadbir Bangunan,

kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi daripada kegagalan bekalan elektrik dan bekalan yang sesuai. b. Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah diperiksa, diuji dan diselenggara secara berjadual.	Pentadbir Pusat Data dan Pentadbir Rangkaian ICT, Pihak Ketiga (Pengurus Bangunan)

0312 Keselamatan Kabel	
Objektif: Mencegah maklumat dan aset ICT dari hilang, rosak dan dikompromi atau gangguan kepada operasi RISDA berkaitan dengan punca kuasa dan kabel komunikasi.	
031201 Keselamatan Kabel	**Tanggungjawab**
Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan	Pentadbir Bangunan, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT, Pihak Ketiga

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

0313 Penyelenggaraan Peralatan	
Objektif: Mencegah maklumat dan aset ICT dari hilang, rosak dan dikompromi atau gangguan kepada operasi RISDA berpunca dari kekurangan penyelenggaran.	
031301 Kawalan Penyelenggaraan Peralatan	**Tanggungjawab**
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 pengeluar yang telah ditetapkan; b. Peralatan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap peralatan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d. Semua peralatan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; e. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pentadbir Peralatan ICT berkenaan. f. Semua aktiviti penyelenggaraan perlu direkodkan; dan g. Memaklumkan warga RISDA sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pentadbir Peralatan ICT, Pihak Ketiga

0314 Pelupusan Yang Selamat Atau Penggunaan Semula Peralatan	
Objektif: Mencegah ketirisan maklumat dari peralatan yang mengandungi media storan yang perlu dilupuskan atau diguna semula.	
031401 Kawalan Pelupusan Yang Selamat Atau Penggunaan Semula Peralatan	**Tanggungjawab**
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh RISDA. Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan RISDA: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui kaedah: i. penyingkiran (*purging*) seperti *secure erase* atau *degaussing;* atau ii. pemusnahan media secara fizikal (*destroying*) seperti penghancuran (*disintegration*), kisaran halus (*pulverization*), peleburan dan pembakaran. b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c. Peralatan ICT yang akan dilupuskan hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupus atau sebaliknya; e. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT; f. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan	Pegawai Aset,Pentadbir Peralatan ICT, Warga RISDA

tersebut; g. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; h. Warga RISDA bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti external hard disk atau thumb drive sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; dan i. Warga RISDA adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. ii. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, hard disk, motherboard dan sebagainya; iii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di RISDA; iv. Memindah keluar dari RISDA mana-mana peralatan ICT yang hendak dilupuskan; dan v. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab RISDA.	

BIDANG 04: KAWALAN TEKNOLOGI

0401 Peralatan Pengguna

Objektif:

Melindungi maklumat daripada risiko yang didapati dari penggunaan peralatan oleh pengguna.

040101 Peralatan Mudah Alih	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi daripada risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; dan b. Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Warga RISDA
040102 Peralatan Pengguna Yang Tiada Pengawasan	**Tanggungjawab**
Peralatan yang tiada pengawasan perlu dilindungi dengan cara berikut: a. Menamatkan sesi penggunaan selepas digunakan; b. Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; dan c. Memastikan peralatan tidak digunakan oleh pihak yang tidak berkaitan.	Warga RISDA

0402 Hak Capaian Istimewa

Objektif:

Memastikan pengguna, komponen perisian dan perkhidmatan yang sah sahaja diberi hak capaian istimewa.

040201 Hak Capaian	Tanggungjawab
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan	Pentadbir Sistem ICT, Pentadbir

skop tugas.	Pusat Data dan Pentadbir Rangkaian ICT

0403 Sekatan Capaian Aplikasi dan Maklumat	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat dalam sistem aplikasi.	
040301 Sekatan Capaian Aplikasi dan Maklumat	**Tanggungjawab**
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; c. Setiap aktiviti capaian kepada sistem dan aplikasi yang berisiko tinggi hendaklah dihadkan kepada pengguna yang sah sahaja. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; d. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah dibenarkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Pentadbir Sistem ICT, Pentadbir Pusat Data, Pentadbir Rangkaian ICT dan ICTSO

0404 Capaian Kepada Kod Sumber	
Objektif: Memastikan supaya kod sumber dikawal dan dikendalikan dengan baik dan selamat.	
040401 Kawalan Kod Sumber	**Tanggungjawab**
Kawalan kod sumber (*source code*) dan dokumentasi sistem aplikasi hendaklah dilaksanakan ke atas sistem yang baharu dibangunkan secara *outsource* dan *in-house*. Ini bagi memastikan kesinambungan sistem aplikasi itu dapat berjalan dengan lancar sama ada selepas pertukaran pegawai atau penyerahan sistem kepada pemilik sistem aplikasi. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Pentadbir Sistem ICT

0405 Kawalan Capaian Sistem Pengoperasian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
040501 Capaian Sistem Pengoperasian	**Tanggungjawab**
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan b. Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a. Mengesahkan pengguna yang dibenarkan; b. Mewujudkan jejak audit ke atas semua capaian sistem	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

pengoperasian terutama pengguna bertaraf super user; dan c. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; b. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c. Menghadkan dan mengawal penggunaan program; dan d. Menghadkan tempoh capaian (*session timed-out*) ke sesebuah aplikasi berisiko tinggi.	

0406 Pengurusan Kapasiti	
Objektif: Memastikan kapasiti yang diperlukan oleh kemudahan pemprosesan maklumat, sumber manusia, pejabat dan kemudahan lain.	
040601 Pengurusan Perancangan Kapasiti	**Tanggungjawab**
a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	ICTSO dan Pentadbir Sistem ICT, Pentadbir Pusat Data, Pentadbir Rangkaian ICT, Pentadbir Pangkalan Data

0407 Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan*, *malware* dan sebagainya.	
040701 Perlindungan Dari Perisian Berbahaya	**Tanggungjawab**
a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang 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 *pattern* antivirus yang terkini; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Melaksana dan menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan dalam mana-mana perjanjian yang telah ditawarkan kepada pembekal perisian, bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	Pentadbir Sistem ICT, Warga RISDA
040702 Perlindungan Dari *Mobile Code*	**Tanggungjawab**
Penggunaan *mobile code* yang boleh mendatangkan ancaman	Warga RISDA

keselamatan ICT adalah tidak dibenarkan.	

0408 Kawalan Teknikal Kerentanan (*Vulnerability*)	
Objektif: Memastikan kawalan teknikal kerentanan (*vulnerability*) adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
040801 Kawalan dari Ancaman Teknikal	**Tanggungjawab**
Kawalan teknikal kerentanan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memperoleh maklumat teknikal kerentanan (*vulnerability*) yang terkini ke atas sistem maklumat yang digunakan; b. Menilai tahap teknikal kerentanan (vulnerability) bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT, Pentadbir Pusat Data, dan Pentadbir Rangkaian ICT.

0409 Pengurusan Konfigurasi	
Objektif: Memastikan peralatan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul dengan aturan keselamatan yang diperlukan dan konfigurasi tidak diubah oleh perubahan yang tidak sah dan tidak betul.	
040901 Kawalan Pengurusan Konfigurasi	**Tanggungjawab**
Perkara yang perlu dipatuhi termasuklah mewujudkan, mendokumenkan, melaksana, ICTSO dan Pentadbir memantau dan mengkaji semula konfigurasi keselamatan bagi peralatan, perisian, Sistem ICT perkhidmatan dan rangkaian.	ICTSO dan Pentadbir Sistem ICT

0410 Penghapusan Maklumat	
Objektif: Mencegah pendedahan maklumat sensitif yang tidak sewajarnya dan mematuhi undang-undang, peraturan dan keperluan perjanjian dalam penghapusan maklumat.	
041001 Kawalan Penghapusan Maklumat	**Tanggungjawab**
Maklumat yang disimpan di dalam sistem informasi, peralatan dan mana-mana storan media perlu dihapuskan apabila tidak diperlukan.	Pentadbir Sistem ICT dan Warga RISDA

0411 *Data Masking*	
Objektif: Untuk menghadkan pendedahan data sensitif termasuk maklumat data peribadi (PII), dan mematuhi keperluan undang-undang, peraturan dan perjanjian.	
041101 *Data Masking*	**Tanggungjawab**
Sekiranya pemprosesan melibatkan data sensitif termasuk maklumat data peribadi (contohnya PII), pihak RISDA hendaklah mempertimbangkan untuk menyembunyikan data tersebut. Teknik-teknik yang boleh digunakan untuk Data Masking termasuk, tetapi tidak terhad kepada: a. Pseudonymization b. Anonymization c. Enkripsi (memerlukan pengguna yang diberi kuasa untuk mempunyai kunci); d. Membatalkan (*nulling*) atau memadamkan aksara (menghalang pengguna yang tidak dibenarkan daripada melihat mesej penuh); e. Nombor dan tarikh yang berbeza-beza; f. Penggantian (mengubah satu nilai bagi yang lain untuk menyembunyikan data sensitif); atau g. Menggantikan nilai dengan fungsi hash.	Pentadbir Sistem ICT

0412 Pencegahan Kebocoran Data (DLP)	
Objektif: Untuk mengesan dan mencegah pendedahan dan pengekstrakan maklumat yang tidak dibenarkan oleh individu atau sistem.	
041201 Kawalan Pencegahan Kebocoran Data	**Tanggungjawab**
a. Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran; dan b. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.	Pentadbir Sistem ICT

0413 Sandaran (*Backup*) Maklumat	
Objektif Membolehkan salinan maklumat, perisian dan sistem diselenggara dan diuji secara berkala berdasarkan polisi tajuk khusus berkaitan *backup.*	
041301 Sandaran (*Backup)*	**Tanggungjawab**
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat salinan keselamatan ke atas semua data, sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi baharu; b. Menguji sistem sandaran dan prosedur *restore* yang sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; c. Tempoh pengekalan sandaran (*retention backup*) adalah selama 90 hari.	Pentadbir Pusat Data

d. Melaksanakan sandaran secara harian, mingguan, bulanan dan tahunan bergantung kepada tahap kritikal maklumat; dan e. Merekod dan menyimpan salinan sandaran di lokasi yang berlainan dan selamat.	

0414 *Redundancy* Pada Kemudahan Pemprosesan Maklumat	
Objektif: Menjamin operasi berterusan pada kemudahan pemprosesan maklumat.	
041401 Ketersediaan Kemudahan Pemprosesan Maklumat	**Tanggungjawab**
RISDA mempunyai system atau sumber sandaran untuk memastikan kesinambungan operasi. Ia melibatkan penduaan Komponen kritikal atau keseluruhan system untuk mengurangkan risiko kegagalan akibat kerosakan perkakasan, ralat perisian atau isu lain yang tidak dijangka. Ia perlu diuji keberkesanannya dari semasa ke semasa.	ICTSO, Pentadbir Sistem ICT dan Pemilik Sistem

0415 *Logging*	
Objektif: Merekod kejadian, menjana pembuktian, memastikan integriti maklumat log, mencegah capaian tidak sah, mengenal pasti kejadian keselamatan maklumat yang membawa kepada insiden keselamatan maklumat dan menyokong penyiasatan.	
041501 Sistem Log	**Tanggungjawab**
a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. Menyemak log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan baik pulih dengan segera; dan c. Melaporkan kepada ICTSO sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

041502 Jejak Audit	Tanggungjawab
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: a. Rekod setiap aktiviti transaksi; b. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; d. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan; e. 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; dan f. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem ICT
041503 Perlindungan Maklumat Log	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; b. Kemudahan merekod dan maklumat log perlu dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan; dan c. Kesalahan, kesilapan dan/atau penyalahgunaan perlu	Pentadbir Sistem ICT

direkodkan log, dianalisis dan diambil tindakan sewajarnya.	
041504 Pemantauan Maklumat Log	**Tanggungjawab**
Aktiviti pentadbiran dan operator sistem perlu direkodkan dan dipantau secara kerap.	Pentadbir Sistem ICT

0416 Aktiviti Pemantauan	
Objektif: Mengesan tingkah laku anomali dan potensi kepada insiden keselamatan maklumat.	
041601 Pemantauan Berterusan	**Tanggungjawab**
Pemantauan kepada rangkaian, sistem dan aplikasi perlu dilaksanakan secara berterusan mengikut tempoh yang bersesuaian. Perkara-perkara yang memerlukan pemantauan termasuklah tetapi tidak terhad kepada: a. Trafik keluar masuk rangkaian, sistem dan aplikasi; b. Capaian kepada sistem, server, perkakasan rangkaian, sistem pemantauan, sistem aplikasi yang kritikal dan lain-lain; c. Tahap pentadbir sistem dan fail konfigurasi rangkaian; d. Log dari peralatan/perisian keselamatan (contoh: Antivirus, IDS, IPS, Firewall dan lain-lain); e. Log kejadian berkaitan aktiviti sistem dan rangkaian; f. Penggunaan kod yang disahkan tidak disalah guna; dan g. Penggunaan sumber (contoh: CPU, *hard disks*, *memory* dan *bandwith*).	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT
041602 Pengauditan dan Forensik ICT	Tanggungjawab
Bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT RISDA;	ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT,

b. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery*, *phising*), 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 (IP *address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT; i. Aktiviti penyalahgunaan akaun e-mel; dan j. Aktiviti penukaran alamat IP (IP *address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	Pentadbir Pangkalan Data

0417 Penyeragaman Waktu	
Objektif: Membolehkan korelasi dan analisis kejadian berkaitan keselamatan dan lain-lain data yang direkodkan dan untuk menyokong siasatan kepada insiden keselamatan maklumat.	
041701 Keperluan Penyeragaman Waktu	**Tanggungjawab**
Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam RISDA atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

0418 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa	
Objektif: Memastikan penggunaan program utiliti tidak mendatangkan mudarat kepada keselamatan maklumat bagi kawalan sistem dan aplikasi.	
041801 Kawalan Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa	**Tanggungjawab**
Penggunaan program utiliti yang berkemungkinan mengakibatkan keperluan *overriding* pada kawalan sistem dan aplikasi perlu dihadkan dan dikawal.	ICTSO dan Pentadbir Sistem ICT

0419 Pemasangan Perisian Pada Sistem Operasi	
Objektif: Memastikan integriti pada sistem operasi dan mengelakkan eksploitasi kepada kerentanan (*vulnerabilities*) teknikal.	
041901 Kawalan Pemasangan Perisian Pada Sistem Operasi	**Tanggungjawab**
Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan ICTSO adalah seperti berikut: a. Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian dilaksanakan dan diperaku berjaya; b. Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur; c. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan RISDA; d. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; e. Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada CD-ROM disk atau	ICTSO dan Pentadbir Sistem ICT

media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak;	
041902 Sekatan Ke Atas Pemasangan Perisian	**Tanggungjawab**
Warga RISDA dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran ICTSO.	ICTSO, Pentadbir Sistem ICT dan Warga RISDA

0420 Keselamatan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
042001 Kawalan Rangkaian	**Tanggungjawab**
Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; b. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; c. Firewall hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat terperingkat Kerajaan serta dikonfigurasi sendiri oleh pentadbir sistem dan perlu mengambil kira perkara-perkara berikut: i. Sebarang permohonan buka/tutup *port* perlu dimaklumkan secara rasmi untuk tujuan rekod; ii. Semua aliran trafik (*multimedia* dan data) daripada dalam ke luar RISDA dan sebaliknya mestilah melalui *firewall;*	ICTSO, Pentadbir Rangkaian ICT dan Pentadbir Sistem ICT

iii. Hanya trafik yang disahkan sahaja dibenarkan untuk melepasinya berasaskan polisi semasa yang berkuatkuasa.; dan iv. Reka bentuk *firewall* hendaklah mengambilkira perkara berikut: • Keperluan audit dan arkib; • Kebolehsediaan; • Kerahsiaan; dan • Melindungi maklumat RISDA. d. Semua sistem aplikasi berasaskan web hendaklah diletakkan di dalam zon DMZ (*demilitarized* zone), manakala pangkalan data ditempatkan di *secured* zone; e. Semua perisian *sniffer* atau *network* analyser adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; f. Sebarang penyambungan peralatan rangkaian yang bukan di bawah kawalan RISDA hendaklah mendapat kebenaran ICTSO/Ketua Jabatan; g. Sebarang talian tambahan hendaklah mendapat kelulusan JPICT; h. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum; i. Sebarang penyambungan rangkaian daripada pihak ketiga (*remote tunneling*) ke dalam sistem rangkaian RISDA hendaklah mendapat kebenaran ICTSO; j. Capaian rangkaian Pusat Data hanya dihadkan melalui nod atau alamat IP yang dibenarkan sahaja; k. Pengawalan keperluan capaian peralatan melalui konfigurasi VLAN yang telah ditetapkan; l. Menyahaktifkan hebahan (*broadcast*); dan m. Kerja-kerja berkaitan rangkaian hanya boleh dilaksanakan oleh kakitangan yang terlatih dan dibenarkan sahaja; dan n. Tapisan kandungan (*content filtering*) perlu	

dilaksanakan bagi menyekat aktiviti-aktiviti yang dilarang serta mengakibatkan peningkatan *bandwith*.	

0421 Keselamatan Pada Perkhidmatan Rangkaian	
Objektif: Memastikan keselamatan dalam penggunaan perkhidmatan rangkaian.	
042101 Kawalan Perkhidmatan Rangkaian	**Tanggungjawab**
a. Pengurusan bagi semua perkhidmatan rangkaian yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian; dan b. Semua peralatan rangkaian yang dibekalkan oleh Jabatan Digital Negara (dahulunya dikenali sebagai MAMPU) bagi sistem rangkaian MyGov*Net tidak dibenarkan dialih dan dipinda konfigurasinya tanpa kebenaran ICTSO.	ICTSO dan Pentadbir Rangkaian ICT

0422 Pengasingan Dalam Rangkaian	
Objektif: Memisahkan rangkaian dalam sempadan keselamatan dan mengawal trafik di kalangan rangkaian tersebut berdasarkan keperluan perkhidmatan RISDA.	
042201 Kawalan Pengasingan Rangkaian	**Tanggungjawab**
Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian RISDA.	Pentadbir Sistem ICT

0423 Penapisan Web (*Web Filtering*)	
Objektif: Untuk melindungi sistem daripada terjejas oleh perisian hasad dan untuk menghalang akses kepada sumber web yang tidak dibenarkan.	
042301 Kawalan Penapisan Web	**Tanggungjawab**
Memasang *Web Content Filtering* pada Internet *Gateway* atau kawalan capaian Internet yang bersesuaian untuk menyekat aktiviti/capaian laman web yang dilarang.	Pentadbir Sistem ICT

0424 Penggunaan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
042401 Enkripsi	**Tanggungjawab**
Warga RISDA hendaklah membuat enkripsi ke atas maklumat sensitif atau maklumat rahsia rasmi yang termaktub di dalam buku arahan keselamatan pada setiap masa sekurang-kurangnya dengan penggunaan kata laluan.	Warga RISDA
042402 Tandatangan Digital	**Tanggungjawab**
Penggunaan tandatangan digital adalah dibenarkan kepada semua warga RISDA berkaitan khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Warga RISDA dan Pihak Ketiga
042403 Media Tandatangan Digital	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Warga RISDA hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital (GPKI) bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b. Media ini tidak boleh dipindah milik atau dipinjamkan; dan	Warga RISDA

c. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan mengikut peraturan semasa yang ditetapkan.	
042404 Pengurusan Infrastruktur Kunci Awam (PKI)	**Tanggungjawab**
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedah sepanjang tempoh sah kunci tersebut. Perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan sijil digital hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; b. Sijil digital hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c. Perkongsian sijil digital untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali; dan d. Sebarang perubahan kepada pemilik atau kehilangan/kerosakan hendaklah dilaporkan kepada pentadbir sistem.	Pemilik Sistem dan Pentadbir Sistem ICT

0425 Keselamatan Kitar Hayat Pembangunan	
Objektif: Memastikan keselamatan maklumat direka bentuk dan dilaksanakan pada kitar hayat pembangunan perisian dan sistem aplikasi.	
042501 Dasar Keselamatan Pembangunan	**Tanggungjawab**
Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Keselamatan persekitaran pembangunan; b. Keselamatan pangkalan data; i. Pemantauan Capaian Pangkalan Data di Pelayan Produksi secara berkala; ii. Permohonan Capaian Pangkalan Data di Pelayan	Pentadbir Sistem ICT

Produksi; dan iii. Pewujudan Pangkalan Data Baharu/Peningkatan direkodkan dengan permohonan perlu disertakan dengan dokumen yang berkaitan. c. Keperluan keselamatan dalam fasa reka bentuk; d. Keperluan check point keselamatan dalam carta perbatuan projek; e. Keperluan pengetahuan ke atas keselamatan aplikasi; f. Keselamatan dalam kawalan versi; dan g. Bagi pembangunan secara penyumberluaran (*outsource*), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	

0426 Keperluan Keselamatan Aplikasi	
Objektif: Memastikan sebarang aplikasi yang dibangunkan atau diperolehi adalah selamat.	
042601 Keperluan Keselamatan Aplikasi	**Tanggungjawab**
Keperluan keselamatan maklumat hendaklah dikenalpasti, ditentukan dan diluluskan sebelum membangunkan atau memperoleh sebarang sistem aplikasi.	ICTSO dan Pentadbir Sistem ICT
042602 Prosedur Pembangunan Sistem Aplikasi	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a. Proses pembangunan sistem aplikasi hendaklah berpandukan kepada Buku Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA). b. Pembangunan sistem aplikasi hendaklah mengambil kira sistem aplikasi sedia ada di RISDA dan agensi lain bagi mengelakkan pertindihan pembangunan sistem aplikasi yang sama; c. Sesuatu pembangunan sistem aplikasi perlu	Pemilik Sistem dan Pentadbir Sistem ICT

mempunyai pemilik sistem kepada sistem aplikasi tersebut; d. Pemilik Sistem aplikasi bertanggungjawab mempromosi dan memastikan kelancaran pelaksanaan sistem; e. Pemilik Sistem aplikasi hendaklah membaca dan memahami dokumentasi serta mematuhi prosedur yang berkaitan; f. Memastikan pembangunan sistem menggunakan teknik *secure coding*; g. Setiap sistem, aplikasi dan perisian hendaklah mematuhi garis panduan keselamatan dan lulus *User Acceptance Test* (UAT) dan *Final Acceptance Test* (FAT); dan h. Setiap sistem perlu mendapatkan pengesahan daripada JPICT atau lain-lain mesyuarat yang setara sebelum dilancarkan.	
042603 Prosedur Pembangunan Laman Web/Portal	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a. Semua maklumat yang hendak dimuatkan ke dalam laman web/portal mestilah mendapat kelulusan mengikut prosedur yang telah ditetapkan; b. Maklumat di laman web/portal hendaklah dikemas kini dari semasa ke semasa; c. Pembangunan laman web/portal hendaklah mempunyai ciri-ciri keselamatan bagi mengelak diceroboh dan digodam; dan d. Pembangunan laman web/portal perlu mematuhi Pekeliling Pengurusan Laman Web Agensi Sektor Awam.	Pentadbir Sistem ICT
042604 Prosedur Integrasi Pembangunan Aplikasi Mudah Alih	**Tanggungjawab**
Pembangunan aplikasi mudah alih yang melibatkan integrasi dengan sistem induk hendaklah menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang	Pentadbir Sistem ICT dan Pemilik Sistem

bersesuaian yang tidak memberi risiko ancaman keselamatan.	
042605 Kawalan Fail Sistem	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan d. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal.	Pemilik Sistem dan Pentadbir Sistem ICT

0427 Prinsip Keselamatan Arkitektur Dan Kejuruteraan Sistem	
Objektif: Memastikan aktiviti pembangunan sistem maklumat adalah selamat.	
042701 Prinsip Keselamatan Arkitektur Dan Kejuruteraan Sistem	**Tanggungjawab**
Prinsip umum pembangunan sistem: a. Kebergantungan (*Dependability*) - Sistem yang dibangunkan boleh beroperasi dengan lancar di bawah semua keadaan dan platform, termasuklah sekiranya terdapat serangan atau pelbagai niat jahat. b. Dipercayai (*Trustworthiness*) - Sistem boleh dipercayai walaupun terdapat kelemahan yang sengaja dieksploitasi untuk mengganggu pengoperasian sistem. Sistem yang boleh dipercayai mesti mengandungi logik yang boleh menghalang sebarang pencerobohan jahat. c. Daya tahan (*Resilience*) - Sistem yang berdaya tahan adalah	Pentadbir Sistem ICT

sistem yang mampu menentang serangan atau dapat dipulihkan dengan cepat sekiranya ada serangan yang tidak boleh ditolak/ ditahan. Ciri-ciri keselamatan utama pembangunan sistem termasuk: a. Keselamatan tahap sistem - Sistem dapat mengawal akses aplikasi berasaskan paparan pilihan menu yang berbeza mengikut peranan pengguna. b. Keselamatan *row-level* - Pengguna hanya dapat melihat data yang dibenarkan mengikut peranan mereka di dalam aplikasi yang sama. c. *Single sign-on* (SSO) - Proses pengesahan pengguna yang membolehkan pengguna memasukkan id dan kata laluan mereka pada satu sistem sahaja tetapi pengesahan tersebut memberi kebenaran untuk mengakses sistem lain yang berkaitan pada sesi yang sama tanpa perlu log masuk ke sistem tersebut. d. Parameter keistimewaaan pengguna - Parameter keistimewaan pengguna digunakan untuk memperibadikan ciri dan keselamatan kepada pengguna individu atau peranan pengguna. Parameter keistimewaan pengguna disimpan ke profil pengguna dan boleh diakses pada keseluruhan sistem. Ianya sangat fleksibel, dapat mengawal, menambah atau menyembunyi pilihan pengguna. e. Pilihan pengesahan fleksibel (*Flexible authentication options*) - Sistem aplikasi yang dibangunkan sepatutnya menawarkan pelbagai pilihan kaedah pengesahan pengguna, sistem sepatutnya fleksibel untuk menggunakan kaedah pengesahan yang sedia ada tanpa perlu wujud atau mengubah kaedah pengesahan semasa. f. Sumber data pengguna (*User specific data source*): Ciri keselamatan ini adalah sama dengan row-level keselamatan, tetapi di peringkat pangkalan data. Aplikasi yang dibangunkan boleh mengakses sumber data yang berbeza bergantung kepada pengguna. g. Pengauditan aktiviti sistem - Pengauditan aktiviti sistem membolehkan pembangun log aktiviti pengguna akhir untuk setiap aktiviti *Sign on/Sign off*. Ini membolehkan sistem	

menjejaki dengan cepat dan merekod log masuk dan keluar pengguna, fungsi yang dicapai dan aktiviti yang dilakukan terhadap data.	

0428 Kod Selamat (*Secure Coding*)	
Objektif: Memastikan perisian ditulis dengan selamat dengan mengurangkan potensi kerentanan (*vulnerability*) keselamatan maklumat di dalam perisian.	
042801 Kawalan Kod Selamat	**Tanggungjawab**
a. Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. b. Prinsip dan prosedur kejuruteraan sistem hendaklah sentiasa dikaji dari semasa ke semasa mengikut keperluan dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat.	Pentadbir Sistem ICT

0429 Pengujian Keselamatan Dalam Pembangunan Dan Penerimaan	
Objektif: Mengesahkan keperluan keselamatan maklumat dicapai semasa aplikasi atau kod dilancarkan ke persekitaran produksi.	
042901 Pengujian Keselamatan Sistem	**Tanggungjawab**
Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan sistem hendaklah sentiasa dikaji dari semasa ke semasa mengikut keperluan dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat.	Pentadbir Sistem ICT

042902 Pengujian Penerimaan Sistem	Tanggungjawab
Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubah suai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT

0430 Pembangunan Oleh Sumber Luar (*Outsourced*)	
Objektif: Memastikan langkah-langkah keselamatan maklumat yang diperlukan oleh RISDA dilaksanakan oleh pembangun sistem dari sumber luar (*outsourced*).	
043001 Kawalan Pembangunan Oleh Sumber Luar (*Outsourced*)	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua spesifikasi perolehan dan perjanjian komersial hendaklah mengandungi keperluan mandatori seperti yang berikut: “Kod sumber, data/maklumat, prosedur dan dokumen adalah hak milik Kerajaan.”; b. Bagi sistem yang dibangunkan, spesifikasi perolehan dan perjanjian komersial hendaklah memasukkan keperluan mandatori seperti yang berikut: “Kerajaan berhak mencapai kod sumber dan data/maklumat” dan “Kerajaan berhak melaksanakan pengolahan risiko ke atas perisian yang dibangunkan.”; c. Perolehan produk tempatan atau yang dibangun menggunakan teknologi tempatan hendaklah diberi keutamaan dalam pembangunan dan keseluruhan kitar hayat sistem. Kakitangan dan sumber berkaitan sistem hendaklah dipilih untuk mengurangkan kebergantungan kepada sumber luaran, kepakaran dan teknologi asing; d. Setiap sistem, aplikasi dan perisian hendaklah mematuhi garis panduan keselamatan dan lulus *User Acceptance Test* (UAT) dan *Final Acceptance Test* (FAT); e. Setiap sistem perlu mendapatkan kelulusan daripada	Pengurus ICT, Pemilik Sistem dan Pentadbir Sistem ICT

JPICT sebelum dibangunkan; dan f. Penilaian keselamatan perlu dilakukan oleh pihak ketiga untuk memastikan keselamatan sistem.	

0431 Pengasingan Persekitaran Pembangunan, Pengujian dan Produksi	
Objektif: Melindungi persekitaran produksi dan data dari dikompromi semasa aktiviti pembangunan dan pengujian.	
043101 Keperluan Pengasingan Persekitaran Pembangunan, Pengujian dan Produksi	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan dan perisian yang diperlukan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari peralatan yang digunakan sebagai produksi; b. Pengasingan juga merangkumi tindakan memisahkan kumpulan produksi dan rangkaian; dan c. Kawalan keselamatan pada data yang mengandungi maklumat rahsia rasmi sekiranya digunakan di dalam persekitaran pembangunan.	Pengurus ICT, Pemilik Sistem dan Pentadbir Sistem ICT
043102 Persekitaran Pembangunan Yang Selamat	**Tanggungjawab**
Mewujudkan dan melindungi persekitaran pembangunan supaya selamat untuk pembangunan sistem dan integrasi yang meliputi seluruh kitar hayat pembangunan sistem. RISDA perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: a. Sensitiviti data yang akan diproses, disimpan dan dihantar/diterima dari/ke sistem; b. Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; c. Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem;	ICTSO dan Pentadbir Sistem ICT

d. Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; dan e. Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	

0432 Pengurusan Perubahan	
Objektif: Memelihara keselamatan maklumat ketika melaksanakan perubahan.	
043201 Kawalan Perubahan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada Pengurus ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh Juruteknik Komputer RISDA atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Pengurus ICT, ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT, Pentadbir Pangkalan Data
043202 Prosedur Kawalan Perubahan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum digunapakai; b. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian	Pemilik Sistem, Pentadbir Sistem ICT

untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pihak ketiga; c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d. Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pembangun sistem yang dibenarkan sahaja; dan e. Menghalang sebarang peluang untuk membocorkan maklumat.	
043203 Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi	**Tanggungjawab**
Apabila platform operasi berubah, aplikasi bagi perkhidmatan kritikal hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan RISDA. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; b. Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan c. Memastikan perubahan yang sesuai dibuat kepada Pelan Kesinambungan Perkhidmatan (PKP) RISDA dan Pelan Pemulihan Bencana (DRP) yang berkaitan.	ICTSO dan Pentadbir Sistem
043204 Sekatan Ke Atas Perubahan Dalam Pakej Perisian	**Tanggungjawab**
Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.	ICTSO dan Pentadbir Sistem

0433 Maklumat Aktiviti Pengujian	
Objektif: Memastikan perkaitan pengujian dan perlindungan maklumat operasi yang digunakan untuk pengujian.	
043301 Perlindungan Maklumat Untuk Aktiviti Pengujian	**Tanggungjawab**
Maklumat yang digunakan untuk aktiviti pengujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; b. Pentadbir Sistem ICT yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; c. Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; d. Permohonan penyalinan dan penggunaan data sebenar sebagai data pengujian hendaklah direkodkan; e. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna serta sistem output untuk memastikan data yang telah diproses adalah tepat; f. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan g. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pengurus ICT, ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT, Pentadbir Pangkalan Data

0434 Perlindungan Keselamatan Maklumat Ketika Pengujian Audit	
Objektif: Meminimumkan kesan audit dan lain-lain aktiviti jaminan terhadap sistem operasi dan proses dalam perkhidmatan RISDA.	
043401 Pematuhan Keperluan Audit	**Tanggungjawab**
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	ICTSO, Pentadbir Sistem ICT dan Pihak Ketiga

TERMA DAN TAFSIRAN	
Antivirus	Perisian yang mengimbas virus pada media storan untuk mengesan sebarang kemungkinan adanya virus.
Ancaman	Apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah
Aset ICT	Termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Jalur Lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan 112omputer) dalam jangka masa yang ditetapkan.
BYOD	*Bring Your Own Device*, merupakan peralatan mudah alih persendirian seperti telefon pintar, tablet dan laptop yang digunakan oleh pengguna yang melaksanakan tugas rasmi melalui sambungan rangkaian Jabatan
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.
Clear Desk dan Clear Screen	Tidak meninggalkan dokumen data dan maklumat terperingkat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
CDO	*Chief Digital Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
CSIRT	*Cybersecurity Incidents Response Team* atau Pasukan Tindak Balas Insiden Keselamatan Siber bertanggungjawab menerima, menganalisis, dan bertindak balas terhadap laporan insiden berkaitan keselamatan siber.

TERMA DAN TAFSIRAN	
Denial of service	Pencegahan akses yang dibenarkan kepada sumber atau penangguhan operasi kritikal mengikut masa (*time-critical operation*)
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*).
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* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
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.

TERMA DAN TAFSIRAN	
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.
Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Malicious Code	Program atau kod hasad yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
Mobile code	Kod perisian yang dipindahkan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi-fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pegawai Keselamatan	Termasuk pegawai yang dilantik sebagai Pegawai Keselamatan Kerajaan atau mana-mana pegawai yang berkhidmat sebagai Pegawai Keselamatan Kerajaan atau pegawai yang menjalankan tugas sebagai Pegawai Keselamatan Kerajaan.
Pemilik Projek	Pemilik projek adalah pegawai yang mengurus dan memantau sesuatu projek ICT.

TERMA DAN TAFSIRAN	
Pengurus Projek	Pegawai yang mempunyai tanggungjawab keseluruhan untuk pengurusan dan perjalanan sesuatu projek.
Pemilik Sistem	Pemilik sistem (*business owner*) bagi sistem yang dibangun atau yang paling banyak memiliki data.
Pengurus ICT	Pengarah Bahagian Teknologi Maklumat RISDA
Pengurus Sumber Manusia	Pegawai yang bertanggungjawab dalam aspek pengurusan personel dan pembangunan sumber manusia
Penilaian Risiko	Penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.
Pentadbir Media Sosial	Pegawai yang bertanggungjawab memelihara nama baik RISDA melalui kandungan yang berkualiti di media sosial.
Pentadbir Pangkalan Data	Pegawai yang bertanggungjawab menentukan keselamatan pangkalan data.
Pentadbir Peralatan ICT	Pegawai yang bertanggungjawab mengawal dan menjaga semua perkakasan dan perisian ICT.
Pentadbir Pusat Data	Pentadbir yang mengurus dan menyelenggara Pusat Data RISDA.
Pentadbir Rangkaian ICT	Pentadbir yang melaksana dan menyelenggara rangkaian ICT dan komunikasi ICT.
Pentadbir Sistem ICT	Pentadbir yang menyelenggarakan sistem aplikasi, portal dan aplikasi mudah alih serta mengurus operasi/sokongan teknikal dan keselamatan ICT.
Peralatan ICT	Merujuk kepada semua perkakasan dan perisian ICT.
Perisian	Set atur cara komputer yang menjalankan sesuatu tugas pada sistem komputer. Terdapat tiga (3) jenis perisian iaitu sistem pengendali (contohnya: Linux dan Windows), sistem utiliti (contohnya: *Disk Cleanup* dan *Disk Defregmenter*) dan perisian

TERMA DAN TAFSIRAN	
	aplikasi (contohnya: Microsoft Office dan Google Chrome).
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.
Perkakasan ICT	Merujuk kepada komponen dalaman peralatan ICT.
Pihak Ketiga	Pihak yang membekalkan perkhidmatan dan pakar runding kepada RISDA.
PII	*Personally Identifiable Information* Maklumat Pengenalan Diri (PII) adalah maklumat yang boleh digunakan untuk mengenal pasti individu tertentu. Ia termasuk data yang, dengan sendirinya atau apabila digabungkan dengan maklumat lain, membolehkan pengenalan seseorang. Contoh: Nama, Alamat, Nombor Telefon, Alamat E-mel, Nombor Kad Pengenalan, Nombor Pasport, Nombor Lesen Memandu, Tarikh Lahir, Bangsa, Tempat Lahir, dsb.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Restore	Proses penarikan semula data.
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.
Switch	Alat yang boleh menapis (*filter*) dan memajukan (*forward*) isyarat paket data antara segmen rangkaian LAN.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.

TERMA DAN TAFSIRAN	
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Warga RISDA	Kakitangan RISDA dan KRH.

LAMPIRAN A

SENARAI PERUNDANGAN DAN PERATURAN

1. Akta Hak Cipta (Pindaan) Tahun 1997;
2. Akta Jenayah Komputer 1997;
3. Akta Keselamatan Siber 2024 (Akta 854)
4. Akta Komunikasi dan Multimedia 1998;
5. Akta Rahsia Rasmi 1972;
6. Akta Tandatangan Digital 1997;
7. Arahan Keselamatan (Semakan dan Pindaan 2017);
8. Arahan Perbendaharaan;
9. Arahan Teknologi Maklumat 2007;
10. Garis Panduan Pengadaptasian Kecerdasan Buatan (AI) Sektor Awam
11. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
12. Perintah-Perintah Am;
13. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) April 2016, versi 1.0;
14. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;
15. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
16. Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024
17. Surat Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan Pengendalian Insiden Keselamatan Siber Sektor Awam;
18. Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024
19. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
20. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;

21. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

22. Akta-akta/Kaedah/Pekeliling/Arahan lain yang berkaitan.

LAMPIRAN B

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
PIHAK BERKUASA KEMAJUAN PEKEBUN KECIL PERUSAHAAN GETAH

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 B-1

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
PIHAK BERKUASA KEMAJUAN PEKEBUN KECIL PERUSAHAAN GETAH

Nama (Huruf Besar) : ……

No. Kad Pengenalan : ……

Jawatan : ……

Syarikat : ……

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;

2. Saya juga berjanji akan melaksanakan tanggungjawab saya sebagaimana yang telah termaktub dalam Polisi Keselamatan Siber RISDA; dan

3. Sekiranya saya atau mana-mana individu yang mewakili syarikat ini didapati melanggar dasar yang telah ditetapkan, maka saya sebagai wakil syarikat bersetuju tindakan undang-undang boleh diambil ke atas sesiapa yang terlibat mengikut peruntukan-peruntukan undang-undang sedia ada yang sedang berkuatkuasa.

Tandatangan : …….

Tarikh : …….

Disahkan oleh;

……...

Pegawai Keselamatan ICT (ICTSO)

b.p. Timbalan Ketua Pengarah Pengurusan RISDA

Tarikh : ……..

LAMPIRAN C-1

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 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 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 mendapatkan kebenaran bertulis daripada 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 / Organisasi : .....

Tarikh : .....

Cap Jabatan/Organisasi

LAMPIRAN C-2

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 PERKHIDMATANDENGAN 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 : .....

Jawatan : .....

Jabatan / Organisasi : .....

Tarikh : .....

Disaksikan oleh : _____
(Tandatangan)

Nama (huruf besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan / Organisasi : .....

Tarikh : .....

Cap Jabatan/Organisasi

LAMPIRAN D

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 : ……..
Company No : ……..
Address : ……..
……...
……...
Telephone : ……..
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 writingby 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 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 : _____