DASAR KESELAMATAN SIBER KERAJAAN SARAWAK

VERSI 1.0 @ 2025

ISI KANDUNGAN

1. PENGENALAN

Dasar Keselamatan Siber (DKS) Kerajaan Sarawak mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam penggunaan aset teknologi maklumat dan komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna Kerajaan Sarawak mengenai peranan dan tanggungjawab dalam melindungi aset ICT

1.1 OBJEKTIF

Dasar Keselamatan Siber Kerajaan Sarawak diwujudkan untuk menjamin kesinambungan urusan Kerajaan Sarawak dengan meminimumkan kesan in-siden keselamatan siber.

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

Manakala, objektif utama DKS Kerajaan Sarawak adalah seperti berikut:

(a) Menjamin kelancaran operasi dan kesinambungan perkhidmatan agensi Kerajaan dengan meminimumkan impak insiden keselamatan maklumat;
(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dalam aspek kerahsiaan, integriti, kebolehsediaan, dan kesahihan maklumat serta penyangkalan;
(c) Mematuhi keperluan perundangan, peraturan, standard, pekeliling dan prosedur yang sedang berkuat kuasa;
(d) Memudahkan perkongsian maklumat yang selamat dan terjamin;
(e) Mencegah sebarang penyalahgunaan atau kecurian maklumat kerajaan.

1.2. 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 siber yang bersifat dinamik.

Keselamatan siber adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan siber berkait rapat dengan perlindungan aset. Terdapat empat (4) komponen asas keselamatan siber iaitu:

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan dari ca-paian tanpa kuasa yang sah;
(b) Menjamin setiap maklumat adalah tepat dan sempurna;

(c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
(d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

DKS Kerajaan Sarawak 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 siber 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.

1.3. SKOP

Aset ICT Kerajaan Sarawak terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan Siber Kerajaan Sarawak 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, DKS Kerajaan Sarawak 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 system kawalan dan prosedur dalam pengendalian semua perkara berikut:

(a) Perkakasan - Semua aset yang digunakan untuk menyokong pemprosesan dan penyimpanan maklumat, termasuk komputer, pelayan, dan peralatan komunikasi;
(b) Perisian - Program dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer, termasuk perisian, aplikasi dan sistem operasi yang digunakan untuk pemprosesan maklumat di jabatan.
(c) Perkhidmatan infrastruktur ICT– sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:
    - ✓ Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
    - ✓ Sistem halangan akses seperti sistem kad akses; dan
    - ✓ 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-maklumat untuk digunakan bagi mencapai misi dan objektif Kerajaan Sarawak. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod di agensi Kerajaan, profil pelanggan, pangkalan data dan fail-fail data, maklumat arkib dan lain-lain.
(e) Manusia - Individu yang memiliki pengetahuan dan kemahiran untuk melaksanakan tugas harian bagi mencapai misi dan objektif jabatan. Mereka ialah aset berdasarkan tugas dan peranan yang mereka laksanakan.
(f) Premis - Semua kemudahan dan premis yang menempatkan aset-aset di atas, yang mesti dilindungi dengan ketat untuk mencegah kebocoran rahsia atau kelemahan perlindungan. Sebarang kebocoran maklumat rasmi atau kelemahan perlindungan adalah dianggap sebagai pelanggaran keselamatan.

1.4. PRINSIP KESELAMATAN DATA DAN MAKLUMAT

Prinsip-prinsip keselamatan data dan maklumat yang menjadi asas kepada Dasar Keselamatan Siber Kerajaan Sarawak dan perlu dipatuhi ialah seperti yang berikut:

(a) Capaian Atas Dasar Perlu Mengetahui

Capaian terhadap penggunaan aset maklumat hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar perlu mengetahui sahaja. Ini bermakna capaian hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk capaian ialah berdasarkan klasifikasi dan peringkat dokumen seperti mana yang dinyatakan dalam para 53 Arahan Keselamatan (Semakan dan Pindaan 2017).

(b) Hak Capaian Minimum

Hak capaian minimum 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 capaian perlu 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

Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset maklumat daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

(e) Prinsip Kepercayaan Sifar (Zero Trust)

Prinsip ini menegaskan bahawa tiada pengguna, peranti, atau rangkaian harus dipercayai secara automatik, sama ada berada dalam atau luar perimeter rangkaian. Setiap permintaan untuk mencapai data atau maklumat mesti melalui proses pengesahan yang teliti sebelum hak capaian diberikan. Prinsip ini menyatakan bahawa:

- ✓ Semua trafik rangkaian (dalaman dan luaran) dianggap sebagai tidak dipercayai;

- ✓ Capaian kepada sumber diberikan berdasarkan set kriteria yang komprehensif dan dinamik, termasuk identiti pengguna, keadaan dan kesihatan peranti, lokasi capaian, serta faktor konteks lain yang relevan. Capaian kepada sumber hanya akan diluluskan selepas pengesahan menyeluruh terhadap identiti pengguna dan status peranti, tanpa mengira lokasi fizikal, untuk memastikan keselamatan yang maksimum; dan
- ✓ Menekankan prinsip keistimewaan yang paling sedikit, capaian kepada sumber yang perlu dicapai akan diberikan berdasarkan keperluan, apabila diperlukan dan hanya untuk tempoh masa yang ditetapkan.

(f) 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 maklumat seperti computer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*.

(g) Pematuhan

Dasar Keselamatan Siber Kerajaan Sarawak hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan maklumat.

(h) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kesediaan 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.

(i) Saling Bergantungan

Setiap prinsip keselamatan adalah saling melengkapi dan bergantung antara satu dengan lain untuk membentuk sistem keselamatan yang menyeluruh dan berkesan. Prinsip-prinsip ini tidak boleh dilaksanakan secara terpisah, tetapi mesti diintegrasikan dan diselaraskan untuk mencapai keselamatan yang maksimum.

1.5. IMPLIKASI KETIDAKPATUHAN POLISI KESELAMATAN SIBER

Ketidakpatuhan terhadap Dasar Keselamatan Siber Kerajaan Sarawak boleh mengakibatkan pelbagai implikasi yang serius, termasuk tetapi tidak terhad kepada:

(a) **Risiko Keselamatan**

Ketidakpatuhan boleh menyebabkan pendedahan data sensitif, pencerobohan sistem, atau gangguan operasi, yang boleh mengakibatkan kehilangan maklumat penting atau kerosakan kepada infrastruktur digital.

(b) **Gangguan Operasi**

Ketidakpatuhan boleh menyebabkan gangguan kepada operasi harian Jabatan, termasuk masa henti sistem, kehilangan data, dan kerosakan peralatan, yang boleh memberi kesan langsung kepada penyampaian perkhidmatan.

(c) **Kesan Undang-Undang**

Kegagalan mematuhi polisi ini boleh menyebabkan tindakan undang-undang diambil terhadap pihak yang terlibat, termasuk denda atau tindakan undang-undang lain yang berkaitan dengan pelanggaran peraturan dan undang-undang keselamatan siber.

(d) **Kerugian Kewangan**

Ketidakpatuhan boleh membawa kepada kerugian kewangan yang besar, sama ada melalui denda, kos pemulihan, atau kehilangan kepercayaan pelanggan dan pihak berkepentingan yang boleh menjejaskan kedudukan kewangan Jabatan.

(e) **Kerosakan Reputasi**

Insiden keselamatan siber yang disebabkan oleh ketidakpatuhan boleh merosakkan reputasi Kerajaan Sarawak, mengurangkan kepercayaan pihak berkepentingan dan masyarakat umum terhadap keupayaan Kerajaan Sarawak dalam menguruskan keselamatan maklumat.

(f) **Tindakan Disiplin**

Penjawat Awam Agensi Kerajaan yang didapati tidak mematuhi DKS Kerajaan Sarawak ini boleh dikenakan tindakan disiplin, termasuk amaran, penggantungan, atau penamatan perkhidmatan, bergantung kepada tahap pelanggaran yang dilakukan.

2. PENGURUSAN RISIKO

Semua pihak yang terlibat dalam pengurusan data dan maklumat Kerajaan Sarawak harus mengambil kira risiko yang wujud terhadap aset maklumat akibat kelemahan (*vulnerability*) dan ancaman yang semakin berkembang dalam persekitaran digital masa kini. Oleh itu, langkah-langkah proaktif dan bersesuaian perlu diambil untuk menilai tahap risiko terhadap aset maklumat, bagi memastikan pendekatan dan keputusan yang paling berkesan dapat dikenal pasti dalam menyediakan perlindungan dan kawalan yang optimum.

Penilaian risiko ini bertujuan untuk mengenal pasti dan mengambil tindakan susulan serta langkah-langkah mitigasi yang bersesuaian bagi mengurangkan atau mengawal risiko keselamatan maklumat berdasarkan penemuan daripada penilaian risiko tersebut. Penilaian risiko keselamatan maklumat hendaklah dilaksanakan secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT.

Penilaian risiko keselamatan maklumat harus dilaksanakan ke atas semua aset maklumat, termasuk aset fizikal, aplikasi, perisian, pelayan, rangkaian, serta proses dan prosedur yang berkaitan. Selain itu, penilaian risiko ini juga perlu dijalankan di premis yang menempatkan aset maklumat seperti pusat data, bilik media storan, kemudahan utiliti, dan sistem-sistem sokongan lain.

Agensi Kerajaan bertanggungjawab melaksanakan dan menguruskan risiko keselamatan. Agensi Kerajaan 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 atau bersedia menghadapi risiko yang mungkin berlaku selagi risiko tersebut tidak menjejaskan penyampaian perkhidmatan Kerajaan Sarawak;
(c) Mengelakkan atau mencegah risiko dengan mengambil langkah-langkah yang dapat mengelakkan atau mencegah terjadinya risiko; dan
(d) Memindahkan risiko kepada pihak ketiga seperti pembekal, pakar runding, atau pihak berkepentingan lain.

3. KAWALAN ORGANISASI

3.1. POLISI KESELAMATAN SIBER

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

ID	KETERANGAN	PERANAN
3.1.1	**Pelaksanaan Dasar** Pelaksanaan dasar ini akan dijalankan dengan arahan Setiausaha Kerajaan Sarawak.	Setiausaha Kerajaan Sarawak
3.1.2	**Penyebaran Dasar** Dasar ini perlu disebarkan kepada semua penjawat awam serta mana-mana pihak berkepentingan yang berurusan dengan Kerajaan Sarawak.	Agensi Pusat, Ketua Agensi, CIO/CDO Agensi ACIO/ACDO Agensi
3.1.3	**Kajian Semula Dasar** Dasar Keselamatan Siber Kerajaan Sarawak hendaklah dikaji semula mengikut keperluan dan arahan semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial untuk memastikan kesinambungan perkhidmatan. Prosedur kajian semula Dasar Keselamatan Siber Kerajaan Sarawak adalah seperti berikut: ▪ Kenal pasti dan tentukan perubahan yang diperlukan; ▪ Cadangan pindaan akan dikaji dan dipertimbangkan oleh agensi bertanggungjawab sebelum ianya dikemukakan kepada pengurusan tertinggi untuk kelulusan; dan ▪ Memaklumkan kepada semua penjawat awam dan pihak berkepentingan mengenai pindaan yang telah dibuat.	Agensi Pusat
3.1.4	**Pemakaian dan Pengecualian Dasar Keselamatan Siber Kerajaan Sarawak** Dasar Keselamatan Siber Kerajaan Sarawak adalah terpakai kepada semua penjawat awam serta mana-mana pihak berkepentingan yang berurusan dengan Kerajaan Sarawak. Tiada pengecualian bagi pematuhan dasar ini.	Agensi Pusat, Ketua Agensi, Penjawat Awam, Pihak Berkepentingan, Pembekal Perkhidmatan

3.2. PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan Siber Kerajaan Sarawak.

ID	KETERANGAN	PERANAN
3.2.1	**Setiausaha Kerajaan Sarawak** Peranan dan tanggungjawab Setiausaha Kerajaan Sarawak adalah seperti berikut: (a) Menentukan halatuju pelaksanaan keselamatan siber Kerajaan Sarawak (b) Memastikan semua keperluan organisasi dari segi sumber manusia, kewangan dan perlindungan keselamatan adalah mencukupi; (c) Memastikan ketetapan-ketetapan dinyatakan dalam dasar keselamatan siber dilaksanakan sewajarnya; (d) Memastikan perancangan, penyelarasan dan penyeragaman pelaksanaan program/projek/ inisiatif ICT yang berkaitan dengan keselamatan siber diselaras dengan halatuju Kerajaan Sarawak dan Pelan Strategik Pendigitalan Kerajaan Sarawak sedia ada atau dengan mana-mana pelan sedia ada yang digunapakai oleh Kerajaan Sarawak; dan (e) Melantik CDO dan ICTSO Kerajaan Sarawak.	Setiausaha Kerajaan Sarawak
3.2.2	***Digital Government Committee* (DGC)** DGC adalah jawatankuasa ICT tertinggi dalam pentadbiran Kerajaan Sarawak yang bertanggungjawab untuk merangka, mengkaji dan menentukan dasar, objektif, strategi serta piawaian ICT termasuk keselamatan ICT dan siber. Keanggotaan DGC adalah seperti berikut: **Pengerusi:** Setiausaha Kerajaan Sarawak. **Setiausaha:** Pengarah Agensi Pusat	DGC

	Ahli-ahli: a) Peguam Besar Negeri. b) Setiausaha Kewangan Negeri. c) Timbalan Setiausaha Kerajaan Sarawak (Ekonomi) d) Timbalan Setiausaha Kerajaan Sarawak (Pentadbiran) e) Timbalan Setiausaha Kerajaan Sarawak (Operasi) f) Setiausaha Tetap, Kementerian Utiliti dan Telekomunikasi g) Setiausaha Tetap, Kementerian Sumber Asli dan Pembangunan Bandar h) Setiausaha Tetap, Kementerian Kesihatan Awam, Perumahan dan Kerajaan Tempatan i) Pengarah, Unit Pembangunan dan Pengurusan Sumber Manusia j) Pengarah, Unit Pengurusan Ekonomi k) Pengurus Besar Sarawak Multimedia Authority (SMA) Urus Setia bagi DGC adalah Unit Digitalisasi Perkhidmatan Awam. Fungsi-fungsi DGC adalah seperti berikut: (a) Untuk menasihati Kerajaan Negeri mengenai sebarang program berkaitan Kerajaan Digital yang melibatkan semua Kementerian, Jabatan, Pihak Berkuasa Tempatan, Badan Berkanun, dan syarikat berkaitan Kerajaan (GLCs); (b) Untuk menetapkan hala tuju dan visi bagi Kerajaan Digital Kerajaan Sarawak; (c) Mencadang dan menasihati Sarawak Multimedia Authority (SMA) mengenai dasar, strategi, keutamaan, teknologi, piawaian, rancangan dan belanjawan untuk Kerajaan Digital bagi Kementerian Negeri, Jabatan, Pejabat Residen dan Daerah, Pihak Berkuasa Tempatan dan Badan Berkanun serta syarikat berkaitan Kerajaan (GLC);	

	(d) Untuk menilai dan mengesahkan rancangan dan belanjawan Kerajaan Digital untuk Perkhidmatan Awam Sarawak; dan (e) Untuk menyelaras dan memantau dan mengesahkan rancangan dan belanjawan Kerajaan Digital untuk Perkhidmatan Awam Sarawak.	
3.2.3	**Ketua Pegawai Digital (*Chief Digital Officer*) Kerajaan Sarawak** Peranan dan tanggungjawab CDO Kerajaan Sarawak dalam perkara-perkara seperti berikut: (a) Memperkasakan semua agensi Kerajaan Sarawak melalui Ketua Agensi, Ketua Pegawai Digital (CDO) agensi dalam memastikan pematuhan Dasar Keselamatan Siber (DKS) Kerajaan Sarawak; (b) Memastikan semua penjawat awam dan pihak yang berkepentingan untuk memahami peraturan-peraturan di bawah DKS; (c) Memastikan semua keperluan yang menyokong pelaksanaan DKS bagi agensi Kerajaan Sarawak adalah disediakan; dan (d) Menyelaraskan pembangunan dan semakan semula garis panduan, prosedur dan tatacara keselamatan ICT selaras dengan keperluan semasa.	CDO Kerajaan Sarawak
3.2.4	**Pegawai Keselamatan ICT (ICTSO) Kerajaan Sarawak** Peranan dan tanggungjawab ICTSO Kerajaan Sarawak adalah seperti berikut: (a) Menyelaras pembangunan dan penyelenggaraan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan Siber Kerajaan Sarawak; (b) Memastikan pelaksanaan Dasar Keselamatan Siber Kerajaan Sarawak dengan memberi penerangan dan pendedahan berkenaan dasar; (c) Mengurus dan menyelaras keseluruhan program-	ICTSO Kerajaan Sarawak

	program keselamatan ICT Kerajaan Sarawak kepada semua penjawat awam dan pihak berkepentingan; (d) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti serangan virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (e) Melaporkan insiden keselamatan ICT kepada Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara dan memaklumkan kepada CDO agensi; (f) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera; dan (g) Menyedia dan melaksana program kesedaran mengenai keselamatan siber.	
3.2.5	**Ketua Agensi** Ketua Agensi merujuk kepada Ketua Agensi yang berperanan dan bertanggungjawab dalam perkara-perkara berikut di agensi masing-masing: (a) Menyokong pelaksanaan DKS; (b) Memastikan program keselamatan siber dalaman dilaksanakan sekurang-kurangnya setahun sekali dibawah tanggungjawab jabatan masing-masing berlandaskan DKS; dan (c) Memastikan keperluan keselamatan ICT/ Siber agensi dimaklumkan kepada agensi pusat (jika ada); (d) Bertanggungjawab memastikan insiden-insiden atau perkara-perkara yang berkaitan dengan keselamatan siber agensi dilaporkan kepada agensi pusat (jika ada).	Ketua Agensi

3.2.6	**Ketua Pegawai Maklumat/ Ketua Pegawai Digital (CIO/CDO) Agensi** Dari segi aspek keselamatan ICT, CDO adalah bertanggungjawab kepada perkara berikut: (a) Membantu ketua agensi dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT di peringkat agensi; (b) Memastikan pelaksanaan DKS, piaiwaian ataupun garis panduan diterima pakai di peringkat agensi dan pematuhan dasar oleh pihak yang berkepentingan; (c) Memantau pematuhan DKS dengan melaksanakan ketetapan-ketetapan yang telah ditetapkan yang ada dalam DKS; (d) Menyelaras dan melaksana latihan /program kesedaran keselamatan ICT/siber di agensi (sekurang-kurangnya sekali setahun); (e) Menjalankan audit kendiri/ dalaman bagi memastikan pematuhan DKS serta mengenalpasti risiko-risiko yang ada di agensi masing-masing serta melaporkan kepada agensi pusat sekiranya memerlukan tindakan pencegahan; (f) Melaporkan insiden atau perkara yang berkaitan keselamatan ICT/ siber kepada agensi pusat melalui Pasukan Tindak Balas Insiden Keselamatan Siber Kerajaan Sarawak (CSIRT Sarawak); (g) Bekerjasama dengan agensi pusat serta semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan melaksanakan langkah-langkah baik pulih atau pembetulan dengan segera; (h) Memastikan pelaksanaan DKS, piaiwaian ataupun garis panduan diterima pakai di peringkat agensi dan pematuhan dasar oleh pihak yang berkepentingan; (i) Memantau pematuhan DKS dengan melaksanakan ketetapan-ketetapan yang telah ditetapkan yang ada dalam DKS;	CIO/CDO Agensi

	(j) Menyelaras dan melaksana latihan/ program kesedaran keselamatan ICT/ Siber di agensi (sekurang-kurangnya sekali setahun); (k) Menjalankan audit kendiri/ dalaman bagi memastikan pematuhan DKS serta mengenalpasti risiko-risiko yang ada di agensi masing-masing serta melaporkan kepada agensi pusat sekiranya memerlukan tindakan pencegahan; (l) Melaporkan insiden atau perkara yang berkaitan keselamatan ICT/ Siber kepada agensi pusat melalui Pasukan Tindak Balas Insiden Keselamatan Siber Kerajaan Sarawak (CSIRT Sarawak); (m) Bekerjasama dengan agensi pusat serta semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan melaksanakan langkah-langkah baik pulih atau pembetulan dengan segera; (n) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Kerajaan Sarawak (jika ada); (o) Memastikan akses kebenaran capaian penjawat awam dan pihak berkepentingan ke atas maklumat dan kemudahan proses maklumat ditamatkan/ ditarik balik atau dipinda mengikut peraturan yang ditetapkan oleh Kerajaan Sarawak dan/atau terma perkhidmatan; (p) Memastikan pelaksanaan DKS, piaiwaian ataupun garis panduan diterima pakai di peringkat agensi dan pematuhan dasar oleh pihak yang berkepentingan; dan (q) Memantau pematuhan DKS dengan melaksanakan ketetapan-ketetapan yang telah ditetapkan yang ada dalam DKS	

3.2.7	**Penolong Ketua Pegawai Maklumat/Ketua Pegawai Digital (ACIO/ACDO) Agensi** ACIO Agensi bertanggungjawab kepada perkara berikut: (a) Membantu CDO agensi dalam melaksanakan tanggungjawab berkaitan aset ICT; (b) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang tamat perkhidmatan, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; dan (c) Memantau perkakasan yang diagihkan kepada pengguna mematuhi peraturan yang ditetapkan.	ACIO/ACDO Agensi
3.2.8	**Pasukan Tindak Balas Insiden Keselamatan Siber Sarawak (CSIRT Sarawak)** Keahlian CSIRT Sarawak adalah seperti berikut: **Pengarah CSIRT**: Pengarah Agensi Pusat/ CDO Kerajaan Sarawak **Pengurus CSIRT**: Ketua Seksyen Perkhidmatan Gunasama Infrastruktur dan Keselamatan Siber Agensi Pusat/ ICTSO Kerajaan Sarawak **Ahli-ahli**: (a) Penolong Pengarah, Seksyen Perkhidmatan Gun-asama Infrastruktur dan Keselamatan Siber Agensi Pusat; (b) Pegawai-pegawai Agensi Pusat yang berkaitan;* (c) Wakil agensi yang mengendalikan perkhidmatan kritikal Keahlian CSIRT Agensi boleh dilantik daripada kalangan pegawai sedia ada yang mengendalikan keselamatan maklumat, rangkaian, operasi sistem atau mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.	Agensi Pusat, CSIRT Sarawak

	Peranan dan tanggungjawab CSIRT adalah seperti berikut: (a) Memastikan prosedur pengurusan operasi sistem dilaksanakan seperti yang ditetapkan oleh Agensi Kerajaan Sarawak; (b) Mengambil tindakan yang sesuai dengan segera apabila dimaklumkan mengenai pengguna sistem yang tamat perkhidmatan, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; (c) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian kepada sistem aplikasi ICT berdasarkan arahan pihak pengurusan atasan; (d) Memantau log atau aktiviti capaian harian pengguna sistem; (e) Mengenal pasti aktiviti-aktiviti seperti pencerobohan dan pengubahsuaian data dan/ atau sistem tanpa kebenaran dan mengambil tindakan membatalkan atau memberhentikannya dengan serta-merta; dan (f) Menyimpan dan menganalisis rekod jejak audit *(audit trail);* *Nota:* *Pentadbir Sistem Agensi merupakan pegawai yang dilantik secara rasmi oleh Ketua Agensi selaku pemilik sistem. Peranan ini mungkin hanya terpakai oleh Agensi Kerajaan Sarawak yang bertentu sahaja.*	

3.2.9	**Penjawat Awam Kerajaan Sarawak** Peranan dan tanggungjawab penjawat awam Kerajaan Sarawak adalah seperti berikut: (a) Membaca, memahami dan mematuhi DKS; (b) Memahami implikasi keselamatan siber kesan dari tindakannya; (c) Menjalani tapisan keselamatan sekiranya dikehendaki untuk berurusan dengan maklumat rahsia rasmi; (d) Melaksanakan prinsip-prinsip DKS dan menjaga kerahsiaan maklumat Kerajaan Sarawak; (e) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada agensi pusat dengan segera; (f) Melaksanakan langkah-langkah perlindungan seperti: (i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (ii) Memeriksa maklumat dan mengesahkan ia tepat dan lengkap dari semasa ke semasa; (iii) Menentukan maklumat sedia untuk digunakan; (iv) Menjaga kerahsiaan kata laluan; (v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (vi) Memberi perhatian kepada maklumat rahsia rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. (g) Menghadiri program-program keselamatan siber apabila diperlukan; dan (h) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan Siber Kerajaan Sarawak seperti di Lampiran A.	Penjawat awam

3.3. PENGASINGAN TUGAS

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

ID	KETERANGAN	PERANAN
3.3.1	**Pengasingan Tugas** Pengasingan tugas dan bidang tanggungjawab dilaksanakan bagi mengurangkan peluang pengubahsuaian data dan maklumat tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; (b) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai produksi; (c) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; (d) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya; dan (e) Semakan dan pemantauan hak capaian perkakasan, perisian dan sistem hendaklah dilaksanakan secara berkala.	Ketua Agensi, CIO/CDO Agensi, Pentadbir Sistem Agensi, Pengurus Projek ICT Agensi

3.4. HUBUNGAN DENGAN PIHAK BERKEPENTINGAN YANG KHUSUS

Memastikan aliran maklumat berkaitan keselamatan berlaku dengan sewajarnya.

ID	KETERANGAN	PERANAN
3.4.1	**Hubungan dengan Pihak Berkepentingan yang Khusus** Hubungan baik dengan pihak berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan seperti Agensi Keselamatan Siber Negara (NACSA), Pejabat Ketua Keselamatan Kerajaan (CGSO), Cybersecurity Malaysia (CSM) dan lain-lain	Agensi Pusat CSIRT

3.5. PERISIKAN ANCAMAN (*THREAT INTELLIGENCE*)

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

ID	KETERANGAN	PERANAN
3.5.1	**Keperluan Perisikan Ancaman** Maklumat tentang ancaman sedia ada atau baharu akan dikumpul dan dianalisis untuk: (a) Memudahkan tindakan sewajarnya diambil untuk mencegah ancaman daripada menyebabkan kemudaratan kepada Kerajaan Sarawak; dan (b) Mengurangkan kesan ancaman. 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 ancamaan; (b) Memproses dan menganalisis maklumat untuk memahami bagaimana ia berkaitan dan bermakna kepada agensi Kerajaan; dan (c) Berkomunikasi dan berkongsi kepada pihak berkepentingan yang berkaitan dalam format yang boleh difahami.	Agensi Pusat, CSIRT

	Perisikan ancaman hendaklah dianalisis dan kemudian digunakan: (a) Melaksanakan proses untuk memasukkan maklumat yang dikumpulkan dari sumber perisikan ancaman ke dalam proses pengurusan risiko 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.	

3.6. KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK

Memastikan risiko keselamatan maklumat berkaitan projek dan serahan ditangani dengan berkesan dalam pengurusan projek sepanjang kitaran hayat projek.

ID	KETERANGAN	PERANAN
3.6.1	**Keselamatan Maklumat dalam Pengurusan Projek** Aspek keselamatan secara keseluruhan iaitu fizikal, infrastruktur ICT, aplikasi dan data perlu diambil kira dalam menentukan pendekatan projek.	Agensi Pusat, CIO/CDO Agensi, Pegawai Data, Pengurus Projek ICT Agensi

3.7. INVENTORI MAKLUMAT DAN ASET LAIN YANG BERKAITAN

Memberi dan menyokong perlindungan yang bersesuaian ke atas pengguna aset ICT.

ID	KETERANGAN	PERANAN
3.7.1	**Inventori Aset** 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 mengikut tatacara pengurusan aset yang berkuatkuasa; dan (b) Setiap pengguna aset ICT adalah bertanggung-jawab ke atas aset ICT di bawah kawalannya.	CIO/CDO Agensi, Pegawai Aset, Pegawai Penerima Aset, Penjawat Awam

3.7.2	**Pengelasan dan Pelabelan Maklumat** Maklumat hendaklah dikelaskan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan (semakan dan pindaan 2017). Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagamana yang telah ditetapkan di dalam arahan keselamatan yang sedang berkuatkuasa seperti berikut: (i) Rahsia Besar; (ii) Rahsia; (iii) Sulit; atau (iv) Terhad Selain daripada maklumat rahsia rasmi adalah dikelaskan sebagai terbuka. Maklumat hendaklah ditanda dan dikendali berasaskan peringkat keselamatan yang dikenalpasti selaras dengan peraturan prosedur yang ditetapkan dalam arahan keselamatan. Maklumat hendaklah dilabel dan dikendalikan berasaskan peringkat keselamatan yang dikenal pasti selaras dengan Arahan Keselamatan (Semakan dan Pindaan 2017).	Ketua Agensi, Pegawai Pengelas, Pegawai Data
3.7.3	**Pengendalian Maklumat** 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, penghantaran, penyampaian, pertukaran dan pemusnahan; dan	CIO/CDO Agensi, Pentadbir Sistem Agensi, Pegawai Data, Penjawat Awam

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

3.8. PERTUKARAN MAKLUMAT

Memastikan keselamatan pertukaran maklumat antara Kerajaan Sarawak dan agensi luar terjamin.

ID	KETERANGAN	PERANAN
3.8.1	**Pengurusan Mel Elektronik** Penggunaan e-mel di agensi Kerajaan hendaklah dipantau secara berterusan untuk memenuhi keperluan etika penggunaan e-mel yang terkandung dalam Surat Pekeliling ICT No.7/2011 bertajuk Penggunaan Mel Elektronik Dan Internet Di Agensi-agensi Kerajaan Negeri. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan akaun atau alamat e-mel yang di-peruntukan sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (b) Setiap e-mel yang disediakan hendaklah me-matuhi format yang telah ditetapkan; (c) Semua pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; (d) Semua pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berk-omunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; (e) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat serta mengambil tindakan segera; dan (f) Semua pengguna hendaklah bertanggungja-wab ke atas pengemaskinian dan penggunaan mailbox masing-masing.	Agensi Pusat, CIO/CDO Agensi, Penjawat Awam

3.8.2	**Perkhidmatan Dalam Talian (Online)** Bagi menggalakkan penambahan perkhidmatan dalam talian serta sebagai menyokong hasrat Kerajaan mengoptimumkan penyampaian perkhidmatan melalui media elektronik, semua pengguna harus 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) Malumat yang terlibat pada transaksi dalam talian 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 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) Semua pengguna hendaklah menjaga etika semasa sidang video dijalankan; dan (iii) Penganjur (*host*) dan ahli sidang video perlu menjaga sensitiviti maklumat agar tidak berlaku kebocoran.	CIO/CDO Agensi, Penjawat Awam
3.8.3	**Laman Web Rasmi Dan Media Sosial** Laman web dan media social adalah saluran penyebaran maklumat yang penting antara agensi kerajaan dan orang awam. Pengwujudan laman web dan media sosial rasmi agensi hendaklah dikawal berdasarkan Prosedur Pengurusan Laman Web dan Media Sosial yang dikeluarkan oleh agensi pusat dari semasa ke semasa.	Ketua Agensi, CIO/CDO Agensi, Pentadbir Laman Web Agensi, Pentadbir Media Sosial Agensi

	Perkara-perkara yang perlu dipatuhi bagi memastikan keselamatan dan kawalan penyebaran maklumat yang dikongsi dan disebarkan melalui laman web rasmi dan media sosial agensi adalah seperti berikut: (a) Tidak menjejaskan imej dan kepentingan perkhidmatan awam dan Kerajaan Sarawak; (b) Tidak menyebarkan maklumat dan dokumen rahsia rasmi; (c) Tidak menyentuh isu sensitif seperti agama, politik dan perkauman; (d) Tidak menyebarkan kenyataan yang berunsur fitnah atau hasutan; (e) Semua maklumat yang hendak dimuatkan ke dalam laman web mestilah telah disahkan dan mendapat kelulusan Ketua Agensi; (f) Maklumat yang terkandung dalam laman web dan media sosial adalah di bawah tanggungjawab agensi masing-masing; (g) Maklumat di laman web dan media sosial hendaklah dikemas kini dari semasa ke semasa; (h) Laman web dan media sosial agensi luar yang memerlukan pautan ke Laman Web agensi Kerajaan Sarawak atau sebaliknya mestilah mendapat kebenaran Ketua Agensi; dan (i) Pembangunan laman web dan media sosial hendaklah mempunyai ciri-ciri keselamatan bagi mengelak diceroboh dan digodam.	

3.9. KAWALAN CAPAIAN

Kawalan capaian hendaklah mengambil kira faktor had capaian dan hak capaian ke atas data dan maklumat serta proses capaian maklumat.

ID	KETERANGAN	PERANAN
3.9.1	**Keperluan Kawalan Capaian / Akses** Capaian atau akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan diskripsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan oleh agensi masing-masing, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. 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 perkakasan mudah alih; dan (d) Kawalan ke atas kemudahan pemprosesan maklumat.	CIO/CDO Agensi, Pentadbir Sistem Agensi

3.9.2	**Akaun Pengguna Dan Hak Capaian** Setiap pengguna adalah bertanggungjawab ke atas capaian/akses ke sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan sahaja boleh digunakan; (b) Akaun pengguna mestilah unik, bersesuaian, hendaklah sinonim dengan nama sebenar dan mencerminkan identiti pengguna; (c) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan serta polisi Kerajaan Sarawak. Walau bagaimanapun, pengguna bertanggungjawab sepenuhnya ke atas segala kegunaan melalui akaun dan kata laluannya; (e) Akaun pengguna boleh ditamatkan atas sebab-sebab berikut: (i) Bertukar bidang tugas kerja* (ii) Bertukar tempat bertugas ke agensi lain* (iii) Bersara (iv) Ditamatkan perkhidmatan (f) Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas; dan (g) Hak capaian pengguna diberi berdasarkan peranan dan tanggungjawab pengguna. **Nota: untuk aplikasi-aplikasi yang khusus tidak termasuk akaun emel*	Pentadbir Sistem Agensi, CIO/CDO Agensi, Penjawat Awam
3.9.3	**Capaian Rangkaian** Premis Kerajaan Sarawak hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian rasmi yang dibenarkan oleh Kerajaan	Agensi Pusat, CIO/CDO Agensi

	Sarawak, iaitu rangkaian SarawakNet. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menyediakan platform yang bersesuaian di antara rangkaian agensi Kerajaan Sarawak, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan yang menepati kesesuaian penggunaannya; (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian; (d) Mentadbir dan mengawal rangkaian yang dikongsi (*shared networks*), terutama sekali yang keluar daripada rangkaian SarawakNet; dan (e) Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan menempatkan atau memasang perkakasan ICT yang bersesuaian di rangkaian SarawakNet (f) Pengguna di agensi adalah dilarang memasang atau mengolah semula rangkaian di agensi masing tanpa kebenaran agensi pusat. Ini adalah kerana ianya boleh menjejaskan kualiti perkhidmatan rangkaian SarawakNet.	
3.9.4	**Capaian Internet** (a) Penggunaan internet hendaklah dipantau secara berterusan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Langkah ini dapat melindungi daripada kemasukan malicious code, virus dan bahan tidak sepatutnya ke dalam rangkaian SarawakNet; (b) Penggunaan internet hanya untuk kegunaan rasmi sahaja; (c) Mengawal aktiviti (*video conferencing*, *video streaming, chat, large file downloading* dan aktiviti-aktiviti lain yang seumpamanya) bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan;	Agensi Pusat, Ketua Agensi, CIO/CDO Agensi, ACIO/ACDO Agensi, Penjawat Awam

	(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 Agensi 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 rasmi sahaja; (h) Penjawat Awam adalah **DILARANG** melakukan aktiviti-aktiviti seperti berikut: (i) Memuat naik, memuat turun, menyimpan bahan bacaan, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah/ganas; dan (ii) Menggunakan perisian tidak berlesen dan sebarang aplikasi yang boleh menjejaskan tahap capaian internet. (iii) Perolehan/pembelian dan penggunaan broadband bergantung kepada justifikasi atau keperluan dan tertakluk kepada polisi/ketetapan yang berkuatkuasa dari semasa ke semasa; dan (iv) Penggunaan kemudahan internet peribadi di pejabat untuk urusan rasmi seperti modem, hotspot dan sebagainya adalah **tidak dibenarka**n jika melibatkan sambungan ke rangkaian SarawakNet dan perkakasan milik Kerajaan.	

3.10. PENGURUSAN IDENTITI

Membenarkan individu dan sistem yang menggunakan identiti unik bagi membuat capaian kepada maklumat Kerajaan Sarawak dan aset ICT serta melaksanakan tugasan berdasarkan hak capaian.

ID	KETERANGAN	PERANAN
3.10.1	**Pendaftaran dan Pembatalan Pengguna** Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi mengawal hak capaian pengguna dan pihak ketiga supaya mereka dipertanggungjawabkan ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan sahaja boleh digunakan; (b) Akaun pengguna mestilah unik, bersesuaian, hendaklah sinonim dengan nama sebenar dan mencerminkan identiti pengguna; (c) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan serta polisi Kerajaan Sarawak. Walau bagaimanapun, pengguna bertanggungjawab sepenuhnya ke atas segala kegunaan melalui akaun dan kata laluannya; (e) Akaun pengguna boleh ditamatkan atas sebab-sebab berikut: (i) Bertukar bidang tugas kerja (ii) Bertukar tempat bertugas ke agensi lain (iii) Bersara (iv) Ditamatkan perkhidmatan Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Semua capaian ini perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	Pentadbir Sistem Agensi, CIO/CDO Agensi, Penjawat Awam

3.10.2	**Pengurusan Identiti** Pengurusan akaun pengguna bagi capaian ke sistem atau aset maklumat bermula daripada penciptaan rekod pengguna baharu sehingga penamatan profil apabila pengguna telah meletakkan jawatan, bersara atau meninggal dunia dalam perkhidmatan. Pendaftaran, pengemaskinian dan penamatan akaun pengguna dilaksanakan mengikut prosedur yang ditetapkan. Proses pengurusan akaun pengguna harus memastikan bahawa: (a) Identiti yang diberikan khusus hanya dikaitkan dengan seorang sahaja untuk membolehkan orang itu bertanggungjawab atas tindakan yang dilakukan dengan identiti khusus ini; (b) Identiti yang diberikan kepada entiti selain manusia seperti mesin atau sistem tertakluk kepada kelulusan. Identiti khusus yang diberikan hanya dikaitkan dengan seorang sahaja untuk membolehkan orang itu bertanggungjawab ke atas tindakan yang dilakukan dengan identiti khusus ini; (c) Identiti yang diberikan kepada entiti selain manusia seperti mesin atau sistem tertakluk kepada kelulusan yang diasingkan dengan sewajarnya dan pengawasan berterusan. (d) Akaun pengguna perlu dinyahaktifkan dengan segera tepat pada masanya jika tidak lagi diperlukan; (e) Dalam domain tertentu, identiti tunggal dihubungkan dengan entiti tunggal; dan (f) Rekod penggunaan dan pengurusan identiti pengguna dan maklumat pengesahan hendaklah disimpan.	Pentadbir Sistem Agensi, CIO/CDO Agensi, Penjawat Awam

3.11. MAKLUMAT PENGESAHAN IDENTITI

Memastikan maklumat pengesahan bagi pengguna hendaklah dikawal dan diselia melalui proses pengurusan yang formal.

ID	KETERANGAN	PERANAN
3.11.1	**Pengurusan Maklumat Pengesahan Identiti Pengguna** Peruntukan maklumat pengesahan identiti pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan. Peruntukan dan proses pengurusan hendaklah memastikan bahawa: (a) Kata laluan atau nombor pengenalan diri (*Personel Identification Number*, PIN) yang dijana secara automatik semasa proses pendaftaran sebagai maklumat pengesahan rahsia sementara adalah tidak dapat diteka dan unik untuk setiap individu, dan pengguna dikehendaki menukarnya selepas penggunaan pertama; (b) Prosedur yang telah diwujudkan untuk mengesahkan identiti pengguna sebelum memberikan maklumat pengesahan baharu, gantian atau sementara; (c) Maklumat pengesahan, termasuk maklumat pengesahan sementara, dihantar kepada pengguna secara selamat (contohnya, melalui saluran yang disahkan dan dilindungi), dan penggunaan mesej e-mel elektronik yang tidak dilindungi (*clear text*) untuk tujuan ini hendaklah dielakkan; (d) Pengguna mengakui penerimaan maklumat pengesahan identiti pengguna; (e) Maklumat pengesahan tetapan asal (*default*) seperti yang ditetapkan atau diberikan oleh sistem diubah dengan segera selepas pemasangan sistem, perkakasan atau perisian;	Pentadbir Sistem Agensi, Penjawat Awam

3.11.2	**Penggunaan Maklumat Pengesahan Rahsia** Peranan dan tanggungjawab pengguna ialah seperti yang berikut: (a) Membaca, memahami dan mematuhi DKS Kerajaan Sarawak; (b) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat Kerajaan Sarawak; (c) Melaksanakan langkah-langkah perlindungan seperti yang berikut: (i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (ii) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (iii) Menentukan maklumat sedia untuk digunakan; (iv) Menjaga kerahsiaan kata laluan; (v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (vi) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (vii) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum. (viii) Maklumat pengesahan terjejas atau telah dikompromi hendaklah diubah serta-merta apabila pemberitahuan atau petunjuk sebarang kompromi diterima; (ix) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CSIRT dengan segera; dan (x) Menghadiri program-program kesedaran mengenai keselamatan siber.	CIO/CDO Agensi, Pentadbir Sistem Agensi, Penjawat Awam

	(d) Pengguna perlu mengikut amalan keselamatan yang baik dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti pengguna.	

3.12. HAK CAPAIAN

Memastikan capaian kepada maklumat dan aset ICT ditakrifkan dan disahkan mengikut keperluan perkhidmatan Kerajaan Sarawak.

ID	KETERANGAN	PERANAN
3.12.1	**Peruntukan Capaian Pengguna** 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 sistem dan perkhidmatan ICT perlu dilaksanakan.	CIO/CDO Agensi, Pentadbir Sistem Agensi, Pengurus Projek, Pembekal Perkhidmatan
3.12.2	**Kajian Semula Hak Capaian Pengguna** Perkara-perkara beritkut perlu dipatuhi: (a) Mewujudkan prosedur penetapan dan penggunaan hak capaian pengguna kepada sistem atau 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 ID tidak aktif perlu dilakukan sekurang-kurangnya sekali setahun; dan (d) Hak capaian ini juga tertakluk kepada kebenaran pemilika system atau perkhidmatan ICT dan juga peraturan-peraturan lain yang berkenaan.	CIO/CDO Agensi, Pentadbir Sistem Agensi, Pengurus Projek, Pembekal Perkhidmatan

3.12.3	**Pembatalan Atau Pelarasan Hak Capaian** Hak capaian pengguna kepada maklumat dan aset yang berkaitan hendaklah disemak dan diselaraskan atau ditamatkan sebelum sebarang perubahan atau penamatan pekerjaan berdasarkan penilaian faktor risiko seperti yang berikut: (a) Sama ada penamatan atau perubahan penempatan oleh pengguna atau pengurusan dan sebab penamatan; dan (b) Tanggungjawab semasa pengguna. Hak capaian kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan peranan, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam organisasi.	CIO/CDO Agensi, Pentadbir Sistem Agensi, Pengurus Projek, Pembekal Perkhidmatan
3.12.4	**Tanggungjawab Pengguna** Memastikan pengguna sistem atau aset maklumat bertanggungjawab melindungi maklumat pengesahan identiti mereka	Penjawat Awam, Pembekal Perkhidmatan

3.13. KESELAMATAN MAKLUMAT DALAM HUBUNGAN DENGAN PEMBEKAL

Menjamin keselamatan semua aset ICT yang digunakan oleh pihak berkepentingan (pembekal, pakar runding dan lain-lain).

ID	KETERANGAN	PERANAN
3.13.1	**Polisi Keselamatan Siber untuk Hubungan dengan Pembekal** Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset Kerajaan Sarawak. Perkara-perkara yang perlu dilaksanakan adalah seperti berikut:	Ketua Agensi, CIO/CDO Agensi, Pengurus Projek ICT Agensi, Penjawat Awam, Pihak Berkepentingan

	(a) Menggunakan proses kitaran hayat (*lifecycle*) atau kaedah yang bersesuaian untuk pengurusan pembekal; (b) Mengawal dan memantau akses oleh pembekal; (c) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; Agensi hendaklah memastikan perkara-perkara berikut: (i) Melaksanakan program kesedaran terhadap Dasar Keselamatan Siber Kerajaan Sarawak dan Akta Rahsia Rasmi 1972 kepada Pembekal Perkhidmatan; (ii) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan Siber Kerajaan Sarawak dan Perakuan Akta Rahsia Rasmi 1972 seperti LAMPIRAN 1 ; dan (iii) Memastikan pembekal perkhidmatan mematuhi Akta Rahsia Rasmi dan Arahan Keselamatan Kerajaan (Pindaan dan Semakan 2017) yang sedang berkuatkuasa dari semasa ke semasa. (iv) Mematuhi tatacara perolehan dan lain-lain prosedur yang berkaitan yang dilkeuarkan oleh Pejabat Setiausaha Kewangan Negeri yang berkuakuasa dari semasa ke semasa berkenaan dengan pembekal.	

3.14. MENANGANI KESELAMATAN DALAM PERJANJIAN DENGAN PEMBEKAL

Mengekalkan tahap persetujuan bagi keselamatan makumat dalam perjanjian dengan pembekal.

ID	KETERANGAN	PERANAN
3.14.1	**Menangani Keselamatan Dalam Perjanjian Pembekal** Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Keperluan keselamatan maklumat hendaklah disediakan dan dipersetujui dengan pembekal yang akan mengakses, memproses, menyimpan, menyampai atau menyediakan perkhidmatan, peralatan atau infrastruktur ICT di agensi Kerajaan Sarawak. (b) Pembekal hendaklah memastikan semua sumber manusia yang terlibat dalam penyediaan perkhidmatan ICT Kerajaan Sarawak mematuhi dan mengambil tindakan kawalan keselamatan yang dikehendaki oleh agensi selaras dengan peraturan dan kawalan keselamatan yang berkuatkuasa dari semasa ke semasa. (c) Penilaian teknikal oleh agensi pusat boleh dilaksanakan sekiranya perlu untuk memastikan keperluan keselamatan dipatuhi; (d) Perakuan penilaian pihak ketiga yang dikemukakan oleh pembekal kepada agensi/agensi pusat sekiranya ianya melibatkan perkhidmatan/pembekalan oleh pihak ketiga; (e) Pembekal hendaklah bersetuju untuk mengemukakan maklumat berhubung perkhidmatan, peralatan atau infrastruktur ICT yang disediakan kepada Kerajaan Sarawak sekiranya diperlukan; (f) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh Kerajaan Sarawak; dan	Ketua Agensi, CIO/CDO Agensi, Pengurus Projek ICT Agensi, Penjawat Awam, Pihak Berkepentingan

	(g) Kegagalan pembekal untuk mematuhi peraturan kawalan keselamatan yang ditetapkan oleh agensi, ketua agensi adalah berhak untuk menghalang pembekal daripada melaksanakan perkhidmatan tersebut.	

3.15. MENGURUS KESELAMATAN MAKLUMAT DALAM RANTAIAN BEKALAN ICT

Mengekalkan tahap persetujuan bagi keselamatan maklumat dalam hubungan pembekal.

ID	KETERANGAN	PERANAN
3.15.1	**Rantaian Bekalan Teknologi Maklumat dan Komunikasi** Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira ialah seperti yang 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.	Ketua Agensi, CIO/CDO Agensi, Pengurus Projek ICT Agensi, Penjawat Awam, Pihak Berkepentingan

3.16. MEMANTAU, MENYEMAK DAN MENGURUS PERUBAHAN PERKHIDMATAN PEMBEKAL

Mengekalkan tahap keselamatan maklumat yang dipersetujui dengan penyampaian perkhidmatan adalah sama seperti mana dinyatakan dalam perjanjian oleh pembekal.

ID	KETERANGAN	PERANAN
3.16.1	**Memantau Dan Mengkaji Semula Perkhidmatan Pembekal** Agensi hendaklah bertanggungjawab untuk sentiasa memantau, mengkaji semula dan menyemak perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memantau tahap prestasi perkhidmatan/pembekalan untuk mengesahkan Pembekal mematuhi perjanjian; (b) Mengkaji laporan status kemajuan perkhidmatan yang dikemukakan oleh Pembekal; dan (c) Mengambil tindakan yang sewajarnya ke atas semua insiden keselamatan siber serta perlanggaran ketidakpatuhan kepada Dasar Keselamatan Siber sekiranya ada.	Ketua Agensi, CIO/CDO Agensi, Pengurus Projek ICT Agensi, Penjawat Awam, Pihak Berkepentingan

3.16.2	**Menguruskan Perubahan Kepada Perkhidmatan Pembekal (Managing Changes to Supplier Services)** Perubahan kepada peruntukan perkhidmatan oleh pembekal yang disebabkan oleh perubahan pada Kerajaan Sarawak, prosedur dan kawalan, hendaklah diuruskan dengan mengambil kira kepentingan data dan maklumat, sistem penyampaian dan proses perkhidmatan yang terlibat dan risiko seperti: (a) Perubahan dalam perjanjian dengan pembekal hendaklah mengikut tatacara perolehan yang dikeluarkan oleh Pejabat Setiausaha Kewangan Negeri yang berkuatkuasa dari semasa ke semasa; (b) Perubahan yang dilakukan oleh Kerajaan Sarawak bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan (c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran Pembekal dan subkontraktor.	Ketua Agensi, CIO/CDO Agensi, Pengurus Projek ICT Agensi, Penjawat Awam, Pihak Berkepentingan

3.17. KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN PENGKOMPUTERAN AWAN

Mengawal data dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang oleh penyedia perkhidmatan. Perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

ID	KETERANGAN	PERANAN
3.17.1	**Keselamatan maklumat bagi penggunaanperkhidmatan pengkomputeran awan** Penggunaan pengkomputeran awan (*cloud computing*) hendaklah dipastikan selamat bagi menjamin	CIO/CDO Agensi, Penjawat Awam

	keselamatan maklumat untuk tujuan perkongsian maklumat dan pemprosesan data. Penggunaan perkhidmatan pengkomputeran awan perlu mendapat kelulusan daripada pihak Kerajaan Sarawak dan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan Sarawak dari semasa ke semasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan penyedia perkhidmatan memenuhi keselamatan siber, kerahsiaan dan kebole-hpercayaan; (b) Menyediakan perjanjian perkhidmatan di antara Kerajaan Sarawak dengan penyedia perkhid-matan; (c) Memastikan SLA dilaksanakan (jika berkaitan); dan (d) Memastikan tiada kebocoran dan penya-lahgunaan data. (e) Memastikan *data residency* seperti berada di Pusat Data Negeri atau tertakluk kepada arahan yang berkuatkuasa dari semasa ke semasa.	

3.18. PERANCANGAN DAN PENYEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

Memastikan tindak balas yang cepat, berkesan, konsisten dan teratur kepada insiden keselamatan maklumat termasuk komunikasi pada kejadian keselamatan maklumat.

ID	KETERANGAN	PERANAN
3.18.1	**Perkongsian Data dan Maklumat** Kerajaan Sarawak mengambil kira keselamatan maklumat apabila berlaku perkongsian data dan maklumat antara Kerajaan Sarawak dengan pihak luar. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Ketua Agensi, CIO/CDO Agensi, Pegawai Data Agensi

	(a) Merujuk kepada polisi, prosedur dan kawalan perkongsian data dan maklumat untuk melindungi data dan maklumat melalui sebarang jenis kemudahan komunikasi; (b) Menyediakan perjanjian atau kebenaran bertulis untuk perkongsian maklumat dan penggunaan perisian di antara Kerajaan Sarawak dengan Kerajaan Persekutuan atau mana-mana pihak luar; (c) Melindungi media yang mengandungi maklumat daripada capaian yang tidak dibenarkan, didedahkan, disalah guna atau dirosakkan semasa pemindahan keluar dari Kerajaan Sarawak; (d) Memastikan maklumat yang terdapat dalam mel elektronik hendaklah dilindungi sebaik-baiknya; (e) Memastikan prosedur keupayaan mengesan dan tanpa sangkalan semasa perkongsian data dan maklumat; (f) Mengenal pasti pihak yang bertanggungjawab terhadap risiko perkongsian data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan (g) Mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.	

3.18.2	**Pengurusan Mel Elektronik (Emel)** Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa yang sedang berkuatkuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah mengenal pasti dan mengesahkan identiti penghantar emel sebelum meneruskan transaksi maklumat. Emel yang diragui atau tidak dikenali hendaklah dilaporkan dan dihapuskan dengan serta merta; (b) Setiap emel rasmi yang dihantar atau diterima hendaklah disimpan dan direkodkan sekiranya diperlukan terutamanya yang mempunyai nilai arkib; (c) Menggunakan akaun emel yang diperuntukkan oleh Kerajaan Sarawak sahaja sebagai emel rasmi; (d) Memastikan pengemaskinian peti mel (*mailbox*) dilaksanakan supaya kapasiti emel tidak melebihi kuota yang telah ditetapkan; (e) Menggunakan akaun emel rasmi untuk tujuan tugas rasmi sahaja; (f) Mengambil tindakan dan memberi maklum balas segera terhadap emel; (g) Memastikan emel rasmi yang dihantar atau diterima disimpan mengikut prosedur pengurusan sistem fail elektronik yang telah ditetapkan; dan (h) Penggunaan dan pengendalian emel di Kerajaan Sarawak hendaklah merujuk kepada mana-mana tatacara pengurusan emel yang berkuat kuasa dari semasa ke semasa.	CIO/CDO Agensi, Penjawat Awam
3.18.3	**Perjanjian Kerahsiaan dan Ketakdedahan (*Non-Disclosure Agreement)*** Syarat-syarat perkongsian hendaklah dinyatakan secara jelas kepada pihak yang akan menerima	Agensi Pusat, Ketua Agensi, CIO/CDO Agensi

	data seperti skop penggunaan, batasan penggunaan (*limit*) serta tanggungjawab pihak tersebut apabila menggunakan data. Selain daripada itu, pihak yang terlibat hendaklah menandatangai perjanjian ketakdedahan terutamanya sekiranya ianya melibatkan data dan maklumat rahsia rasmi. Salinan asal kontrak yang telah ditandatangani hendaklah direkod dan disimpan dengan selamat untuk rujukan sekiranya perlu.	

3.19. PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT

Memastikan kategori dan keutamaan yang efektif dalam kejadian keselamatan maklumat.

ID	KETERANGAN	PERANAN
3.19.1	**Sistem Log dan Pemantauan** Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Bukti log sistem komputer hendaklah didokumentasikan, direkodkan dan disimpan oleh memandangkan ianya adalah merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Ianya hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti- aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan. Log hendaklah disimpan dan direkodkan selaras dengan arahan/ pekeliling terkini yang dikeluarkan oleh Kerajaan dari semasa ke semasa. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti yang berikut: (a) Fail log sistem pengoperasian; (b) Fail log servis (contoh: web, emel);	CDO Agensi Pusat, ICTSO Agensi Pusat, CIO/CDO Agensi, Pentadbir Sistem Agensi

	(c) Fail log aplikasi (*audit trail*); dan (d) Fail log rangkaian (contoh: *switch, firewall, IPS*). Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, aktiviti ini hendaklah dilaporkan kepada ICTSO Kerajaan Sarawak; (d) Pemantauan berterusan boleh dibuat secara automatik dengan menggunakan perisian tertentu sebagai contoh pengimbas virus, *algoritma check sum*, *password cracker*, semakan integriti, pengesanan penceroboh dan analisis pemantauan prestasi sistem komputer; dan (e) Teknologi yang digunakan untuk pemantauan berterusan ditempatkan secara berpusat bagi menjalankan analisis terhadap log yang dikumpulkan dari pelbagai sistem.	

3.20. TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT

Memastikan tindak balas yang efisien dan efektif kepada insiden keselamatan maklumat.

ID	KETERANGAN	PERANAN
3.20.1	**Pengauditan dan Forensik ICT** Pengauditan dan forensik ICT perlu dilaksanakan berdasarkan arahan atau keperluan agensi atau agensi pusat atau mana-mana pihak yang berkuasa. Ia adalah merupakan proses mengenal pasti bahan bukti fizikal dengan menggunakan teknologi dan sains forensik. Perkara-perkara yang perlu dilaksanakan adalah seperti berikut: (a) Memastikan jadual pelaksanaan disediakan;	Ketua Agensi, Agensi Pusat, CIO/CDO Agensi

	(b) Memastikan laporan dapatan dilaksanakan; (c) Memastikan tindakan pembetulan dilaksanakan; dan (d) Memastikan kemudahan penyimpanan log dan maklumat log dilindungi daripada pengubahan tidak sah dan capaian tanpa izin.	

3.21. PENGAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT

Mengurangkan kebarangkalian atau kesan daripada insiden akan datang.

ID	KETERANGAN	PERANAN
3.21.1	**Pembelajaran Daripada Insiden Keselamatan Maklumat** Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya. Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah. Maklumat yang diperoleh daripada penilaian insiden keselamatan maklumat hendaklah digunakan untuk: (a) Mempertingkat pelan pengurusan insiden termasuk senario dan prosedur insiden; (b) Mengenal pasti insiden berulang atau serius dan puncanya untuk mengemas kini penilaian risiko keselamatan maklumat organisasi dan menentukan serta melaksanakan kawalan tambahan yang diperlukan untuk mengurangkan kemungkinan atau akibat kejadian serupa pada masa hadapan; dan (c) Meningkatkan kesedaran dan latihan pengguna dengan memberikan contoh tentang perkara yang boleh berlaku, cara bertindak balas terhadap insiden tersebut dan cara mengelak pada masa hadapan.	CSIRT, ICTSO Kerajaan Sarawak

3.22. KESEDIAAN ICT BAGI KESINAMBUNGAN PERKHIDMATAN

Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

ID	KETERANGAN	PERANAN
3.22.1	**Pelan Kesinambungan Perkhidmatan ICT** Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan* (BCP)) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan ICT. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan ICT organisasi. Pelan ini mestilah diluluskan oleh Ketua Agensi dan ianya hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai pegawai dan pembekal Kerajaan berserta nombor yang boleh dihubungi (faksimili, telefon dan emel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden; (c) Senarai insiden yang boleh menjejaskan penyampaian perkhidmatan ICT bersama-sama dengan kemungkinan dan impak insiden tersebut terhadap keselamatan siber; (d) Program latihan kepada pengguna mengenai prosedur-prosedur kecemasan; (e) Membuat backup mengikut keperluan *Disaster Recovery Plan* (DRP) (jika aplikasi ICT diselenggara sendiri oleh agensi) (f) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (g) Sumber pemprosesan dan lokasi alternatif untuk menggantikan sumber yang telah lumpuh; dan	Ketua Agensi, CIO/CDO Agensi, Pemilik Proses Agensi

	(h) Keperluan mengadakan perjanjian bertulis dengan pembekal perkhidmatan untuk penyambungan semula perkhidmatan dalam tempoh yang ditetapkan salinan BCP perlu disimpan di lokasi berasingan untuk mengelakkan kehilangan dan kerosakan akibat bencana di lokasi utama. (i) BCP hendaklah diuji mengikut keperluan apabila terdapat perubahan dalam persekitaran atau fungsi agensi untuk memastikan ia sentiasa kekal berkesan. (j) Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. (k) Ujian BCP hendaklah dijadualkan untuk memastikan semua pegawai yang terlibat dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. Agensi hendaklah membuat semakan semula apabila diperlu dari semasa ke semasa.	

3.23. KEPERLUAN PERUNDANGAN DAN KONTRAK

Memastikan pematuhan kepada keperluan undang-undang dan peraturan yang berkaitan dengan keselamatan maklumat.

ID	KETERANGAN	PERANAN
3.23.1	**Pematuhan Terhadap Keperluan Perundangan dan Kontrak** Meningkatkan dan memantapkan tahap keselamatan siber bagi mengelakkan pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	Agensi Pusat, Ketua Agensi, CIO/CDO Agensi, Pembekal Perkhidmatan
3.23.2	**Pengenalpastian Keperluan Undang- Undang dan Kontrak Yang Terpakai** Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga JDN dan pembekal serta semua pihak yang terlibat dalam pembekalan perkhidmatan ICT di JDN. Keperluan perundangan yang perlu dipatuhi ialah seperti **LAMPIRAN C** dokumen ini.	Agensi Pusat, Ketua Agensi, CIO/CDO Agensi, Pembekal Perkhidmatan

3.24. HAK HARTA INTELEK

Memastikan pematuhan kepada keperluan undang-undang, peraturan dan perjanjian yang berkaitan dengan hak harta intelek dan penggunaan hak milik produk.

ID	KETERANGAN	PERANAN
3.24.1	**Hak Harta Intelek** Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Semua pihak yang terlibat hendaklah melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Ketua Agensi, CIO/CDO Agensi, Penjawat Awam, Pembekal Perkhidmatan

3.25. PEMATUHAN DASAR, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT

Memastikan keselamatan maklumat yang dilaksanakan dan beroperasi sesuai dengan polisi, peraturan dan piawaian yang dikaji semula secara berkala.

ID	KETERANGAN	PERANAN
3.25.1	**Pematuhan Dasar** Setiap penjawat awam hendaklah memahami dan mematuhi Dasar Keselamatan Siber Kerajaan Sarawak dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di agensi Kerajaan Sarawak adalah hak milik Kerajaan Sarawak. Agensi pusat berhak memantau aktiviti pengguna untuk mengesan penggunaan yang selain daripada tujuan rasmi. Sebarang penggunaan aset ICT milik Kerajaan Sarawak selain daripada maksud dan tujuan rasmi merupakan satu penyalahgunaan sumber.	Agensi Pusat, Ketua Agensi, CIO/CDO Agensi, Penjawat Awam
3.25.2	**Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal** Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap penjawat awam perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal yang ditetapkan (jika ada); dan (b) Aset ICT perlu diperiksa dan dipantau secara berkala atau mengikut keperluan agar ia selaras dengan pematuhan dasar dan piawaian pelaksanaan keselamatan siber.	Ketua Agensi, ICTSO Agensi Pusat, CIO/CDO Agensi, ACIO/ACDO Agensi

3.25.3	**Pematuhan Keperluan Audit** Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem yang beroperasi perlu dirancang dan dipersetujui sebagai satu strategi pencegahan terhadap kebarangkalian berlakunya gangguan dalam penyediaan perkhidmatan.	Ketua Agensi, CIO/CDO Agensi
3.25.4	**Keperluan Perundangan** Semua penjawat awam hendaklah mematuhi keperluan perundangan atau peraturan-peraturan berkaitan seperti di Lampiran B yang berkuatkuasa dari semasa ke semasa. Sebarang keperluan perundangan atau peraturan-peraturan daripada Kerajaan Persekutuan seperti di Lampiran C juga boleh dirujuk.	Penjawat Awam
3.25.5	**Pelanggaran Dasar** Penjawat awam yang melanggar mana-mana peruntukan dalam Dasar Keselamatan Siber Kerajaan Sarawak boleh dikenakan tindakan tatatertib dan undang-undang tertakluk kepada perundangan kerajaan yang berkuat kuasa dari semasa ke semasa.	Agensi Pusat, Ketua Agensi, CIO/CDO Agensi

3.26. DOKUMENTASI PROSEDUR OPERASI STANDARD

Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.

ID	KETERANGAN	PERANAN
3.26.1	**Pengendalian Prosedur Operasi** Perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur pengurusan operasi ICT yang wujud, dikenalpasti dan diguna pakai hendaklah didokumentasi, disimpan dan dikawal; (b) Setiap prosedur mesti mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; (c) Semua prosedur hendaklah dikemaskini mengikut keperluan semasa; (d) Sekiranya operasi dikendalikan oleh pembekal atau pihak ketiga, agensi yang melantik pembekal tersebut hendaklah memastikan pembekal menyediakan prosedur yang berkaitan bagi memastikan apabila berlakunya gangguan kepada sistem, tempoh gangguan adalah minima dan tindakan baik pulih dapat diambil dengan segera.	Agensi Pusat, CIO/CDO Agensi, Pentadbir Sistem Agensi

3.26.2	**Kawalan Perubahan** Prosedur kawalan perubahan konfigurasi hendaklah diwujudkan dan dilaksana bagi sebarang perubahan kepada sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pemilik sistem dan agensi pusat terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pegawai atau pihak yang dilantik dan mempunyai pengetahuan atau terlibat secara langsung dengan sistem berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian sistem hendaklah direkod, didokumentasi dan dikawal bagi mengelakkan berlakunya ralat, untuk tujuan semakan audit atau sebagai rujukan agensi.	Agensi Pusat, CIO/CDO Agensi, Pentadbir Sistem Agensi

4. KAWALAN SUMBER MANUSIA

4.1. PERANAN DAN TANGGUNGJAWAB

Memastikan sumber manusia yang terlibat termasuk Penjawat Awam dan pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.

ID	KETERANGAN	PERANAN
4.1.1	**Sebelum Perkhidmatan** Memastikan semua pengguna yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, kehilangan, penipuan dan penyalahgunaan aset ICT. Perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab penjawat awam serta pihak yang berkepentingan terlibat dalam menjamin keselamatan ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk penjawat awam serta pihak yang berkepentingan berasaskan keperluan perundangan, peraturan dan etika selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; (c) Memastikan semua penjawat awam dan pihak berkepentingan membuat perakuan pematuhan DKS. Perakuan hendaklah dibuat setiap lima (5) tahun jika berada di tempat kerja yang sama atau apabila pegawai berpindah jabatan; (d) Memastikan penjawat awam dan pihak berkepentingan perlu menandatangani Perakuan Akta Rahsia Rasmi 1972; dan (e) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.	Agensi Pusat, Unit Pengurusan Dan Pembangunan Sumber Manusia (UPPSM), Penjawat Awam

4.1.2	**Dalam perkhidmatan** Perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan penjawat awam serta pihak yang berkepentingan mengurus keselamatan ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Kerajaan Sarawak; (b) Memastikan latihan kesedaran berkaitan pengurusan keselamatan aset ICT diberi kepada penjawat awam dan pihak yang berkepentingan (jika perlu) secara berterusan dalam melaksanakan tugas dan tanggungjawab mereka; (c) Memastikan tindakan disiplin dan/atau undang-undang yang sewajarnya ke atas penjawat awam serta pihak yang berkepentingan jika gagal mematuhi perundangan dan peraturan Kerajaan Sarawak yang berkuatkuasa dari masa ke masa; dan (d) Memantapkan pengetahuan bagi memastikan setiap kemudahan ICT digunakan dengan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	Agensi Pusat, UPPSM, CIO/CDO Agensi, Penjawat Awam,

4.1.3	**Bertukar atau Tamat Perkhidmatan** Memastikan pertukaran atau tamat perkhidmatan semua pengguna yang berkepentingan diuruskan dengan teratur. Perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua perkakasan ICT di bawah kawalan dikembalikan kepada agensi mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan merujuk kepada Tatacara Pengurusan Aset Kerajaan Sarawak yang berkuatkuasa dari semasa ke semasa; (b) Memastikan penjawat awam dan pihak berkepentingan perlu melaksanakan perakuan bagi melupuskan semua maklumat terperingkat dalam simpanan secara selamat; dan (c) Memaklumkan kepada CDO berhubung akses kebenaran capaian penjawat awam dan pihak berkepentingan ke atas maklumat dan kemudahan proses maklumat untuk ditamatkan/ditarik balik atau dipinda mengikut peraturan yang ditetapkan oleh Kerajaan Sarawak dan/atau terma perkhidmatan. (d) Menyediakan dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.	Agensi Pusat, UPPSM, CIO/CDO Agensi Penjawat Awam

4.2. PERJANJIAN KERAHSIAAN ATAU KETAKDEDAHAN

Mengekalkan kerahsiaan maklumat yang boleh dicapai oleh warga kerja dan pihak luar/ketiga.

ID	KETERANGAN	PERANAN
4.2.1	**Perjanjian Kerahsiaan atau Ketakdedahan** Syarat-syarat perjanjian kerahsiaan atau ketak-dedahan (non-disclosure agreement) perlu mengambil kira keperluan organisasi dan hen-daklah dikenal pasti dan didokumentasi dan ditandatangani oleh kakitangan Kerajaan Sarawak dan pihak berkepentingan terlibat yang lain. Pembekal atau pihak berkepentingan yang terlibat dengan perkhidmatan ICT Kerajaan Sarawak hendaklah bersetuju dan mematuhi semua keper-luan keselamatan maklumat yang relevan. Perjanjian kerahsiaan dan ketakdedahan bagi setiap pembekal atau pihak berkepentingan yang terlibat dengan perkhidmatan ICT Kerajaan Sarawak ini perlu disemak secara berkala **sekurang-ku-rangnya sekali dalam tempoh setahun** bagi memastikan senarai pihak pembekal atau pihak yang terlibat dengan perkhidmatan ICT Kerajaan Sarawak.	Agensi Pusat Ketua Agensi, CIO/CDO Agensi, Pentadbir Sistem Agensi, Pembekal Perkhidmatan

4.3. BEKERJA SECARA JARAK JAUH

Memastikan keselamatan maklumat bagi kakitangan yang bekerja jarak jauh.

ID	KETERANGAN	PERANAN
4.3.1	**Bekerja Secara Jarak Jauh** Dasar dan langkah-langkah keselamatan hendaklah dilaksanakan bagi melindungi maklumat yang dicapai, diproses atau disimpan secara jarak jauh. Penjawat awam yang bekerja jarak jauh hendaklah memastikan keselamatan maklumat agensi dipatuhi dan tidak disebarkan kepada pihak ketiga.	Agensi Pusat, Pengurusan Sumber Manusia, Penjawat Awam

4.4. PELAPORAN INSIDEN KESELAMATAN MAKLUMAT

Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

ID	KETERANGAN	PERANAN
4.4.1	**Pelaporan Insiden Keselamatan Maklumat** Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat berdasarkan pekeliling atau prosedur pengendalian insiden yang sedang berkuat kuasa. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menentukan mekanisme untuk melaporkan sebarang insiden melalui saluran dan dalam tempoh masa yang ditentukan; (b) Memberi kesedaran berkaitan prosedur pengendalian insiden dan hebahan kepada Penjawat Awam sekiranya terdapat perubahan; dan	Agensi Pusat, CSIRT

	(c) Memastikan pegawai yang mengurus insiden mempunyai kompetensi yang diperlukan. Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT Sarawak berdasarkan prosedur pengendalian insiden yang sedang berkuat kuasa.	

5. KAWALAN FIZIKAL

5.1. PERIMETER KESELAMATAN FIZIKAL

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

ID	KETERANGAN	PERANAN
5.1.1	**Kawalan Kawasan** Kawalan kawasan bertujuan mencegah akses tanpa kebenaran, kerosakan dan gangguan secara fizikal terhadap premis, aset dan maklumat agensi. Perkara yang harus 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 perimeter keselamatan (halangan seperti dinding, pagar kawalan, pengawal keselamatan, *Electronic Security Surveilence System* untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (c) Menghadkan laluan keluar masuk; (d) Mengadakan kaunter kawalan berserta perkhidmatan kawalan keselamatan; (e) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan dan pelawat yang diberi kebenaran sahaja boleh melalui pintu masuk ini;	Unit Keselamatan dan Penguatkuasaan Sarawak (UKPS), Pegawai Keselamatan Jabatan, Penjawat Awam Sarawak

	(f) Mereka bentuk dan susun atur pejabat bagi melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan pejabat; (g) Menyediakan kemudahan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan lain-lain bencana; (h) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (i) Memastikan akses ke kawasan penghantaran, pemunggahan dan lain-lain lokasi terhad hanya kepada pihak yang dibenarkan.	

5.2. KEMASUKAN FIZIKAL

Memastikan penggunaan laluan masuk fizikal kepada maklumat dan aset ICT yang disahkah sahaja.

ID	KETERANGAN	PERANAN
5.2.1	**Kawalan Kemasukan Fizikal** Perkara yang perlu dipatuhi termasuk yang berikut: (a) Penjawat awam hendaklah memakai pas pengenalan jabatan/pas keselamatan sepanjang waktu bertugas; (b) Pas tersebut hendaklah dikembalikan kepada Agensi Kerajaan Sarawak apabila pemilik pas tamat perkhidmatan atau bersara; (c) Pelawat hendaklah melapor diri dan mendapatkan Pas Pelawat di pintu masuk bangunan pejabat/kaunter perkhidmatan Agensi Kerajaan Sarawak dan mengembalikannya selepas tamat urusan. Tarikh, masa dan maklumat pelawat hendaklah direkodkan; dan (d) Kehilangan pas mestilah dilaporkan kepada pihak polis dengan segera.	Pegawai Keselamatan Jabatan, Penjawat Awam, Pelawat Agensi, Pihak yang mempunyai urusan dengan Kerajaan Sarawak

5.3. KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN

Mencegah dari akses fizikal yang tidak sah, kerosakan dan gangguan terhadap maklumat dan aset ICT Kerajaan Sarawak di pejabat, bilik dan kemudahan.

ID	KETERANGAN	PERANAN
5.3.1	**Keselamatan Pejabat, Bilik dan Kemudahan** Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan bilik fail, bilik cetakan, bilik kawalan kamera litar tertutup (CCTV) dan pusat data perlu dihadkan daripada dicapai tanpa kebenaran; (b) Kawasan tempat bekerja, bilik dan tempat operasi ICT perlu dihadkan daripada dicapai oleh orang luar; dan (c) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan.	Agensi Pusat, Ketua Agensi, CIO/CDO Agensi, Pegawai Keselamatan Jabatan

5.4. PEMANTAUAN KESELAMATAN FIZIKAL

Mengesan dan menghalang akses fizikal yang tidak sah.

ID	KETERANGAN	PERANAN
5.4.1	**Pemantauan keselamatan fizikal** Premis fizikal harus dipantau oleh sistem pengawasan termasuk pengawal, penggera pencerobo, sistem pemantauan video seperti CCTV dan perisian pengurusan maklumat keselamatan fizikal sama ada diurus secara dalaman atau oleh penyedia perkhidmatan pemantauan. Sistem pemantauan harus dilindungi daripada capaian yang tidak dibenarkan untuk mengelakkan maklumat pengawasan, seperti suapan video, daripada dicapai oleh orang yang tidak dibenarkan atau sistem diceroboh secara jarak jauh.	Ketua Agensi, CIO/CDO Agensi Pegawai Keselamatan Jabatan,

	Melaksanakan pemantauan secara berterusan di premis bagi mengelakkan capaian secara fizikal yang tidak dibenarkan. Capaian kepada bangunan yang menempatkan sistem kritikal harus dipantau secara berterusan untuk mengesan capaian yang tidak dibenarkan atau tingkah laku yang mencurigakan dengan: (a) Memasang sistem pemantauan video seperti CCTV untuk melihat dan merakam capaian ke kawasan sensitif di dalam dan di luar premis Kerajaan; (b) Memasang, mengikut piawaian terpakai yang berkaitan, dan menguji pengesan sentuhan, bunyi atau gerakan secara berkala untuk mencetuskan penggera pencerobohseperti: (i) Memasang pengesan sesentuh yang mencetuskan penggera apabila sesentuh dibuat atau pecah di mana- mana tempat di mana sentuhan boleh dibuat atau dipecahkan (seperti tingkap dan pintu dan di bawah objek) untuk digunakan sebagai penggera panik; (ii) Memasang pengesan yang sensitif kepada bunyi kaca pecah yang boleh digunakan untuk mencetuskan penggera bagi memberi amaran kepada kakitangan keselamatan; (c) Menggunakan penggera tersebut untuk melindungi semua pintu luar dan tingkap yang boleh dicapai. Kawasan yang tidak berpenghuni perlu sentiasa diberi perhatian; dan (d) Perlindungan juga perlu disediakan untuk kawasan lain (contoh komputer atau bilik komunikasi).	

5.5. BEKERJA DI KAWASAN SELAMAT

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

ID	KETERANGAN	PERANAN
5.5.1	**Bekerja di Kawasan Selamat** Langkah-langkah kawalan keselamatan bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pihak yang dibenarkan sahaja. Kawalan ini dilakukan untuk melindungi aset maklumat yang terdapat dalam premis Kerajaan termasuklah Pusat Data. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Langkah-langkah kawalan keselamatan ke atas kawasan tersebut ialah seperti yang berikut: (a) Sumber data atau pelayan, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik pelayan atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; dan sistem pendinginan yang bersesuaian untuk bilik server. (b) Capaian adalah terhad kepada pihak yang telah diberi kuasa sahaja dan dipantau pada setiap masa; (c) Pemantauan dibuat menggunakan CCTV atau lain-lain peralatan yang sesuai; (d) Peralatan keselamatan (CCTV, log capaian) perlu diperiksa secara berjadual; (e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; (f) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan;	Agensi Pusat, UKPS, Ketua Agensi, CIO/CDO Agensi

	(g) Lokasi premis yang menempatkan aset maklumat serta infrastruktur, peralatan atau perkakasan yang berkaitan hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; (h) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; (i) Memperkukuh dinding dan siling; dan (j) Mengehadkan jalan keluar masuk.	

5.6. POLISI MEJA KOSONG DAN SKRIN KOSONG

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.

ID	KETERANGAN	PERANAN
5.6.1	**Polisi Meja Kosong dan Skrin Kosong** Polisi Meja Kosong dan Skrin Kosong bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna, pada paparan skrin komputer, mesin pencetak, mesin faksimile atau mesin pengimbas apabila pengguna tidak berada di tempatnya. Polisi Meja Kosong dan Skrin Kosong ialah satu set garis panduan yang digunakan dalam pengurusan keselamatan maklumat dan keberkesanan dalam organisasi untuk melindungi maklumat sensitif dan menjaga privasi pekerja. Objektif utama polisi ini adalah untuk memastikan data dan maklumat terjamin keselamatannya dan tidak didedahkan kepada pihak yang tidak mempunyai hak capaian ke atas data atau maklumat tersebut. Polisi ini merangkumi aspek-aspek berikut: (a) Penggunaan fungsi kata laluan penyelamat skrin (*screen saver*	Agensi Pusat, CIO/CDO Agensi, ACIO/ACDO Agensi, Penjawat Awam

	password) atau log keluar apabila meninggalkan komputer; (b) Pengaktifan fungsi mod senyap; (c) Penyimpanan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; (d) Semua dokumen hendaklah diambil segera daripada pencetak, pengimbas, mesin faksim-ile dan mesin fotostat; (e) Pengawalan e-mel masuk dan keluar; (f) Kawalan penggunaan mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital; (g) Penetapanan dan hebahan peraturan serta panduan berkaitan konfigurasi mesej timbul (*pop-up message*) di skrin (contohnya memat-ikan *pop-up* e-mel dan mesej baharu semasa pembentangan, perkongsian skrin atau di kawasan awam); dan (h) Memadamkan maklumat sensitif atau kritikal pada papan putih dan jenis paparan lain apabila tidak diperlukan lagi.	
5.6.2	**Peralatan Pengguna Tanpa Kawalan** Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan me-matuhi perkara yang berikut: (a) Tamatkan sesi aktif apabila selesai tugas; (b) Log keluar komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.	CIO/CDO Agensi, Penjawat Awam

5.7. PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT

Melindungi peralatan ICT Kerajaan Sarawak daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

ID	KETERANGAN	PERANAN
5.7.1	**Penempatan dan Perlindungan Peralatan ICT** Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkah-langkah keselamatan yang perlu diambil ialah seperti yang berikut: (a) Penggunaan kata laluan untuk dicapai ke sistem komputer diwajibkan; (b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing- masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; (d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran CIO/CDO Agensi; (e) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated)* dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; (f) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna; (g) Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;	CIO/CDO Agensi, ACIO/ACDO Agensi, Penjawat Awam, Pegawai Aset

	(h)	Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Gen- Set);	
	(i)	Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan;	
	(j)	Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci;	
	(k)	Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;	
	(l)	Peralatan ICT yang hendak dibawa ke luar premis jabatan, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan;	
	(m)	Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden;	
	(n)	Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;	
	(o)	Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pegawai Aset;	
	(p)	Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pegawai Aset untuk dibaik pulih;	
	(q)	Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;	
	(r)	Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal tanpa kebenaran;	

	(s) Pengguna dilarang sama sekali mengubah kata laluan pentadbir yang telah ditetapkan; dan (t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi kerajaan sahaja.	

5.8. KESELAMATAN ASET DI LUAR PREMIS

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

ID	KETERANGAN	PERANAN
5.8.1	**Keselamatan Aset di Luar Premis** Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis jabatan. Peralatan yang dibawa keluar dari premis jabatan adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (c) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	CIO/CDO Agensi, ACIO/ACDO Agensi, Penjawat Awam, Pembekal Pihak Berkepentingan

5.9. MEDIA STORAN

Memastikan pendedahan, pengubahsuaian, penghapusan dan pemusnahan yang sah pada media storan.

ID	KETERANGAN	PERANAN
5.9.1	**Pengurusan Media Boleh Alih** Untuk mengelakkan kerosakan pada aset maklumat dan gangguan kepada aktiviti perkhidmatan, media boleh alih harus dikawal dan dilindungi secara fizikal. Media boleh alih mesti dikendalikan mengikut klasifikasi maklumat. Prosedur-prosedur pengendalian media yang perlu dipatuhi ialah seperti yang berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan (e) Menyimpan semua jenis media di tempat yang selamat.	CIO/CDO Agensi, ACIO/ACDO Agensi, Pegawai Aset
5.9.2	**Pelupusan Media** Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan; dan Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	CIO/CDO Agensi, ACIO/ACDO Agensi, Pegawai Aset

5.9.3	**Pengalihan Aset** Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran JDN terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: (a) Peralatan ICT yang hendak dibawa keluar dari premis jabatan untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Agensi atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan (b) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	CIO/CDO Agensi, ACIO/ACDO Agensi, Pegawai Aset
5.9.4	**Pengendalian Media** Melindungi aset maklumat daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	CIO/CDO Agensi, ACIO/ACDO Agensi, Pegawai Aset, Penjawat Awam

5.10. PENYELENGGARAAN PERKAKASAN ICT

Mencegah maklumat dan aset ICT dari hilang, rosak dan dikompromi atau gangguan kepada operasi agensi berpunca dari kekurangan penyelenggaran.

ID	KETERANGAN	PERANAN
5.10.1	**Penyelenggaraan Peralatan** Perkakasan ICT hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penyelenggaraan perkakasan ICT yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh agensi pusat; Penyelenggaraan perkakasan ICT hendaklah mematuhi spesifikasi yang ditetapkan oleh agensi pusat dan tatacara pengurusan aset yang berkuatkuasa dari semasa ke semasa. (b) Memastikan perkakasan ICT hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Pengurus aset/pegawai aset bertanggungjawab terhadap penyelenggaraan setiap perkakasan ICT dalam tempoh jaminan sehingga masa untuk pelupusan; (d) Menyemak dan menguji semua perkakasan ICT sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Sebarang penyelenggaraan mestilah mendapat kebenaran daripada pengurus aset/pegawai aset.	CIO/CDO Agensi, ACIO/ACDO Agensi, Pentadbir Sistem Agensi, Pegawai Aset

5.11. PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN

Mencegah ketirisan maklumat dari peralatan yang mengandungi media storan yang perlu dilupuskan atau diguna semula.

ID	KETERANGAN	PERANAN
5.11.1	**Pelupusan yang Selamat atau Penggunaan Semula Peralatan** Pelupusan melibatkan perkakasan ICT yang telah rosak, usang dan tidak boleh dibaikpulih sama ada harta modal atau inventori yang dibekalkan, perlu melalui prosedur semasa dan dilakukan secara terkawal untuk memastikan keselamatan maklumat.Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pelupusan perkakasan ICT hendaklah mengikut prosedur atau tatacara pelupusan semasa yang berkuat kuasa; dan (b) Perkakasan ICT yang hendak dilupuskan perlulah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (c) Semua kandungan peralatan ICT khususnya maklumat buangan rahsia rasmi hendaklah melalui proses sanitasi media dihapuskan terlebih dahulu sebelum pelupusan; (d) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; (e) Data-data dalam storan peralatan ICT yang akan dilupuskan secara pindah milik hendaklah dihapuskan dengan cara yang selamat; (f) Pengguna adalah dilarang untuk melakukan perkara seperti berikut: (i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk menjadi milik peribadi; (ii) Mencabut, menanggal dan menyimpan alat ganti, aksesori dan komponen komputer; dan	CIO/CDO Agensi, ACIO/ACDO Agensi, Pentadbir Sistem Agensi, Pegawai Data, Pegawai Aset,

	(iii) Memindah keluar dari lokasi asal mana-mana peralatan ICT yang hendak dilupuskan; dan (iv) Membuat pendua kepada maklumat rahsia rasmi sebelum maklumat tersebut dihapuskan daripada peralatan ICT.	

6. KAWALAN TEKNOLOGI

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

6.1. Peralatan Pengguna

ID	KETERANGAN	PERANAN
6.1.1	**Peralatan Mudah Alih** 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.	CIO/CDO Agensi, Penjawat Awam
6.1.2	**Peralatan Pengguna Yang Tiada Pengawasan** 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.	CIO/CDO Agensi, Penjawat Awam

6.2. HAK CAPAIAN ISTIMEWA

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

ID	KETERANGAN	PERANAN
6.2.1	**Pengurusan Hak Capaian Istimewa** Peruntukan dan penggunaan hak capaian istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak capaian perlu diberikan kawalan dan penyeliaan yang ketat mengikut keperluan skop tugas yang telah dikenal pasti berdasarkan prosedur yang berkuat kuasa.	CIO/CDO Agensi, Pentadbir Sistem Agensi, Penjawat Awam

6.3. SEKATAN CAPAIAN MAKLUMAT

Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat dalam sistem aplikasi.

ID	KETERANGAN	PERANAN
6.3.1	**Sekatan Capaian Maklumat** 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;	CIO/CDO Agensi, Pentadbir Sistem Agensi, Pegawai Data

	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.	

6.4. PENGESAHAN IDENTITI YANG SELAMAT

ID	KETERANGAN	PERANAN
6.4.1	**Prosedur Log Masuk yang Selamat** Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan ialah seperti yang berikut: (i) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Jabatan; (ii) Menjana amaran (*alert*) sekiranya berlaku perlanggaran semasa proses log maşuk terhadap aplikasi sistem; (iii) Mengawal capaian ke atas aplikasi sistem mengikut prosedur yang ditetapkan; (iv) Mewujudkan teknik pengesahan pelbagai faktor (*multi factor authentication* - MFA) berdasarkan pengkelasan maklumat yang bersesuaian bagi mengesahkan pengenalan diri pengguna;	CIO/CDO Agensi, Pentadbir Sistem Agensi

	(v) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan yang kukuh dan berkualiti; dan (vi) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	
6.4.2	**Sistem Pengurusan Kata Laluan** Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh Agensi Pusat seperti yang 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 atau setelah mencapai tempoh masa pertukaran kata laluan yang ditetapkan oleh Pentadbir Sistem Agensi; c) Panjang kata laluan mestilah sekurang-kurangnya **DUA BELAS (12) AKSARA** dengan gabungan antara huruf, aksara khas dan nombor (*alphanumeric*) **KECUALI** bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekali pun e) Fungsi kunci skrin (*lock screen*) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan dalam atur cara; g) Kuat kuasa pertukaran kata laluan semasa yang ditetapkan oleh sistem secara automatik (*default password)* selepas login kali pertama atau selepas tetapan semula kata laluan; h) Kata laluan tidak berdasarkan perkataan kamus atau gabungannya;	CIO/CDO Agensi, Pentadbir Sistem Agensi

	i) Kata laluan yang sama tidak digunakan merentas perkhidmatan dan sistem yang berbeza; j) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; k) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum **TIGA (3) KALI** sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; dan l) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	

6.5. PENGURUSAN KAPASITI

Memastikan kapasiti yang diperlukan oleh kemudahan pemprosesan, maklumat, sumber manusia, pejabat dan kemudahan lain.

ID	KETERANGAN	PERANAN
6.5.1	**Pengurusan Kapasiti** Kapasiti sesuatu komponen atau sistem aplikasi hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai penyelaras projek yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan, kegunaan dan operasi sistem aplikasi pada masa akan dating. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	CIO/ CDO Agensi, Pentadbir Sistem Agensi Agensi

6.6. PERLINDUNGAN DARIPADA PERISIAN HASAD

Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti *virus*, *trojan*, *malware* dan sebagainya.

ID	KETERANGAN	PERANAN
6.6.1	**Perlindungan daripada Perisian Hasad** Perkara yang perlu dipatuhi adalah seperti berikut: a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti *antivirus*, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan dan penyelenggaraan yang betul, selamat dan diluluskan oleh agensi pusat; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah undang-undang yang berkuatkuasa dan diluluskan oleh agensi pusat; c) Mengimbas semua perisian atau sistem dengan anti-virus sebelum menggunakannya; d) Mengemaskini perisian anti-virus dengan versi yang terkini dan ditetapkan oleh agensi pusat; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan data dan maklumat; f) Meningkatkan kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian dan sistem tersebut mengandungi program berbahaya; h) Pengguna dikehendaki melapor sebarang ralat mengenai ancaman keselamatan siber kepada CIO/CDO agensi untuk tindakan lanjut. CIO/CDO haruslah memajukan laporan kepada CSIRT Kerajaan Sarawak. Penggunaan *mobile*	Agensi Pusat, CSIRT, CIO/CDO Agensi, Pentadbir Sistem Agensi

	code hendaklah daripada sumber yang sah dan dipercayai. i) Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada serangan perisian hasad hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut.	

6.7. PENGURUSAN KERENTANAN TEKNIKAL

Memastikan kawalan teknikal kerentanan (*vulnerability*) adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.

ID	KETERANGAN	PERANAN
6.7.1	**Kawalan dari Ancaman Teknikal** Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b) Memastikan maklumat ancaman diperolehi daripada sumber yang sahih; c) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan d) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan	Agensi Pusat, CIO/CDO Agensi, Pentadbir Sistem Agensi, Pembekal Perkhidmatan

6.8. PENGURUSAN KONFIGURASI

Memastikan peralatan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul, aturan keselamatan yang diperlukan dan konfigurasi tidak diubah oleh perubahan yang tidak sah dan tidak betul.

ID	KETERANGAN	PERANAN
6.8.1	**Pengurusan konfigurasi** Pengurusan konfigurasi perlu dilaksanakan untuk memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul berserta dengan keperluan keselamatan. Konfigurasi tidak diubah tanpa kebenaran berdasarkan prosedur yang ditetapkan. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Melindungi capaian terhadap fail konfigurasi mengikut kawalan yang ditetapkan; (b) Merekod dan menyimpan sebarang perubahan konfigurasi dengan selamat; dan (c) Memantau konfigurasi untuk mengesahkan tetapan konfigurasi dan menilai kawalan keselamatan.	Agensi Pusat, Pembekal Perkhidmatan

6.9. PENGHAPUSAN MAKLUMAT

Mencegah pendedahan maklumat sensitif yang tidak sewajarnya dan mematuhi undang-undang, peraturan dan keperluan perjanjian dalam penghapusan maklumat.

ID	KETERANGAN	PERANAN
6.9.1	**Kawalan Penghapusan Maklumat** Keselamatan maklumat penting bagi perlindungan data-dalam penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	CIO/CDO Agensi, Pegawai Data

	(i) Maklumat terperingkat hanya boleh dilakukan penduaan dan penyalinan pada media storan oleh Pengguna yang dibenarkan sahaja; (ii) Menggunakan teknologi enkripsi dan lain-lain kaedah keselamatan yang bersesuaian ke atas maklumat terperingkat yang disediakan dan di-hantar secara elektronik; dan (iii) Semua maklumat terperingkat hendaklah **dihapuskan** mengikut prosedur pelupusan se-masa yang sedang berkuatkuasa.	

6.10. SANDARAN *(BACKUP)* MAKLUMAT

Membolehkan salinan maklumat, perisian dan sistem diselenggara dan diuji secara berkala berdasarkan polisi tajuk khusus berkaitan *backup*.

ID	KETERANGAN	PERANAN
6.10.1	**Sandaran *(Backup)* Maklumat** Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara berkala mengikut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di off site. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi; (c) Menguji sistem sandaran sedia ada secara berkala **sekurang-kurangnya setahun sekali** bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan	Agensi Pusat, CIO/CDO Agensi, Pentadbir Sistem Agensi

	(d) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang- kurangnya TIGA GENERASI.	

6.11. PENGELOGAN *(Logging)* MAKLUMAT

Merekod kejadian, menjana pembuktian, memastikan integriti maklumat log, mencegah capaian tidak sah, mengenal pasti kejadian keselamatan makumat yang membawa kepada insiden keselamatan maklumat dan menyokong penyiasatan.

ID	KETERANGAN	PERANAN
6.11.1	**Menyediakan Log** Sistem yang dibangunkan perlu merekod aktiviti dan menjana bahan bukti untuk memastikan maklumat log adalah berintegriti dan boleh digunakan sebagai bahan bukti jika berlaku insiden keselamatan maklumat. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menyedia, menyimpan, melindungi dan menganalisis log yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa berkaitan keselamatan maklumat; (b) Log hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti- aktiviti yang tidak normal serta aktiviti- aktiviti yang tidak dapat dijelaskan; (c) Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi pelayan dan aplikasi yang perlu diaktifkan ialah seperti yang berikut: • Fail log sistem pengoperasian; • Fail log perkhidmatan (*service*) • Fail log aplikasi (*audit trail*); dan • Fail log rangkaian	Agensi Pusat; CIO/CDO Agensi; Pentadbir Sistem Agensi, Pembekal Perkhidmatan

ID	KETERANGAN	PERANAN
6.11.2	**Jejak Audit** Setiap sistem mesti 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) Catatan jejak audit hendaklah disemak dari semasa ke semasa dan menyediakan laporan jika perlu; dan (f) Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	CIO/CDO Agensi; Pentadbir Sistem Agensi

6.12. AKTIVITI PEMANTAUAN

Mengesan tingkah laku anomali dan potensi kepada insiden keselamatan maklumat.

ID	KETERANGAN	PERANAN
6.12.1	**Aktiviti Pemantauan** 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 aplikasi yang kritikal dan lain-lain; (c) Log dari peralatan/perisian keselamatan (contoh: *antivirus*, IDS, IPS, *firewall* dan lain-lain; (d) Log kejadian berkaitan aktiviti sistem dan rangkaian; (e) Penggunaan kod yang disahkan tidak disalah guna; dan (f) Penggunaan sumber (contoh: CPU, *hard disk*, *memory* dan *bandwidth*).	Agensi Pusat, CIO/CDO Agensi, Pentadbir Sistem Agensi, Pembekal Perkhidmatan

6.13. PENYEGERAKAN WAKTU

Membolehkan korelasi dan analisis kejadian berkaitan keselamatan dan lain-lain data yang direkodkan dan untuk menyokong siasatan kepada insiden keselamatan maklumat.

ID	KETERANGAN	PERANAN
6.13.1	**Penyegerakan Waktu** Waktu bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut waktu piawai Malaysia.	Agensi Pusat, Pentadbir Sistem Agensi, Pembekal Perkhidmatan

6.14. PEMASANGAN PERISIAN PADA SISTEM OPERASI

Memastikan integriti pada sistem operasi dan mengelakkan eksploitasi kepada kerentanan (*vulnerabilities*) teknikal.

ID	KETERANGAN	PERANAN
6.14.1	**Pemasangan Perisian pada Sistem yang Operasi** Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut: (a) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian dilaksanakan dan di-peraku berjaya; (b) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur; (c) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan agensi; (d) Sistem aplikasi dalaman tidak dibenarkan didemonstrasikan atau diagih kepada pihak lain kecuali dengan kebenaran Agensi Pusat; dan (e) Lesen perisian (*registration code*, *serials*, *CD-keys*) perlu disimpan berasingan daripada *CD-ROM*, disk atau media berkaitan bagi menge-lakkan dari berlakunya kecurian atau cetak rompak.	Agensi Pusat, CIO/CDO Agensi, Pentadbir Sistem Agensi, Pembekal Perkhidmatan
6.14.2	**Sekatan ke atas pemasangan perisian** Semua pengguna dilarang membuat pemasangan sebarang perisian tambahan tanpa kebenaran CIO/CDO agensi.	CIO/CDO Agensi, Penjawat Awam

6.15. KESELAMATAN RANGKAIAN

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

ID	KETERANGAN	PERANAN
6.15.1	Sistem aplikasi hendaklah dikawal dan diurus dengan baik dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah ditempatkan di bilik khas yang mempunyai ciri-ciri fizikal yang selamat, bersih dan bebas dari sebarang risiko seperti kebakaran dan banjir; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada agensi pusat atau mana-mana pihak yang dilantik oleh agensi pusat; (d) Sebarang penyambungan rangkaian selain SarawakNet adalah tidak dibenarkan. Mana-mana pemasangan selain rangkaian SarawakNet perlu mendapat kelulusan agensi pusat.; (e) Pengguna hanya dibenarkan untuk menggunakan rangkaian SarawakNet sahaja untuk kegunaan rasmi. Penggunaan rangkaian peribadi (sambungan dari *mobile broadband*) semasa di pejabat adalah tidak dibenarkan; (f) Agensi pusat akan memantau dan mengawal penggunaan *wireless* LAN; (g) Sekiranya perkhidmatan rangkaian diperolehi secara *outsource*, perjanjian perkhidmatan rangkaian hendaklah sentiasa dipantau bagi mematuhi tahap perkhidmatan yang telah ditetapkan; (h) Bagi mana-mana agensi Kerajaan Sarawak yang menggunakan aplikasi Kerajaan Persekutuan atau sebaliknya, capaian hendaklah melalui laluan integrasi rangkaian SarawakNet-MyGovNet atau mana-mana rangkaian yang ditetapkan; dan	Agensi Pusat, Ketua Agensi, CIO/CDO Agensi, Pembekal Perkhidmatan

	(i) Memantau dan mengawal capaian pengguna yang dibenarkan sahaja mengakses kepada perkhidmatan rangkaian SarawakNet.	

6.16. PENAPISAN WEB (*WEB FILTERING*)

Untuk melindungi sistem daripada terjejas oleh perisian hasad dan untuk menghalang akses kepada sumber web yang tidak dibenarkan.

ID	KETERANGAN	PERANAN
6.16.1	**Penapisan Web** Memasang *Web Content Filtering* pada *Internet Gateway* atau kawalan capaian internet yang bersesuaian untuk menyekat aktiviti/capaian laman web yang dilarang.	Agensi Pusat, CIO/CDO Agensi, Pembekal Perkhidmatan

6.17. PENGGUNAAN KRIPTOGRAFI

Melindungi kerahsiaan, integrati dan kesahihan maklumat melalui kawalan kriptografi.

ID	KETERANGAN	PERANAN
6.17.1	**Enkripsi** Semua maklumat sensitif atau maklumat rahsia rasmi yang termaktub dalam buku Arahan Keselamatan hendaklah membuat enkripsi pada setiap masa sekurang-kurangnya dengan penggunaan kata laluan.	Agensi Pusat, CIO/CDO Agensi, Pegawai Data, Pembekal Perkhidmatan
6.17.2	**Tandatangan Digital** Selaras dengan *Electronic Sarawak Government Activities* (ESGA) 2022, penggunaan tandatangan digital adalah dibenarkan kepada semua warga kerja Kerajaan Sarawak untuk menguruskan maklumat rahsia rasmi secara elektronik. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan tandatangan digital hendaklah mendapat kelulusan daripada agensi pusat;	Agensi Pusat, CIO/CDO Agensi, Pegawai Data, Penjawat Awam, Pembekal Perkhidmatan

	(b) Permohonan dan pembaharuan tandatangan digital hendaklah dibuat melalui agensi pusat; (c) Penggunaan tandatangan digital adalah untuk pengguna yang mempunyai akses tertentu khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik; dan (d) Sijil Digital yang digunakan hendaklah diperoleh daripada Pihak Berkuasa Pemerakuan Berlesen (*Authorised Certificate Authority*) yang dilantik oleh agensi pusat.	
6.17.3	**Pengurusan Infrastruktur Kunci Awam** Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengurusan ke atas PKI hendaklah dilakukan dengan baik bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut; dan (b) Kunci persendirian mesti disimpan dengan selamat dan hanya digunakan oleh entiti yang memilikinya sahaja bagi tujuan nyahsulit atau mewujudkan tandatangan digital. Kunci awam tersedia bagi ahli kumpulan yang menggunakan enkripsi bagi menentusah tandatangan digital yang diterima.	Agensi Pusat, Ketua Agensi, CIO/CDO Agensi, Penjawat Awam

6.17.4	**Sijil Digital** Sijil Digital adalah sijil yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (*Certificate Authority* (CA)) untuk mengesahkan tanpa penafian identiti pengguna atau pelayan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan sijil digital hendaklah dilaksanakan dalam capaian aplikasi yang ditetapkan; (b) Sijil Digital terdapat dalam tiga (3) medium iaitu *token, roaming dan softcert*; dan (c) Semua akses dan peranan Pengguna yang bertukar keluar/ bersara hendaklah dimaklumkan kepada agensi pusat untuk disekat dan ditamatkan sijil digitalnya melalui sistem aplikasi yang ditetapkan oleh CIO/CDO/ACIO agensi.	Agensi Pusat, Ketua Agensi, CIO/CDO Agensi, Penjawat Awam

6.18. PEMBANGUNAN SISTEM YANG SELAMAT

Memastikan supaya pembangunan sistem aplikasi secara dalaman dan *outsource* diselia dan dipantau untuk memastikan ia mengikut prosedur serta tatacara berkaitan yang telah ditetapkan.

ID	KETERANGAN	PERANAN
6.18.1	**Pembangunan Sistem Aplikasi** Sistem aplikasi membantu pengguna melaksanakan tugas rasmi harian. Contoh sistem aplikasi adalah sistem aplikasi pengurusan data. Sistem aplikasi juga merujuk kepada sistem aplikasi web dan sistem aplikasi mudah alih. Sistem aplikasi yang selamat perlu dibangunkan meliputi seluruh kitar hayat pembangunan sistem aplikasi berdasarkan prosedur pembangunan sistem aplikasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Permohonan pembangunan sistem aplikasi secara rasmi hendaklah dikemukakan kepada agensi pusat untuk kelulusan; (b) Permohonan hendaklah lengkap meliputi spesifikasi teknikal, anggaran kos yang terlibat,	Agensi Pusat, CIO/CDO Agensi, Pengurus Projek ICT Agensi

	guna tenaga dan juga skop perluasan sistem aplikasi tersebut; (c) Permohonan pembangunan sistem aplikasi secara rasmi hendaklah dikemukakan kepada agensi pusat untuk kelulusan; (d) Permohonan hendaklah lengkap meliputi spesifikasi teknikal, anggaran kos yang terlibat, guna tenaga dan juga skop perluasan sistem aplikasi tersebut; (e) Pembangunan sistem aplikasi hendaklah mengambil kira sistem aplikasi sedia ada di agensi pusat bagi mengelakkan pertindihan pembangunan sistem aplikasi yang sama; (f) Pembangunan sistem aplikasi mestilah menggunakan kod-kod piawaian di bawah *data dictionary* yang diselenggara oleh agensi pusat; (g) Pemilik Sistem aplikasi bertanggungjawab mempromosi dan memastikan kelancaran pelaksanaan sistem; (h) Pemilik Sistem aplikasi hendaklah membaca dan memahami dokumentasi serta mematuhi prosedur yang berkaitan; (i) Pemilik Sistem aplikasi perlu melaporkan kepada agensi pusat secara berkala bagi kemajuan pelaksanaan sistem aplikasi; (j) Pembangunan sistem aplikasi hendaklah menggunakan teknik pengaturcaraan dan pangkalan data yang selamat; (k) Sistem aplikasi gunasama boleh didemonstrasi atau diagihkan kepada Kementerian/Jabatan lain dengan kebenaran agensi pusat; (l) Kod sumber sistem aplikasi hendaklah disimpan dengan teratur dan sebarang pindaan hendaklah direkodkan bagi tujuan kawalan versi; (m) Proses perolehan pembangunan sistem aplikasi secara *outsource* perlu dilakukan melalui prosedur perolehan yang sedang berkuatkuasa dari semasa ke semasa;	

6.18.2	**Pembangunan Sistem Aplikasi Mudah Alih** Sistem aplikasi mudah alih yang selamat perlu dibangunkan meliputi seluruh kitar hayat pembangunan sistem aplikasi Kerajaan Sarawak berdasarkan Prosedur Pembangunan Sistem Aplikasi ICT Kerajaan Sarawak semasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pembangunan sistem aplikasi mudah alih hendaklah melaksanakan pengujian sebelum dimuatnaik; (b) Penyediaan sistem aplikasi mudah alih kepada orang awam hendaklah melalui perkhidmatan SCS Gov App atau mana-mana aplikasi yang telah ditetapkan; dan (c) Pembangunan sistem aplikasi mudah alih yang melibatkan integrasi antara sistem hendaklah menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang tidak memberi risiko ancaman keselamatan.	Agensi Pusat, Ketua Agensi, CIO/CDO Agensi

6.19. KEPERLUAN KESELAMATAN APLIKASI

Menjaga dan menjamin keselamatan dan kesahihan sistem maklumat dan aplikasi.

ID	KETERANGAN	PERANAN
6.19.1	**Prosedur Kawalan Perubahan** Perubahan pada sistem aplikasi dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan Prosedur Kawalan Perubahan Sistem yang telah ditetapkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem aplikasi dan/atau pakej perisian hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;	Agensi Pusat, CIO/CDO Agensi, Pentadbir Sistem Agensi

	(b) Sistem aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian dan/atau pangkalan data untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan Kerajaan Sarawak. (c) CIO/CDO perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh Pembekal; (d) Akses kepada kod sumber sistem aplikasi perlu dihadkan kepada Pengguna yang dibenarkan sahaja; dan (e) Sebarang kemungkinan kebocoran maklumat hendaklah dihalang. (f) Hanya pegawai bertauliah yang dilantik oleh Ketua Agensi sahaja boleh mengakses kod sumber sistem aplikasi dan ianya mesti dikawal untuk mengelakkan sebarang kebocoran maklumat; dan (g) Semua pembekal tidak boleh melakukan ujian dan latihan menggunakan *live server* atau dalam persekitaran SarawakNet.	Agensi Pusat, CIO/CDO Agensi, Pentadbir Sistem Agensi

6.20. PENGATURCARAAN PROGRAM SELAMAT

Memastikan aplikasi dibangunkan dengan selamat dan mengurangkan potensi kerentanan (*vulnerability*) keselamatan maklumat di dalam aplikasi.

ID	KETERANGAN	PERANAN
6.20.1	**Kawalan capaian kepada kod sumber** Kawalan capaian kepada kod sumber atau atur cara program perlu dilaksanakan bagi mengelakkan kecurian, pengubahsuaian dan penghapusan tanpa kebenaran. Kod sumber bagi semua aplikasi dan perisian ialah hak milik Kerajaan.	Agensi Pusat, CIO/CDO Agensi, Pentadbir Sistem Agensi, Pengurus Projek ICT Agensi, Pembekal Perkhidmatan

6.21. PENGUJIAN DAN PENERIMAAN KESELAMATAN SISTEM

Mengesahkan keperluan keselamatan maklumat dicapai semasa aplikasi atau kod dilancarkan ke persekitaran produksi.

ID	KETERANGAN	PERANAN
6.21.1	**Pengujian Keselamatan Sistem** Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; (b) Membuat semakan pengesahan dalam aplikasi untuk mengenal pasti kesilapan maklumat; (c) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan; (d) Melakukan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem; dan (e) Menjalankan ujian penembusan untuk mengenal pasti kod dan reka bentuk yang tidak selamat.	CIO/CDO Agensi, Pentadbir Sistem Agensi, Penjawat Awam

6.21.2	**Pengujian Penerimaan Sistem** Semua sistem baru (termasuk sistem yang dikemas kini atau diubah suai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	CIO/CDO Agensi, Pentadbir Sistem Agensi

6.22. PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PRODUKSI

Melindungi persekitaran produksi dan data dari dikompromi semasa aktiviti pembangunan dan pengujian.

ID	KETERANGAN	PERANAN
6.22.1	**Keperluan Pengasingan Persekitaran Pembangunan, Pengujian dan Produksi** 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.	Agensi Pusat, CIO/CDO Agensi, Pengurus Projek ICT Agensi, Pentadbir Sistem Agensi, Pembekal Perkhidmatan
6.22.2	**Persekitaran Pembangunan Yang Selamat** Mewujudkan dan melindungi persekitaran pembangunan supaya selamat untuk pembangunan sistem dan integrasi yang meliputi seluruh kitar hayat pembangunan sistem. Semua agensi perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira:	Agensi Pusat, CIO/CDO Agensi, Pengurus Projek ICT Agensi, Pentadbir Sistem Agensi, Pembekal Perkhidmatan

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

6.23. PENGURUSAN PERUBAHAN

Memelihara keselamatan maklumat ketika melaksanakan perubahan.

ID	KETERANGAN	PERANAN
6.23.1	**Pengurusan Perubahan** Prosedur kawalan perubahan konfigurasi hendaklah diwujudkan dan dilaksana bagi sebarang perubahan kepada sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pemilik sistem dan agensi pusat terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pegawai atau pihak yang dilantik dan mempunyai pengetahuan atau terlibat secara langsung dengan sistem berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian sistem hendaklah direkod, didokumentasi dan dikawal bagi mengelakkan berlakunya ralat, untuk tujuan semakan audit atau sebagai rujukan agensi.	Agensi Pusat, CIO/CDO Agensi, Pegawai Data, Pegawai Aset

6.24. DATA PENGUJIAN

Memastikan perkaitan pengujian dan perlindungan maklumat operasi yang digunakan untuk pengujian.

ID	KETERANGAN	PERANAN
6.24.1	**Perlindungan Data Ujian** Untuk memastikan perlindungan ke atas maklumat yang digunakan untuk pengujian, data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; (b) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; (c) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; (d) Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar; (e) Melindungi maklumat sensitif melalui penyingkiran atau pengaburan data jika digunakan untuk ujian; (f) Memadam maklumat operasi daripada persekitaran ujian serta-merta dengan betul selepas ujian selesai untuk mengelakkan penggunaan maklumat ujian tanpa kebenaran.	Agensi Pusat, Pengurus Projek ICT Agensi, Pentadbir Sistem Agensi, Pembekal Perkhidmatan

6.25. PERLINDUNGAN SISTEM MAKLUMAT SEMASA PELAKSANAAN AUDIT

Meminimumkan kesan audit dan lain-lain aktiviti jaminan terhadap sistem operasi dan proses perkhidmatan agensi.

ID	KETERANGAN	PERANAN
6.25.1	**Kawalan Audit Sistem Maklumat** Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan di-persetujui bagi mengurangkan kebarangkalian ber-laku gangguan dalam penyediaan perkhidmatan.	CIO/CDO Agensi, Pentadbir Sistem Agensi, Pihak Berkepentingan

LAMPIRAN A

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN SIBER KERAJAAN SARAWAK

Nama Penuh Pegawai (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan / Gred : .....

Agensi : .....

Adalah dengan sesungguhnya saya memperakui bahawa: -

1. Sebagai penjawat awam Kerajaan Sarawak, saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan Siber Kerajaan Sarawak; dan
2. Sekiranya saya tidak mematuhi mana-mana perkara di dalam dasar ini, yang mana telah menyebab wujudnya sebarang risiko dan mendatangkan ancaman keselamatan siber kepada agensi serta Kerajaan, saya boleh dianggap cuai dan maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan Pegawai : .....

Tarikh : .....

Pengesahan Ketua Agensi

.....

(Tandatangan Ketua Agensi)

Cop Rasmi Jabatan

Ketua Agensi: .....

Tarikh : .....

LAMPIRAN B

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua penjawat awam Negeri:

(a) Surat Pekeliling ICT No.3/2012 - Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 (ISMS) Dalam Sektor Awam Negeri
(b) Surat Pekeliling ICT No.4/2012 - Penilaian Risiko Keselamatan Maklumat Sektor Awam Negeri
(c) Surat Pekeliling ICT No.5/2012 - Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam
(d) Surat Pekeliling ICT No.1/2010 - Capaian Internet Bagi Pegawai Sokongan (Gred 27-38), Jurutrengkas, Seetiausaha Sulit kepada Menteri dan Menteri Muda di Sektor Awam Kerajaan Sarawak
(e) Surat Pekeliling ICT No. 4/2008 - Penggunaan Telefon Mudah Alih Blackberry
(f) Surat Pekeliling ICT No. 1/2008 - Garis Panduan Mengenai Pembangunan Dan Penyelenggaraan Laman Web/Portal Kerajaan Sarawak
(g) Surat Pekeliling No. 2/2007 - Penyediaan Piagam Pelanggan Di Laman Web/Portal Agensi Kerajaan
(h) Surat Pekeliling ICT No. 3/2007 - Langkah-langkah Mengenai Penggunaan Mel Elektronik (E-MEL) Di Agensi-agensi Kerajaan
(i) Surat Pekeliling No. 1/2007 - Pelaksanaan Dan Pemasangan Infrastruktur ICT Bagi Bangunan Kerajaan Sarawak
(j) Surat Pekeliling No. 2/2006 - Pelaksanaan Voice Over Internet Protocol (VOIP) dan Panggilan Telefon Berdiskaun (Discounted Call) untuk Kerajaan Sarawak
(k) Surat Pekeliling (Perj. Bil. 4/2000) - Mel Elektronik (EMel)
(l) Surat Pekeliling Bil. 40/2000 - Laman Web Agensi Dan Capaian Internet
(m) Surat Pekeliling Np. 47/2006 - Kata Laluan Tidak Dienkripsikan Di Dalam Pangkalan Data Komputer
(n) Surat Pekeliling No. 1/2006 - Polisi Keselamatan ICT Negeri Sarawak – Pengurusan Keselamatan Komputer Peribadi (Desktop Security Management – DSM)
(o) Perintah-Perintah Am Negeri 1996
(p) Akta Hak Cipta 1997;
(q) Perintah-Perintah Am;
(r) Arahan Perbendaharaan;
(s) Electronic Sarawak Government Activities (ESGA) 2022

LAMPIRAN C

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang boleh dirujuk oleh semua penjawat awam Negeri:

(a) Arahan Keselamatan;
(b) Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
(c) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
(d) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
(e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
(f) Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
(g) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
(h) Surat Arahan Ketua Setiausaha Negara – Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
(i) Surat Arahan Ketua Pengarah Kerajaan Sarawak – Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
(j) Surat Arahan Ketua Pengarah Kerajaan Sarawak – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
(k) Surat Pekeliling Am Bil. 2 Tahun 2000 – Peranan Jawatankuasa- jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
(l) Akta Tandatangan Digital 1997;
(m) Akta Rahsia Rasmi 1972;
(n) Akta Jenayah Komputer 1997;
(o) Akta Hak Cipta (Pindaan) Tahun 1997;
(p) Akta Komunikasi dan Multimedia 1998;
(q) Perintah-Perintah Am;
(r) Arahan Perbendaharaan;
(s) Arahan Teknologi Maklumat 2007;

LAMPIRAN 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 : _____
Cop Jabatan / Organisasi