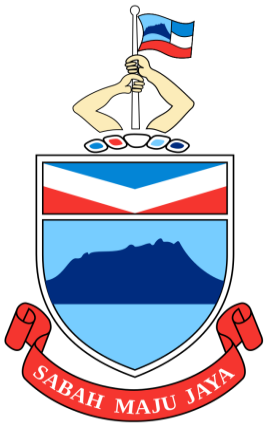
KERAJAAN NEGERI SABAH

DASAR KESELAMATAN SIBER

SEKTOR AWAM NEGERI SABAH



KERAJAAN NEGERI SABAH

DASAR KESELAMATAN SIBER

SEKTOR AWAM SABAH

VERSI 1.0

KANDUNGAN

SEJARAH DOKUMEN

VERSI	KELULUSAN	TARIKH KUAT KUASA	BUTIRAN PINDAAN
1.0	Mesyuarat Kabinet No. 9/2012 - No. Ruj. JKM(R)100-52/5 JLD.69(14) bertarikh 29 Mei 2012 Dasar Keselamatan ICT Sektor Awam Sabah.	29 Mei 2012	1) Mewujudkan Dasar Keselamatan ICT Sektor Awam Negeri Sabah.
1.0	Mesyuarat Jemaah Menteri Siri 3 Tahun 2026. Kertas Kabinet No.KK24/2026, Rujukan[JPKN(R)600-5/7, bertarikh 30 Januari 2026] Dasar Keselamatan Siber Sektor Awam Sabah	12 Februari 2026	1) Menukarkan tajuk Dasar Keselamatan ICT Sektor Awam Negeri Sabah kepada Dasar Keselamatan Siber Sektor Awam Sabah. 2) Menstrukturkan kandungan dasar selaras dengan versi piawai IEC/ISO 27001:2022 Information Security Management System. 3) Menambahkan kawalan untuk memenuhi keperluan Arahan Keselamatan (Semakan Dan Pindaan 2017).

PRAKATA
SETIAUSAHA KERAJAAN NEGERI SABAH

Assalamualaikum Warahmatullahi Wabarakatuh, Salam Malaysia Madani, Salam Sabah Maju Jaya dan salam sejahtera,

Dalam era digital yang semakin berkembang pesat, sektor awam Negeri Sabah menghadapi cabaran yang semakin kompleks dalam memastikan keselamatan siber kekal terjamin. Kemajuan teknologi maklumat bukan sahaja mempermudah urusan pentadbiran tetapi juga membuka ruang kepada ancaman yang boleh menjejaskan integriti, kerahsiaan, dan ketersediaan maklumat penting kerajaan.

Atas kesedaran inilah, **Dasar Keselamatan Siber Sektor Awam Sabah** diperkenalkan sebagai satu langkah strategik untuk melindungi aset digital kerajaan dan memastikan keselamatan maklumat diurus secara berkesan. Dasar ini berfungsi sebagai garis panduan yang menyeluruh kepada semua jabatan dan agensi negeri dalam memperkukuhkan sistem keselamatan siber mereka, sejajar dengan keperluan undang-undang dan piawaian antarabangsa.

Pelaksanaan dasar ini menuntut kerjasama padu daripada semua pihak di peringkat pentadbiran negeri. Setiap individu yang terlibat perlu memainkan peranan masing- masing dengan penuh tanggungjawab, demi memastikan dasar ini mencapai objektif yang disasarkan. Saya percaya, dengan dedikasi dan komitmen yang tinggi, kita mampu mencipta **ekosistem digital yang selamat dan lestari** untuk manfaat rakyat Negeri Sabah.

Saya mengucapkan setinggi-tinggi penghargaan kepada semua pihak yang telah menyumbang kepakaran dan usaha dalam merangka dasar ini. Semoga Dasar Keselamatan Siber Sektor Awam Sabah ini menjadi panduan berguna untuk memperkukuhkan tahap keselamatan siber kita sekaligus menyokong aspirasi Sabah sebagai negeri yang maju dalam dunia digital.

Sekian, terima kasih.

YB DATUK SERI PANGLIMA SR. HAJI SAFAR BIN UNTONG , JP
Setiausaha Kerajaan Negeri Sabah

KATA ALU-ALUAN
KETUA PEGAWAI DIGITAL (CDO) NEGERI

Assalamualaikum Warahmatullahi Wabarakatuh dan Salam Sejahtera.

Terlebih dahulu, syukur alhamdulillah, dengan izin-Nya, Dasar Keselamatan Siber Sektor Awam Sabah ini dapat diterbitkan dengan penambahbaikan selaras dengan perubahan teknologi semasa.

Sebagai sebuah negeri yang semakin maju dalam penggunaan teknologi maklumat, kita juga menghadapi risiko yang tinggi terhadap ancaman siber. Oleh itu, dasar ini disusun dengan teliti bagi memastikan langkah-langkah dan garis panduan keselamatan siber yang terkini, menyeluruh dan berkesan dapat dilaksanakan oleh semua pihak, khususnya agensi-agensi Kerajaan Negeri.

Dasar ini diharapkan menjadi rujukan utama dalam usaha mencapai tahap keselamatan siber yang lebih efektif. Marilah kita bersama-sama memainkan peranan masing-masing untuk mematuhi dasar ini serta melaksanakan langkah-langkah pencegahan yang perlu demi memastikan persekitaran digital yang lebih selamat dan terjamin.

Akhir kata, saya ingin mengucapkan setinggi-tinggi penghargaan dan terima kasih kepada semua pihak yang telah menyumbang tenaga dan kepakaran dalam menghasilkan Dasar Keselamatan Siber Sektor Awam Sabah ini. Semoga usaha ini membawa manfaat dan menjadikan negeri kita lebih selamat, cekap dan bersedia menghadapi cabaran keselamatan siber yang mendatang.

Sekian dan terima kasih.

DATUK DR. AHEMAD SADE
Timbalan Setiausaha Kerajaan Negeri (Pembangunan)
merangkap Ketua Pegawai Digital (CDO) Negeri

KATA ALU-ALUAN
PEGAWAI KESELAMATAN ICT(ICTSO) NEGERI

Assalamualaikum Warahmatullahi Wabarakatuh dan Salam Sejahtera.

Alhamdulillah, dengan limpah kurnia Allah Subhanahu Wa Ta'ala, Buku Dasar Keselamatan Siber Sektor Awam Sabah telah berjaya diterbitkan.

Dasar ini adalah berlandaskan prinsip-prinsip Sistem Pengurusan Keselamatan Maklumat yang merupakan piawai antarabangsa ISO/IEC 27001: 2022 (*Information Security Management System* [ISMS]). Penerbitan dasar ini mencerminkan komitmen tinggi Kerajaan Negeri Sabah dalam memperkukuhkan perlindungan keselamatan siber terutama sekali dalam era teknologi digital yang penuh dengan cabaran risiko keselamatan siber.

Saya mengajak semua warga sektor awam Negeri Sabah untuk memahami, menghayati dan mengamalkan langkah-langkah yang digariskan dalam dasar ini untuk meminimumkan risiko ancaman keselamatan siber di persekitaran kerja masing-masing.

Melalui penerapan kesedaran keselamatan siber yang tinggi dan bersedia memikul tanggungjawab bersama oleh seluruh warga sektor awam Negeri Sabah, saya yakin sistem penyampaian perkhidmatan kerajaan digital akan kekal selamat dan berdaya tahan.

Sebagai penutup, saya ingin mengucapkan setinggi-tinggi tahniah dan penghargaan kepada semua pihak yang telah menyumbangkan tenaga dan masa dalam penerbitan Dasar Keselamatan Siber Sektor Awam Sabah ini.

Sekian dan terima kasih.

ERNYWATI DEWI BINTI ABAS
Pengarah Jabatan Teknologi Digital dan Inovasi Negeri Sabah
merangkap Pegawai Keselamatan ICT(ICTSO) Negeri

1. PENGENALAN

Dasar Keselamatan Siber Sektor Awam Sabah mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) dan ruang siber. Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT dan ruang siber Kerajaan Negeri.

2. OBJEKTIF

Dasar Keselamatan Siber Sektor Awam Sabah diwujudkan untuk:

(a) Menjamin kesinambungan perkhidmatan Sektor Awam Negeri dengan meminimumkan kesan insiden keselamatan siber;

(b) Memudahkan perkongsian maklumat sesuai dengan keperluan operasi Sektor Awam Negeri dengan memastikan semua aset ICT dan ruang siber dilindungi;

(c) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

(d) Mencegah salah guna atau kecurian aset ICT dan ruang siber Kerajaan Negeri;

(e) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;

(f) Meningkatkan tahap kesedaran keselamatan siber kepada kakitangan, pengguna dan pembekal; dan

(g) Memperkukuhkan pengurusan risiko.

3. PERNYATAAN DASAR

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

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

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan khususnya Sektor Awam Negeri dari capaian tanpa kuasa yang sah;

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

(c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

(d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar Keselamatan Siber Sektor Awam Sabah 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 dari itu, langkah-langkah ke arah menjamin keselamatan siber hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT dan ruang siber, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

4. SKOP

Aset ICT dan ruang siber Sektor Awam Negeri terdiri daripada peralatan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan Siber Sektor Awam Sabah 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 dan ruang siber ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan Siber Sektor Awam Sabah ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

(a) **Peralatan**

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan Jabatan/Agensi Sektor Awam Negeri. Contohnya komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) **Perisian**

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada Jabatan/Agensi;

(c) **Media Storan**

Semua media storan yang berkaitan seperti storan mudah alih, *cartridge*, CD-ROM, pita, cakera, pemacu cakera, pemacu pita, storan awan (*cloud storage*) dan lain-lain;

(d) **Perkhidmatan**

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

(e) **Data atau Maklumat**

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

(f) **Manusia**

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

(g) **Premis Komputer dan Komunikasi**

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara a) - f) di atas.

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang ketirisan rahsia atau kelemahan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah keselamatan.

5. PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan Siber Sektor Awam Sabah dan perlu dipatuhi adalah seperti berikut:

(a) Capaian atas dasar perlu mengetahui

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

Penggunaan *encryption*, tandatangan digital atau sebarang mekanisme lain yang boleh melindungi maklumat mestilah juga dipertimbangkan. Dasar klasifikasi ke atas sistem aplikasi juga hendaklah mengikut klasifikasi maklumat yang sama;

(b) Hak capaian minimum

Hak capaian pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, 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 dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT dan ruang siber. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap kepekaan sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka;

Akauntabiliti atau tanggungjawab pengguna termasuklah:

(i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

(ii) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;

(iii) Menentukan maklumat sedia untuk digunakan;

(iv) Menjaga kerahsiaan kata laluan;

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

(vi) Memberi perhatian kepada maklumat rahsia rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

(vii) Menjaga kerahsiaan langkah-langkah keselamatan siber dari diketahui umum.

(d) Pengasingan Fungsi

Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT dan ruang siber daripada kesilapan, ketirisan maklumat rahsia rasmi atau di manipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

(e) Pengauditan Keselamatan

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

(f) Pematuhan

Dasar Keselamatan Siber Sektor Awam Sabah hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan siber;

(g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh

dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan;

(h) Integriti

Data dan maklumat hendaklah tepat, lengkap dan sentiasa terkini. Sebarang perubahan terhadap data hendaklah dilaksanakan oleh kakitangan yang diberi kebenaran sahaja;

(i) Perimeter Keselamatan Fizikal

Perimeter merujuk kepada keadaan persekitaran fizikal di mana aset-aset ICT dan ruang siber dilindungi. Perimeter tersebut hendaklah dijaga dengan rapi bagi mengelakkan sebarang pencerobohan; dan

(j) Saling Bergantungan

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

6. PENILAIAN RISIKO KESELAMATAN SIBER

Jabatan/Agensi Sektor Awam Negeri hendaklah mengambil kira kewujudan risiko ke atas aset ICT dan ruang siber akibat dari ancaman dan kerentanan (*vulnerability*) yang semakin meningkat. Justeru itu Kerajaan Negeri perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT dan ruang siber supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT dan ruang siber.

Jabatan/Agensi Sektor Awam Negeri hendaklah melaksanakan penilaian risiko keselamatan siber secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan siber. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan siber berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan siber hendaklah dilaksanakan ke atas sistem maklumat Kerajaan Negeri termasuk aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuk pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

Jabatan/Agensi Sektor Awam Negeri bertanggungjawab melaksanakan dan menguruskan risiko keselamatan siber selaras dengan keperluan Arahan Keselamatan, Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

Jabatan/Agensi Sektor Awam Negeri perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

(a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

(b) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;

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

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

BIDANG A KAWALAN ORGANISASI	
A.1 DASAR KESELAMATAN MAKLUMAT	
Objektif: Memastikan kesesuaian, kecukupan, keberkesanan hala tuju dan sokongan pengurusan yang berterusan untuk keselamatan maklumat selaras dengan keperluan perkhidmatan Jabatan / Agensi Sektor Awam Negeri, undang-undang, kawal selia, peraturan dan kontrak.	
KENYATAAN	**TANGGUNGJAWAB**
A.1.1 PELAKSANAAN DASAR	
Pelaksanaan dasar ini akan dijalankan oleh Setiausaha Kerajaan Negeri yang dibantu oleh: (i) Jawatankuasa Pemandu Keselamatan Siber Sabah, yang dipengerusikan oleh Setiausaha Kerajaan Negeri; (ii) Jawatankuasa Teknikal Keselamatan Siber Sabah, yang dipengerusikan oleh Ketua Pegawai Digital Negeri (CDO Negeri) / Setiausaha Tetap Kementerian Pendidikan, Sains, Teknologi dan Inovasi Sabah; (iii) Jawatankuasa Kerja Keselamatan Siber Sabah (Sabah Government Cyber Security Incident Response Team (sgCSIRT)) yang dipengerusikan oleh Pegawai Keselamatan ICT Negeri (ICTSO Negeri); (iv) Jabatan Teknologi Digital dan Inovasi Negeri Sabah (JTDINS); (v) Semua Ketua Pegawai Digital (CDO) Jabatan/Agensi; (vi) Semua Ketua Pegawai Keselamatan (ICTSO) Jabatan/Agensi; (vii) Semua Ketua Jabatan; dan (viii) Semua Pengurus ICT Jabatan/Agensi.	Setiausaha Kerajaan Negeri

A.1.2 PENYEBARAN DASAR	
Dasar ini perlu disebarkan kepada semua pengguna Jabatan / Agensi Sektor Awam Negeri (termasuk kakitangan, pembekal, pakar runding dan lain-lain) menggunakan platform yang boleh dicapai oleh pihak berkaitan seperti Laman Web Intra, Laman Web Jabatan / Agensi Sektor Awam Negeri, serahan *hardcopy*, e-mel dan lain-lain medium komunikasi.	ICTSO
A.1.3 PENYELENGGARAAN DASAR	
Dasar ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan Siber Sektor Awam Sabah: (a) Kenal pasti dan tentukan perubahan yang diperlukan; (b) Kemuka cadangan pindaan secara bertulis kepada JTDINS untuk pembentangan dan persetujuan Jawatankuasa Pemandu Keselamatan Siber Sabah; (c) Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh Jawatankuasa Pemandu Keselamatan Siber Sabah; (d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali dalam tempoh lima tahun atau mengikut keperluan semasa; dan (e) Perubahan yang tidak menjejaskan kawalan di dalam Dasar Keselamatan Siber Sektor Awam Sabah hanya perlu dikemukakan kepada ICTSO dan dimaklumkan kepada pengguna.	ICTSO dan Pengurus ICT

BIDANG A KAWALAN ORGANISASI	
A.2 PERANAN DAN TANGGUNGJAWAB DALAM KESELAMATAN MAKLUMAT	
Objektif: Mewujudkan struktur yang ditakrifkan, diluluskan dan difahami untuk pelaksanaan, pengendalian dan pengurusan keselamatan maklumat Jabatan / Agensi Sektor Awam Negeri.	
KENYATAAN	**TANGGUNGJAWAB**
A.2.1 SETIAUSAHA KERAJAAN NEGERI	
Setiausaha Kerajaan Negeri berperanan dan bertanggungjawab bagi perkara seperti berikut: (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan Siber Jabatan / Agensi Sektor Awam Sabah; (b) Memastikan semua pengguna mematuhi Dasar Keselamatan Siber Sektor Awam Sabah; (c) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan (d) Memastikan penilaian risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan Siber Sektor Awam Sabah.	Setiausaha Kerajaan Negeri
A.2.2 KETUA PEGAWAI DIGITAL NEGERI (CDO Negeri)	
Ketua Pegawai Digital (CDO Negeri) Negeri iaitu Timbalan Setiausaha Kerajaan Negeri (Pembangunan) berperanan dan bertanggungjawab bagi perkara seperti berikut: (a) Membantu Setiausaha Kerajaan Negeri dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber;	CDO

(b) Memberi kepimpinan dan halatuju kepada CDO Jabatan / Agensi dalam mengurus hal-hal berkaitan keselamatan siber Jabatan/Agensi; (c) Menasihati Setiausaha Kerajaan Negeri tentang penyediaan segala kemudahan berkaitan pembangunan dan pengembangan keselamatan siber Sektor Awam Negeri yang diperlukan; dan (d) Bertanggungjawab ke atas fungsi-fungsi Jawatankuasa Keselamatan siber Kerajaan Negeri secara keseluruhan;	
A.2.3 PEGAWAI KESELAMATAN ICT NEGERI (ICTSO NEGERI)	
Pegawai Keselamatan ICT Negeri (ICTSO Negeri) iaitu Pengarah Jabatan Teknologi Digital dan Inovasi Negeri Sabah berperanan dan bertanggungjawab bagi perkara seperti berikut: (a) Membantu Setiausaha Kerajaan Negeri dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber; (b) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan siber Sektor Awam Negeri secara keseluruhan; (c) Menasihati ICTSO Negeri perihal pembangunan, perkembangan, pelaksanaan dan pematuhan keselamatan siber Sektor Awam Negeri; (d) Bertanggungjawab ke atas fungsi-fungsi sgCSIRT secara keseluruhan; (e) Bertindak sebagai penasihat dalam penyediaan rancangan keselamatan siber Sektor Awam Negeri; dan (f) Memastikan perhubungan yang rapat di antara Negeri / Persekutuan dalam usahasama melindungi aset-aset ICT Kerajaan.	ICTSO Negeri

A.2.4 KETUA PEGAWAI DIGITAL (CDO)	
Peranan dan tanggungjawab Ketua Pegawai Digital (CDO) di semua Jabatan dan Agensi Negeri adalah seperti berikut: (a) Menentukan keperluan keselamatan siber Jabatan/Agensi; (b) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan siber; (c) Memastikan setiap pegawai dan kakitangan menandatangani Surat Akuan Pematuhan Dasar Keselamatan Siber Sektor Awam Sabah; (d) Mengambil tindakan tatatertib ke atas anggota yang melanggar Dasar Keselamatan Siber Sektor Awam Sabah; dan (e) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan Siber Jabatan/Agensi.	CDO
A.2.5 PEGAWAI KESELAMATAN ICT (ICTSO)	
Peranan dan tanggungjawab Pegawai Keselamatan ICT (ICTSO) di semua Jabatan dan Agensi Negeri adalah seperti berikut: (a) Mengurus program-program keselamatan siber Jabatan/Agensi; (b) Menguatkuasakan pelaksanaan Dasar Keselamatan Siber Sektor Awam Sabah; (c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan Siber Sektor Awam Sabah kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan Siber Sektor Awam Sabah;	ICTSO

(e) Menjalankan pengurusan risiko; (f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan Jabatan / Agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; (g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (h) Melaporkan insiden keselamatan siber kepada sgCSIRT, dan memaklumkannya kepada CDO; (i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; (j) Mengesyorkan proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan Siber Sektor Awam Sabah; (k) Memberikan hak capaian yang berkaitan keselamatan siber kepada pengguna; dan (l) Bertindak sebagai koordinator dan melaporkan insiden keselamatan siber kepada CDO bagi insiden siber berdasarkan Pelan Pemulihan Bencana (DRP).	
A.2.6 PENGURUS ICT	
Peranan dan tanggungjawab Pengurus ICT di semua Kementerian, Jabatan dan Agensi Negeri adalah seperti berikut: (a) Mengkaji semula dan melaksanakan kawalan keselamatan siber selaras dengan keperluan Jabatan / Agensi Sektor Awam Negeri;	Pengurus ICT

(b) Menentukan kawalan capaian pengguna terhadap aset ICT Jabatan / Agensi Sektor Awam Negeri; (c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan siber kepada CDO; (d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan siber Jabatan / Agensi Sektor Awam Negeri; (e) Membangun, mengkaji semula dan mengemas kini Pelan Pemulihan Bencana (DRP) keselamatan siber Jabatan / Agensi Sektor Awam Negeri; (f) Memastikan Dasar Keselamatan Siber Sektor Awam Sabah dikemas kini sesuai dengan perubahan teknologi, perubahan dasar kerajaan dan ancaman-ancaman dari semasa ke semasa; dan (g) Memastikan Dasar Strategik ICT Jabatan / Agensi Sektor Awam Negeri mengandungi aspek keselamatan siber.	
A.2.7 MAJLIS PEMBANGUNAN TEKNOLOGI DAN INOVASI SABAH (MaPTIS)	
Peranan dan tanggungjawab MaPTIS adalah seperti berikut:- (a) Merangsang dan mempermudahkan pembangunan penyelidikan dalam bidang Sains, Teknologi dan Inovasi di Sabah; (b) Mengkoordinasi, memantau dan membantu pengembangan penyelidikan yang dilakukan oleh jabatan Kerajaan, Badan Berkanun, Syarikat berkaitan Kerajaan dan Badan bukan Kerajaan (NGOs) selain daripada menjadi medium jalinan kerjasama dan komunikasi di antara mereka; (c) Mempromosikan dan mengekalkan persekitaran yang kondusif seperti berikut:- (i) Mengembangkan dan memelihara bakat dan modal intelektual dengan pengetahuan saintifik	MaPTIS

dan teknologi, kemahiran dan kemampuan inovatif yang diperlukan untuk menyokong kemajuan negeri dan secara tidak langsung dapat mempromosikan pertumbuhan dan kemajuan ekonomi negeri; (ii) Mempermudahkan aplikasi komersial hasil pembangunan penyelidikan dan inovasi yang dilakukan di Negeri; dan (iii) Meningkat standard dan keupayaan penyelidikan untuk menarik bakat saintifik dan teknologi di institusi pendidikan di Sabah. (d) Mempromosikan pendidikan dalam penyelidikan saintifik dan teknologi. Keanggotaan MaPTIS adalah seperti berikut:- Penaung : YAB Ketua Menteri SABAH Pengerusi : Menteri Pendidikan, Sains, Teknologi dan Inovasi Sabah. Ahli : (1) Setiausaha Tetap Kementerian Pendidikan, Sains, Teknologi dan Inovasi. (2) Ketua Pengerusi Jawatankuasa Teknikal MaPTIS. (3) Timbalan Setiausaha Tetap I Kementerian Pendidikan, Sains, Teknologi dan Inovasi. (4) Timbalan Setiausaha Tetap II Kementerian Pendidikan, Sains, Teknologi dan Inovasi. (5) Pengerusi Jawatankuasa Teknikal Penyelidikan dan Inovasi. (6) Pengerusi Jawatankuasa Teknikal Aplikasi Teknologi. (7) Pengerusi Jawatankuasa Teknikal Pembangunan Modal Insan.	

Terma Rujukan: Majlis Pembangunan Teknologi dan Inovasi Sabah adalah untuk memberi panduan kepada semua pihak yang terlibat dalam melaksanakan tugas masing-masing dalam MaPTIS.	
A.2.8 JAWATANKUASA PEMANDU KESELAMATAN SIBER SABAH	
Objektif penubuhan Jawatankuasa Pemandu Keselamatan Siber Sabah adalah seperti berikut:- (a) Menetapkan hala tuju strategik dan tadbir urus keselamatan siber di peringkat Negeri Sabah untuk memastikan perlindungan aset maklumat kritikal Kerajaan Negeri; (b) Menyelaras pelaksanaan dasar/pekeliling, piawai dan inisiatif keselamatan siber di semua Agensi Kerajaan Negeri Sabah (AKNS); dan (c) Memantau pematuhan kepada perundangan, dasar dan pekeliling berkaitan ICT. Jawatankuasa berfungsi sebagai badan pembuat keputusan dan pengawasan tertinggi dengan tugas-tugas berikut:- (a) **Strategi dan Dasar:** Meluluskan dan menyemak dasar/pekeliling berkaitan keselamatan siber Sabah serta rangka kerja dan implikasi kewangan berkaitan; (b) **Pengurusan Risiko:** Menilai, memantau, dan meluluskan pelan mitigasi untuk risiko siber utama yang boleh memberi impak kepada perkhidmatan awam Negeri; (c) **Pematuhan dan Audit:** Memastikan semua agensi Negeri mematuhi arahan dan piawai keselamatan siber yang ditetapkan; (d) **Kesiapsiagaan Insiden:** Menyelia kesiapsiagaan Negeri dalam menghadapi insiden siber berskala	

besar, termasuk meluluskan pelan tindak balas insiden; dan (e) **Penyelarasan:** Bertindak sebagai platform penyelarasan utama antara agensi-agensi Negeri dan badan keselamatan siber Persekutuan (NACSA dan Cybersecurity Malaysia). Keanggotaan Jawatankuasa Pemandu Keselamatan Siber Sabah adalah seperti berikut:- Pengerusi : Setiausaha Kerajaan Negeri Ahli: (1) Timbalan Setiausaha Kerajaan Negeri (Pembangunan). (2) Semua Setiausaha Tetap Kementerian. (3) Jabatan Peguam Besar Negeri Sabah. Urus Setia: (4) Jabatan Teknologi Digital dan Inovasi Negeri Sabah (JTDINS). Ahli Jemputan: (5) Jabatan Audit Dalam Negeri (6) Unit Perancang Ekonomi Negeri (7) Sabah.Net Sdn. Bhd (8) Panel Pakar Bidang ICT dan Bidang Khusus (dalaman dan / luaran)	
A.2.9 JAWATANKUASA TEKNIKAL KESELAMATAN SIBER SABAH	
Objektif penubuhan Jawatankuasa Teknikal Keselamatan Siber Sabah adalah seperti berikut:- (a) Menyediakan kepakaran teknikal dan mengawasi pelaksanaan operasi keselamatan siber di peringkat agensi Kerajaan Negeri Sabah; dan	

(b) Memastikan keseragaman dalam penggunaan piawaian, seni bina (*architecture*), dan prosedur teknikal keselamatan siber di seluruh Negeri. Jawatankuasa berfungsi sebagai badan penasihat teknikal dan pelaksana bagi tugas-tugas berikut:- (a) **Piawaian Teknikal**: Mencadangkan, menilai, dan mengesyorkan piawaian teknikal dan konfigurasi keselamatan siber (Contoh: penetapan hardening pelayan, spesifikasi perisian keselamatan) untuk penggunaan seragam agensi Negeri; (b) **Pengurusan Risiko**: Mencadangkan, menilai risiko dan mengesyorkan rawatan risiko kepada agensi Kerajaan Negeri Sabah; (c) **Seni Bina Keselamatan**: Menyemak dan menasihati mengenai reka bentuk (*design*) dan pelaksanaan seni bina keselamatan siber yang cekap dan berkesan untuk infrastruktur kritikal Negeri; (d) **Pengurusan Operasi**: Menyelaras operasi harian keselamatan siber, termasuk pengurusan kelemahan (*vulnerability management*), pengurusan patching, dan pemantauan ancaman secara kolektif; (e) **Tindak Balas Insiden**: Berfungsi sebagai unit teknikal barisan hadapan untuk menyelaraskan tindak balas segera dan analisis teknikal bagi insiden siber yang melibatkan pelbagai agensi Negeri; dan (f) **Penilaian Teknologi**: Menilai dan mengesyorkan perolehan teknologi keselamatan siber baharu yang sesuai dengan keperluan teknikal dan risiko Negeri. Keanggotaan Jawatankuasa Teknikal Keselamatan Siber Sabah adalah seperti berikut:- Pengerusi : Setiausaha Kerajaan Negeri Ahli :	

(1) Setiausaha Tetap Kementerian Pendidikan, Sains, Teknologi dan Inovasi (KPSTI). (2) Semua Ketua Jabatan / Agensi / Badan Berkanun. (3) Wakil Jabatan Peguam Besar Negeri Sabah Pegawai Undang-Undang, Jabatan Peguam Negeri Sabah. Urus setia: (4) Jabatan Teknologi Digital dan Inovasi Negeri Sabah (JTDINS). Ahli Jemputan: (5) Jabatan Audit Dalam Negeri (6) Unit Perancang Ekonomi Negeri (7) Sabah.Net Sdn. Bhd (8) Panel Pakar Bidang ICT dan Bidang Khusus (dalaman dan /luaran)	
A.2.10 JAWATANKUASA KERJA KESELAMATAN SIBER SABAH (SABAH GOVERNMENT CYBER SECURITY INCIDENT RESPONSE TEAM [sgCSIRT])	
Objektif penubuhan Jawatankuasa Kerja Keselamatan Siber Sabah adalah seperti berikut:- **(a) Meningkatkan Keupayaan Tindak Balas Insiden ICT** Menyediakan mekanisme pantas dan berkesan dalam menangani insiden keselamatan siber di peringkat Kerajaan Negeri Sabah; **(b) Melaksanakan Analisis Teknikal dan Forensik** Menjalankan siasatan teknikal terhadap insiden keselamatan, termasuk pengumpulan bukti digital dan analisis forensik untuk tujuan pemulihan serta tindakan undang-undang; **(c) Memastikan Kesinambungan Operasi ICT** Menyokong pemulihan sistem kritikal dengan segera bagi memastikan perkhidmatan kerajaan tidak	SgCSIRT

terganggu akibat serangan atau kelemahan keselamatan; **(d) Menyelaras Tindakan Pencegahan dan Penambahbaikan** Melaksanakan langkah pembaikan seperti patch management, pengukuhan konfigurasi sistem, dan penutupan kelemahan yang dikenal pasti; **(e) Membangunkan Kepakaran Teknikal Dalaman** Melatih dan meningkatkan kemahiran teknikal anggota pasukan dalam bidang keselamatan siber, forensik digital dan pengurusan insiden; **(f) Menyediakan Laporan dan Cadangan Strategik** Menyediakan laporan teknikal insiden serta mencadangkan tindakan susulan untuk meningkatkan tahap keselamatan ICT kerajaan negeri; dan **(g) Bekerjasama dengan Agensi Berkaitan** Menjalin kerjasama dengan agensi keselamatan, pihak berkuasa undang-undang, dan pembekal (vendor) teknologi bagi memastikan tindak balas insiden yang menyeluruh. Keanggotaan sgCSIRT adalah seperti berikut:- Pengerusi : Pengarah Jabatan Teknologi Digital dan Inovasi Negeri Sabah selaku Pegawai Keselamatan ICT Negeri (ICTSO Negeri). Ahli : (1) Pasukan Tindak Balas Insiden dan Forensik Kerajaan Negeri (State Government Incident Response and Forensic Team - SgIRF). (2) Pasukan Audit dan Penilaian Keselamatan ICT Kerajaan Negeri (State Government ICT Security Audit and Assessment Team - SgSAT).	

(3) Pasukan Penyelidikan & Pembangunan Keselamatan ICT Kerajaan Negeri (State Government ICT Security R&D Team - SgRnD). (4) Pasukan Latihan, Pendidikan dan Penghayatan Keselamatan ICT Kerajaan Negeri (State Government ICT Security Training, Education and Acculturation Team - SgHRD). (5) Pasukan Pemantauan Keselamatan ICT Kerajaan Negeri (State Government ICT Security Monitoring Team - SgSMT). Fungsi Utama sgCSIRT adalah seperti berikut:- (a) Menyediakan perkhidmatan pengurusan insiden, kerentanan (*vulnerability*) dan bukti pencerobohan Sektor Awam Negeri; (b) Menyebar '*security alerts and warnings*' dari semasa ke semasa; (c) Menjalankan audit keselamatan aset-aset ICT Negeri untuk mempastikan pematuhan langkah-langkah dan garis panduan keselamatan ICT; (d) Mempertingkatkan tahap kesedaran ancaman keselamatan ICT di kalangan penjawat sektor awam Negeri; dan (e) Mempertingkatkan usaha sama dengan NACSA dalam hal-hal berkaitan keselamatan ICT. Peranan dan tanggungjawab Pasukan Tindak Balas Insiden dan Forensik Kerajaan Negeri (SgIRF) adalah seperti berikut:- (a) Menggubal dan mengkaji semula prosedur-prosedur tindak balas insiden keselamatan siber; (b) Merekod dan menjalankan siasatan awal insiden yang diterima;	

(c) Menangani tindak balas (*response*) insiden keselamatan siber dan mengambil tindakan baik pulih minimum; dan (d) Mengumpul dan menganalisa bukti-bukti forensik dan menyediakan laporan serta mencadangkan tindakan yang perlu diambil seperti:- (i) membuat laporan polis; dan/atau. (ii) melakukan *'patch'* ke atas sistem. Peranan dan tanggungjawab Pasukan Audit dan Penilaian Keselamatan ICT Kerajaan Negeri (sgSAT) adalah seperti berikut:- (a) Menyediakan rangka (*frame work*) pengauditan keselamatan siber, mewujudkan dan menyemak prosedur pengauditan serta penilaian keselamatan siber; (b) Mengambil tindakan *'pre-emptive'* untuk mengelakkan ancaman melalui *'penetration test'* yang dilakukan scara berkala; (c) Menyediakan pelan pengukuhan keselamatan siber; (d) Mendaftar semua kemudahan dan perkhidmatan siber; dan (e) Menjalankan penilaian dan menyediakan pelan pengukuhan keselamatan ICT bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan. Peranan dan tanggungjawab Pasukan Latihan, Pendidikan dan Penghayatan Keselamatan ICT Kerajaan Negeri (SgHRD) adalah seperti berikut:- (a) Menggubal dan mengkaji semula kurikulum latihan keselamatan siber; (b) Merancang, melaksanakan dan mengkaji semula aktiviti-aktiviti kesedaran keselamatan siber; dan	

(c) Menjalankan latihan keselamatan siber secara berkala. Peranan dan tanggungjawab Pasukan Pemantauan Keselamatan (sgSMT) adalah seperti berikut:- (a) Mewujudkan dan menyemak terhadap prosedur pemantauan keselamatan siber; (b) Memantau dan memastikan pematuhan polisi keselamatan siber dan yang berkaitan; (c) Menyediakan perkhidmatan konsultasi keselamatan siber; (d) Merekod dan melaporkan aktiviti yang mencurigakan; dan (e) Memantau log-log sistem dan berkaitan. Peranan dan tanggungjawab Pasukan Penyelidikan & Pembangunan Keselamatan ICT Kerajaan Negeri (SgRnD) adalah seperti berikut:- (a) Menilai dan membuat cadangan terhadap teknologi keselamatan siber; (b) Menjalankan penyelidikan ke atas sistem/rangkaian/aplikasi keselamatan dan cadangan penambahbaikan; dan (c) Melapor ancaman siber baharu (*advisory*) dan cadangan langkah pengukuhan.	
A.2.11 JAWATANKUASA TEKNIKAL INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)	
Keanggotaan Jawatankuasa Teknikal ISMS adalah seperti berikut: Pengerusi: Pengarah Jabatan Teknologi Digital dan Inovasi Negeri Sabah	ICTSO, JK Teknikal ISMS, Pasukan Pelaksana ISMS, Pasukan Audit Dalam ISMS, Urus Setia ISMS, Pengurus Dokumen ISMS

Ahli: (a) Pemilik Sistem: Pengarah/Wakil Bahagian (b) Timbalan-Timbalan Pengarah (c) Ketua Penolong Pengarah/Pegawai Teknologi Maklumat (d) Penolong Pegawai Teknologi Maklumat Urus setia : Bahagian Keselamatan Siber, Jabatan Teknologi Digital dan Inovasi Negeri Sabah. Kuasa dan Bidang Tugas adalah untuk memantau: (a) Keperluan kursus kesedaran untuk melaksanakan standard ISO/IEC 27001; (b) Pelaksanaan pensijilan ISMS ke atas perkhidmatan di dalam skop ISMS; (c) Kriteria penerimaan risiko, tahap risiko, penemuan awal penilaian risiko dan *risk treatment plan*; (d) Struktur organisasi ISMS; (e) Mesyuarat Kajian Semula Pengurusan ISMS sekurang-kurangnya satu kali setahun; (f) Menyediakan sumber-sumber untuk melaksanakan ISMS; (g) Pengurusan dokumen dan rekod pelaksanaan ISMS; dan (h) Laporan audit dan laporan audit susulan dan tindakan pembetulan ke atas ketakakuran yang ditemui oleh pasukan audit.	
A.2.12 PENTADBIR SISTEM ICT	
Pentadbir Sistem ICT iaitu Ketua Pegawai Teknologi Maklumat/Pegawai Teknologi Maklumat atau gred F tertinggi di semua Kementerian, Jabatan dan Agensi Negeri	

adalah berperanan dan bertanggungjawab bagi perkara berikut:- **Pentadbir Sistem ICT** (a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan Siber Sektor Awam Sabah; (c) Memantau aktiviti capaian harian sistem aplikasi pengguna; (d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (e) Menganalisis dan menyimpan rekod jejak audit; (f) Menyediakan laporan mengenai aktiviti capaian secara berkala; (g) Memastikan setiap pengguna dikenali dengan menggunakan *User ID* yang unik; dan (h) Bertanggungjawab memantau setiap peralatan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik. Peranan dan tanggungjawab Pentadbir Sistem ICT mengikut fungsi bidang tugas adalah seperti berikut: **Pentadbir Rangkaian dan Keselamatan**	

(a) Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di Kerajaan Negeri beroperasi sepanjang masa; (b) Memastikan semua peralatan dan perisian rangkaian diselenggara dengan sempurna; (c) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; (d) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; (e) Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; (f) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan sambungan rangkaian selainnya perlu mendapat kelulusan ICTSO; (g) Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian; dan (h) Melibatkan diri dalam sebarang aktiviti penilaian tahap keselamatan, pengauditan dan penilaian risiko keselamatan maklumat. **Pentadbir Pangkalan Data** (a) Melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data; (b) Memastikan pangkalan data boleh digunakan pada setiap masa; (c) Melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data; (d) Melaksanakan *data masking* dalam menyediakan data latihan; (e) Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah	

pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur; (f) Melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip Dasar Keselamatan Siber Sektor Awam Sabah; (g) Melaksanakan proses pembersihan data (*housekeeping*) di dalam pangkalan data; (h) Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO; dan (i) Melibatkan diri dalam sebarang aktiviti penilaian tahap keselamatan, pengauditan dan penilaian risiko keselamatan maklumat. **Pentadbir Laman Web** (a) Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah; (b) Memantau prestasi capaian dan menjalankan penilaian prestasi untuk memastikan akses yang lancar; (c) Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman; (d) Mengehadkan capaian Pentadbir Laman Web bahagian ke *web server*; (e) Mengasingkan kandungan dan aplikasi atas talian untuk capaian secara Intranet dan Internet ke portal Kerajaan Negeri; (f) Memastikan maklumat rahsia rasmi (RAHSIA BESAR, RAHSIA, SULIT, TERHAD) tidak dibenarkan dicapai melalui laman web tanpa ada ciri-ciri keselamatan yang khusus pada laman web	

berkenaan. Laman web hanya untuk paparan maklumat rasmi sahaja; (g) Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; (h) Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di web server; (i) Melaksanakan proses *backup* dan *restoration* secara berkala; dan (j) Melaporkan sebarang pelanggaran keselamatan laman portal kepada ICTSO. **Pentadbir Pusat Data** (a) Memastikan persekitaran fizikal dan keselamatan Pusat Data berada dalam keadaan baik dan selamat; (b) Memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data; (c) Menjadual dan melaksanakan proses sokongan dan pemulihan ke atas pangkalan data dan sistem secara berkala; (d) Melaksanakan Dasar Pemulihan Bencana (DRP) mengikut Prinsip Kesinambungan Perkhidmatan dalam Dasar Keselamatan Siber Sektor Awam Sabah; (e) Melaksanakan prinsip-prinsip Dasar Keselamatan Siber Sektor Awam Sabah; (f) Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan; dan (g) Melibatkan diri dalam sebarang aktiviti penilaian tahap keselamatan, pengauditan dan penilaian risiko keselamatan maklumat.	

Pentadbir Sistem Aplikasi (a) Mengkaji cadangan pembangunan atau penyelarasan sistem atau modul di Kerajaan Negeri; (b) Membuat kajian semula serta memperbaiki sistem atau modul sedia ada di Kerajaan Negeri; (c) Membuat pertimbangan dan mengusulkan cadangan pelaksanaan sistem atau modul di Kerajaan Negeri; (d) Membuat pemantauan dan penyelenggaraan terhadap sistem atau modul dari semasa ke semasa; (e) Bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem atau modul; (f) Menyediakan dokumentasi sistem atau modul dan manual pengguna; (g) Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; (h) Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya; (i) Memastikan *virus pattern, hotfix* dan *patch* yang berkaitan dengan sistem aplikasi terkemaskini supaya terhindar daripada ancaman virus dan penggodam; (j) Mematuhi dan melaksanakan prinsip-prinsip Dasar Keselamatan Siber Sektor Awam Sabah dalam mewujudkan akaun pengguna ke atas setiap sistem aplikasi; (k) Mengehadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan dari penyalahgunaannya; (l) Melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya; dan	

(m) Melibatkan diri dalam sebarang aktiviti penilaian tahap keselamatan, pengauditan dan penilaian risiko keselamatan maklumat. **Pentadbir E-mel** (a) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; (b) Mengesah dan memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan melalui saluran rasmi; (c) Memastikan kemudahan membuat capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi; dan (d) Memastikan pengguna e-mel Jabatan / Agensi Sektor Awam Negeri berkemahiran menggunakan emel melalui penyediaan dokumen tatacara penggunaan emel dan Internet Jabatan / Agensi Sektor Awam Negeri serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan. **Pentadbir Media Sosial** (a) Mematuhi segala peraturan atau syarat-syarat yang digariskan oleh penyedia platform media sosial; (b) Mentadbir dan menyemak ketepatan serta sensitiviti maklumat dalam pengurusan kandungan (video, audio, gambar dan dokumen) dan komen mengikut etika media sosial semasa; dan (c) Melaporkan sebarang pelanggaran polisi atau etika penggunaan media sosial yang sedang berkuat kuasa kepada ICTSO.	

A.2.13 PENGGUNA	
Pengguna mempunyai peranan dan tanggungjawab seperti berikut:- (a) Membaca, memahami dan mematuhi Dasar Keselamatan Siber Sektor Awam Sabah; (b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya; (c) Melepasi tapisan keselamatan (jika berkaitan); (d) Melaksanakan prinsip-prinsip Dasar Keselamatan Siber Sektor Awam Sabah dan menjaga kerahsiaan maklumat Jabatan / Agensi Sektor Awam Negeri; (e) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; (f) Menghadiri program-program kesedaran mengenai keselamatan siber; dan (g) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan Siber Sektor Awam Sabah sebagaimana di **Lampiran 2.**	Pengguna
A.2.14 KEPERLUAN KESELAMATAN DENGAN PIHAK LUARAN/KETIGA	
Bertujuan untuk memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak luaran dikawal. Perkara yang perlu dipatuhi termasuk yang berikut:- (a) Membaca, memahami dan mematuhi Dasar Keselamatan Siber Sektor Awam Sabah yang berkaitan; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;	CDO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Luaran/Ketiga

(c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak luaran/ketiga; (d) Capaian kepada aset ICT Jabatan / Agensi Sektor Awam Negeri perlu berlandaskan kepada perjanjian; (e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak luaran/ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai: (i) Dasar Keselamatan Siber Sektor Awam Sabah; (ii) Tapisan Keselamatan (jika berkaitan); (iii) Perakuan Akta Rahsia Rasmi 1972; dan (iv) Hak Harta Intelek. (f) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan Siber Sektor Awam Sabah sebagaimana di Lampiran 2.	

BIDANG A KAWALAN ORGANISASI	
A.3 PENGASINGAN TUGAS	
Objektif: Mengurangkan risiko pengubahsuaian, kesilapan dan pemintasan dalam kawalan keselamatan maklumat.	
KENYATAAN	**TANGGUNGJAWAB**
A.3.1 KEPERLUAN KESELAMATAN DALAM PENGASINGAN TUGAS	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT. (a) Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, ketirisan maklumat rahsia rasmi atau dimanipulasi; (b) Peralatan yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari peralatan yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan (c) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.	ICTSO dan Pengurus ICT

BIDANG A KAWALAN ORGANISASI	
A.4 TANGGUNGJAWAB PENGURUSAN	
Objektif: Memastikan pengurusan memahami peranan mereka dalam keselamatan maklumat dan mengambil tindakan yang bertujuan untuk memastikan semua kakitangan menyedari dan memenuhi tanggungjawab dalam keselamatan maklumat Jabatan / Agensi Sektor Awam Negeri.	
KENYATAAN	**TANGGUNGJAWAB**
A.4.1 TANGGUNGJAWAB PENGURUSAN TERHADAP KAKITANGAN	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan pegawai dan kakitangan Jabatan / Agensi Sektor Awam Negeri serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan undang-undang dan peraturan yang ditetapkan oleh Jabatan / Agensi Sektor Awam Negeri; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT Jabatan / Agensi Sektor Awam Negeri secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan kakitangan Kerajaan Negeri serta pihak ketiga yang berkepentingan sekiranya berlaku pelanggaran dengan undang-undang dan peraturan ditetapkan oleh Jabatan / Agensi Sektor Awam Negeri; dan (d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Jabatan Teknologi Digital dan Inovasi Negeri Sabah, Jabatan / Agensi Sektor Awam Negeri.	ICTSO dan Semua Pengguna

BIDANG A KAWALAN ORGANISASI	
A.5 HUBUNGAN DENGAN PIHAK BERKUASA	
Objektif: Memastikan aliran maklumat berkaitan keselamatan berlaku dengan sewajarnya di antara Jabatan / Agensi Sektor Awam Negeri dan pihak berkuasa.	
KENYATAAN	**TANGGUNGJAWAB**
A.5.1 HUBUNGAN DENGAN PIHAK BERKUASA	
Mewujudkan dan mengemaskini prosedur/senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan termasuk Polis Diraja Malaysia (PDRM) dan Suruhanjaya Komunikasi dan Multimedia (SKMM). Pihak yang dihubungi semasa kecemasan termasuklah tetapi tidak terhad kepada pihak penyedia utiliti, pembekal elektrik, pembekal perkhidmatan dan lain-lain.	CDO, ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

BIDANG A KAWALAN ORGANISASI	
A.6 HUBUNGAN DENGAN PIHAK BERKEPENTINGAN YANG KHUSUS	
Objektif: Memastikan aliran maklumat berkaitan keselamatan berlaku dengan sewajarnya.	
KENYATAAN	**TANGGUNGJAWAB**
A.6.1 HUBUNGAN DENGAN PIHAK BERKEPENTINGAN YANG KHUSUS	
Keselamatan dan pertubuhan profesional hendaklah dikekalkan seperti Agensi Keselamatan Siber Negara (NACSA), Pejabat Ketua Keselamatan Kerajaan (CGSO), Cybersecurity Malaysia dan lain-lain.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

BIDANG A KAWALAN ORGANISASI	
A.7 KECERDASAN ANCAMAN (THREAT INTELLIGENCE)	
Objektif: Memberi kesedaran tentang persekitaran Jabatan / Agensi Sektor Awam Negeri yang terancam supaya tindakan mitigasi yang bersesuaian dapat diambil.	
KENYATAAN	**TANGGUNGJAWAB**
A.7.1 *THREAT INTELLIGENCE*	
Maklumat berkaitan ancaman sedia ada atau yang bakal muncul perlu dikumpul untuk: (a) Membantu dalam tindakan pencegahan kepada ancaman yang mendatangkan kemudaratan kepada Jabatan / Agensi Sektor Awam Negeri; dan (b) Maklumat ancaman yang diterima akan dikumpul untuk membantu mencegah ancaman dan mengurangkan kesan ancaman.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

BIDANG A KAWALAN ORGANISASI	
A.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK	
Objektif: Memastikan risiko keselamatan maklumat berkaitan projek dan serahan ditangani dengan berkesan dalam pengurusan projek sepanjang kitaran hayat projek.	
KENYATAAN	**TANGGUNGJAWAB**
A.8.1 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK	
Berdasarkan Tatacara Pengurusan Projek ICT, aspek keselamatan secara keseluruhan iaitu fizikal, infrastruktur ICT, aplikasi dan data perlu diambil kira dalam menentukan pendekatan projek. Ciri-ciri keselamatan yang terdapat dalam sistem komputer dan aplikasi juga perlu disertakan dalam Laporan Penyerahan Projek.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT
A.8.2 ANALISIS DAN SPESIFIKASI KEPERLUAN KESELAMATAN MAKLUMAT	
Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada. Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut: (a) Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk konsep perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan pelupusan; (b) Semua sistem yang dibangunkan hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Dasar Keselamatan Siber Sektor Awam Sabah;	Pentadbir Sistem ICT

(c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan (d) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data.	

BIDANG A **KAWALAN ORGANISASI**	
A.9 INVENTORI MAKLUMAT DAN ASET ICT	
Objektif: Mengenalpasti maklumat dan aset ICT bagi memelihara keselamatan maklumat dan menetapkan pemilikan yang bersesuaian.	
KENYATAAN	**TANGGUNGJAWAB**
A.9.1 INVENTORI ASET ICT	
Ini bertujuan untuk memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh setiap pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Merekod dan mengemaskini maklumat aset menggunakan borang daftar harta modal dan inventori; (b) Setiap aset ICT hendaklah mempunyai maklumat berikut: (i) Pemilik yang sah dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan (ii) Rekod penempatan yang betul; (c) Peraturan bagi pengendalian aset ICT hendaklah dikenalpasti, di dokumenkan dan dilaksanakan; dan (d) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pentadbir Sistem ICT dan Pegawai Aset ICT

A.9.2 PEMILIKAN ASET ICT	
Aset ICT yang diselenggara hendaklah hak milik Jabatan / Agensi Sektor Awam Negeri. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut: (a) Memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset; (b) Memastikan aset telah dikelaskan dan dilindungi; (c) Mengenalpasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan; (d) Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan (e) Memastikan semua jenis aset dipelihara dengan baik.	Pentadbir Sistem ICT, Pegawai Aset ICT dan Semua Pengguna

BIDANG A KAWALAN ORGANISASI	
A.10 PENGGUNAAN MAKLUMAT DAN ASET ICT	
Objektif: Memastikan maklumat dan aset ICT dilindungi, diguna dan dikendali sewajarnya.	
KENYATAAN	**TANGGUNGJAWAB**
A.10.1 PENGGUNAAN ASET ICT	
Memastikan semua peraturan pengendalian aset ICT dikenal pasti, didokumenkan dan dilaksanakan.	Pegawai Aset dan Semua Pengguna
A.10.2 PENGENDALIAN MAKLUMAT	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (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 rahsia rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua Pengguna

BIDANG A KAWALAN ORGANISASI	
A.11 PEMULANGAN ASET ICT	
Objektif: Melindungi aset Jabatan / Agensi Sektor Awam Negeri sebagai sebahagian dari proses pertukaran atau penamatan perkhidmatan kakitangan, kontrak dan perjanjian.	
KENYATAAN	**TANGGUNGJAWAB**
A.11.1 PEMULANGAN ASET ICT	
Pengguna hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan apabila bersara, bertukar Jabatan/Agensi dan penamatan perkhidmatan, kontrak dan perjanjian.	ICTSO, Pentadbir Sistem ICT dan Semua Pengguna

BIDANG A KAWALAN ORGANISASI	
A.12 PENGELASAN MAKLUMAT	
Objektif: Memastikan pengenalpastian dan pemahaman terhadap keperluan perlindungan maklumat berdasarkan kepentingan Jabatan / Agensi Sektor Awam Negeri.	
KENYATAAN	**TANGGUNGJAWAB**
A.12.1 PENGELASAN MAKLUMAT	
Maklumat hendaklah dikelaskan sewajarnya oleh pegawai yang diberi kuasa mengikut Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam Arahan Keselamatan yang sedang berkuat kuasa seperti berikut:- (a) Rahsia Besar; (b) Rahsia; (c) Sulit; dan (d) Terhad. Selain daripada maklumat rahsia rasmi adalah dikelaskan sebagai terbuka.	Semua Pengguna

BIDANG A KAWALAN ORGANISASI	
A.13 PENANDAAN MAKLUMAT	
Objektif: Memudahkan komunikasi dalam pengelasan maklumat dan menyokong automasi pemprosesan dan pengurusan maklumat.	
KENYATAAN	**TANGGUNGJAWAB**
A.13.1 PENANDAAN MAKLUMAT	
Maklumat hendaklah ditanda dan dikendali berasaskan peringkat keselamatan yang dikenal pasti selaras dengan Arahan Keselamatan.	Semua Pengguna

BIDANG A KAWALAN ORGANISASI	
A.14 PERTUKARAN MAKLUMAT	
Objektif: Mengekalkan keselamatan dalam pertukaran maklumat di dalam Jabatan / Agensi Sektor Awam Negeri dan dengan mana-mana pihak luar yang berkepentingan.	
KENYATAAN	**TANGGUNGJAWAB**
A.14.1 DASAR DAN PROSEDUR PERTUKARAN MAKLUMAT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; (b) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari Jabatan / Agensi Sektor Awam Negeri; dan (c) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua Pengguna

A.14.2 PERJANJIAN BERKAITAN PERTUKARAN MAKLUMAT	
Perjanjian perlu diwujudkan untuk pertukaran maklumat di antara Jabatan / Agensi Sektor Awam Negeri dengan pihak luar.	ICTSO, Pentadbir Sistem ICT dan Semua Pengguna
A.14.3 MEL ELEKTRONIK (E-MEL)	
Penggunaan e-mel di Jabatan / Agensi Sektor Awam Negeri hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut:- (a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh Jabatan / Agensi Sektor Awam Negeri sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (b) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi, dan pastikan alamat e-mel penerima adalah betul; (c) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; (d) Pengguna dinasihatkan menggunakan fail kepilan sekiranya perlu. Kaedah pemampatan (*compress*) untuk mengurangkan saiz adalah disarankan; (e) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui. Jika terdapat keraguan perlu dilaporkan kepada pentadbir e-mel pada kadar segera; (f) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi	Pentadbir Sistem ICT dan Semua Pengguna

dengannya sebelum meneruskan transaksi maklumat melalui e-mel; (g) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; (h) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; (i) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing; (j) Sebarang status pengguna (bertukar agensi, bersara, diberhentikan, tidak dapat dikesan, meninggal dunia dan sebagainya) perlu dimaklumkan kepada Pentadbir e-mel oleh Pegawai Mengawal Pusat bagi tujuan pengemaskinian e-mel yang terlibat; (k) E-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang bersesuaian; (l) Menggunakan enkripsi (*encryption*) bagi maklumat rahsia rasmi yang dihantar secara elektronik bagi pematuhan kepada perenggan 134 Arahan Keselamatan; (m) Pentadbir E-mel berhak untuk menggantung sementara akaun e-mel pengguna yang didapati telah diceroboh oleh pihak ketiga; dan (n) Pentadbir E-mel perlu mengemas kini keterangan pengguna e-mel dari semasa ke semasa bagi memastikan maklumat tersebut sahih dan tepat (contoh: nama pusat perkhidmatan, jawatan dan lain-lain).	

BIDANG A KAWALAN ORGANISASI	
A.15 KAWALAN CAPAIAN	
Objektif: Memastikan hanya capaian yang disahkan dan mengelakkan capaian yang tidak sah kepada maklumat dan aset ICT.	
KENYATAAN	**TANGGUNGJAWAB**
A.15.1 DASAR KAWALAN CAPAIAN	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Keperluan keselamatan aplikasi; (b) Hak capaian dan dasar klasifikasi maklumat sistem dan rangkaian; (c) Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa; (d) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (e) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; (f) Kawalan ke atas kemudahan pemprosesan maklumat; (g) Pengasingan peranan kawalan capaian; (h) Kebenaran rasmi permintaan capaian;	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

(i) Keperluan semakan hak capaian berkala; (j) Pembatalan hak capaian; (k) Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan (l) Capaian *privilege*.	
A.15.2 CAPAIAN RANGKAIAN	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:- (a) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; (b) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; dan (c) Menyediakan polisi bagi mengawal capaian bagi semua rangkaian yang dikongsi *(shared networks)*, terutama yang keluar dari rangkaian Jabatan / Agensi Sektor Awam Negeri.	ICTSO dan Pentadbir Sistem ICT
A.15.3 CAPAIAN INTERNET	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet di Jabatan / Agensi Sektor Awam Negeri hendaklah dipantau secara berterusan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian Jabatan / Agensi Sektor Awam Negeri; (b) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja;	ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Semua Pengguna

(c) Pentadbir Sistem ICT berhak untuk memantau penggunaan Internet bagi pengguna yang menggunakan sistem rangkaian dan peralatan ICT yang disediakan oleh Jabatan / Agensi Sektor Awam Negeri; (d) Penggunaan teknologi *Bandwidth Management System* untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; (e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan; (f) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; (g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pegawai Mengawal Pusat berkenaan sebelum dimuat naik ke Internet; (h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; (i) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh Jabatan / Agensi Sektor Awam Negeri; (j) Hanya pengguna yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam dan media sosial. Walau bagaimanapun,kandungan perbincangan awam ini tertakluk kepada dasar dan peraturan yang telah ditetapkan;	

(k) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:- (i) Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; (ii) Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah; (iii) Menggunakan perkhidmatan *proxy* atau VPN bagi tujuan *bypass* sistem rangkaian Jabatan / Agensi Sektor Awam Negeri bagi tujuan capaian Internet; dan (iv) Memuat naik sebarang dokumen, perisian berlesen, emel dan sebagainya ke *server* atau ruang storan yang dipunyai oleh pihak luar tanpa sebarang kebenaran daripada ICTSO. (l) Setiap pengguna Jabatan / Agensi Sektor Awam Negeri bertanggungjawab ke atas sebarang salah perlakuan dan tindakan yang diambil sewaktu menggunakan kemudahan Internet yang diberikan; dan (m) ICTSO atau wakil yang dibenarkan ICTSO berhak untuk memeriksa setiap komputer yang dibekalkan oleh Jabatan / Agensi Sektor Awam Negeri atau menggunakan rangkaian komputer Jabatan / Agensi Sektor Awam Negeri untuk memastikan setiap arahan di dalam pelan ini dipatuhi oleh semua pengguna.	

BIDANG A KAWALAN ORGANISASI	
A.16 PENGURUSAN IDENTITI	
Objektif: Membenarkan individu dan sistem yang menggunakan identiti unik membuat capaian kepada maklumat Jabatan / Agensi Sektor Awam Negeri dan aset ICT serta melaksanakan tugasan berdasarkan hak capaian.	
KENYATAAN	**TANGGUNGJAWAB**
A.16.1 PENDAFTARAN DAN PENAMATAN PENGGUNA	
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan capaian dan pembatalan hak capaian. Perkara-perkara berikut hendaklah dipatuhi:- (a) Akaun pengguna yang diperuntukkan oleh Jabatan / Agensi Sektor Awam Negeri sahaja boleh digunakan; (b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (c) Akaun pengguna yang diwujudkan akan diberi tahap capaian mengikut keperluan dan hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; (d) Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem terlebih dahulu dengan mengambilkira kepentingan tugasan dan risiko berkaitan; (e) Penggunaan akaun pengguna milik pengguna lain atau akaun yang dikongsi bersama adalah dilarang; (f) Permohonan akaun pengguna dari pihak luaran/ketiga (contoh: subsidiari Jabatan / Agensi Sektor Awam Negeri, pembekal, pelajar praktikal atau lain-lain) perlu mendapat kelulusan ICTSO terlebih dahulu dengan sokongan pemilik sistem. Pemilik akaun perlu menandatangani Surat Perakuan	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

Pelan Keselamatan Siber di Lampiran 2 dan perakuan Akta Rahsia Rasmi seperti di Lampiran 3; (g) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan Jabatan / Agensi Sektor Awam Negeri. Akaun boleh ditarik balik/dibekukan jika penggunaannya melanggar peraturan; (i) Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan oleh Jabatan / Agensi Sektor Awam Negeri; (ii) Pengguna yang bercuti belajar melebihi tempoh enam (6) bulan seperti mana yang diluluskan oleh Jabatan / Agensi Sektor Awam Negeri; (iii) Bertukar bidang tugas kerja; (iv) Bertukar ke agensi/pusat lain; (v) Bersara; (vi) Ditamatkan perkhidmatan; dan (vii) Dalam prosiding dan/atau dikenakan tindakan tatatertib bagi tujuan dibuang kerja.	

BIDANG A KAWALAN ORGANISASI	
A.17 PENGESAHAN MAKLUMAT	
Objektif: Memastikan pengesahan entiti yang betul dan mengelakkan kegagalan ketika proses pengesahan.	
KENYATAAN	**TANGGUNGJAWAB**
A.17.1 PENGURUSAN PENGESAHAN MAKLUMAT RAHSIA PENGGUNA	
Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal dan diselia melalui proses pengurusan yang formal.	ICTSO dan Pentadbir Sistem ICT
A.17.2 PENGGUNAAN MAKLUMAT PENGESAHAN RAHSIA	
Melaksanakan langkah-langkah perlindungan seperti berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) Menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan; (f) Melaksanakan peraturan berkaitan maklumat rahsia rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan berdasarkan Arahan Keselamatan; (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum; dan (h) Mengawal aktiviti penggunaan media sosial seperti dibawah:	Semua Pengguna

(i) Mengelakkan ketirisan maklumat; (ii) Tidak memberi atau mendedahkan sebarang komen atau pernyataan atau isu yang menyentuh perkara-perkara yang boleh menjejaskan imej dan dasar kerajaan; (iii) Tidak menyebarkan maklumat yang berbentuk fitnah, hasutan dan lucah atau cuba memprovokasikan sesuatu isu yang menyalahi peraturan dan undang undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan (iv) Tidak menggunakan saluran media sosial hingga mengganggu fokus dalam urusan kerja.	
A.17.3 PENGURUSAN KATA LALUAN	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh Jabatan / Agensi Sektor Awam Negeri seperti berikut:- (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara, angka atau aksara khusus. Sekiranya terdapat kekangan teknologi untuk memenuhi bilangan aksara ini, risiko ini perlu didaftarkan dan melaksanakan pelan mitigasi yang bersesuaian; (d) Tukar kata laluan jika diperlukan atau apabila disyaki telah dikompromi;	Pentadbir Sistem ICT dan Semua Pengguna

(e) Penyimpanan kata laluan secara automatik adalah tidak dibenarkan; (f) Kata laluan *Windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (g) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; (h) Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; (i) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (j) Mengelakkan penggunaan semula kata laluan yang baharu digunakan; (k) Pengguna dilarang menggunakan sebarang maklumat peribadi seperti tarikh lahir, nombor gaji, nombor kad pengenalan dan sebagainya sebagai kata laluan; (l) Sistem yang dibangunkan/digunakan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna; (m) Sebarang urusan penukaran kata laluan melalui telefon dan e-mel perlu mengambil langkah-langkah keselamatan yang bersesuaian; (n) Pentadbir Sistem ICT di semua pusat perlu bertanggungjawab ke atas akaun *administrator* dan kata laluan untuk semua perkasasan ICT di pusat masing masing. Kata laluan peralatan dan/atau sebarang sistem hendaklah direkodkan dan disimpan ditempat selamat untuk kelangsungan operasi sekiranya berlaku perubahan Pentadbir Sistem ICT di pusat;	

(o) Pelaksanaan *Multi-Level Authentication* (MFA) / *Two-Level Authentication* (2FA) dalam menangani ancaman keselamatan siber kepada akaun pengguna mengikut keperluan; (p) Penggunaan teknologi tambahan seperti *biometric authentication* boleh dipertimbangkan untuk mengukuhkan keselamatan; dan (q) Penggunaan alat seperti *password vault* atau *Single Sign-On* (SSO) digalakkan kerana ia mengurangkan beban pengguna untuk menghafal banyak kata laluan, sekali gus meningkatkan keberkesanan kawalan.	

BIDANG A KAWALAN ORGANISASI	
A.18 HAK CAPAIAN	
Objektif: Memastikan capaian kepada maklumat dan aset ICT ditakrifkan dan disahkan mengikut keperluan perkhidmatan Jabatan / Agensi Sektor Awam Negeri.	
KENYATAAN	**TANGGUNGJAWAB**
A.18.1 PERUNTUKAN CAPAIAN PENGGUNA	
Prosedur bagi proses penyediaan capaian pengguna untuk kebenaran dan pembatalan capaian pengguna ke atas semua aplikasi dan perkhidmatan ICT perlu dilaksanakan bagi tujuan capaian sistem dan perkhidmatan.	ICTSO, Pemilik Sistem dan Pentadbir Sistem ICT
A.18.2 SEMAKAN SEMULA HAK CAPAIAN	
Mewujudkan prosedur penetapan dan penggunaan hak capaian pengguna kepada perkhidmatan ICT berdasarkan skop tugas yang dikawal dan diselia. Bagi akaun pengguna yang tidak aktif, pentadbir sistem perlu menyemak status semasa pengguna sebelum sebarang tindakan yang bersesuaian diambil. Semakan ID tidak aktif perlu dilakukan sekurang-kurangnya dua kali setahun. Hak Capaian ini juga tertakluk kepada kebenaran daripada pemilik sistem/aplikasi/lesen/data dan juga peraturan-peraturan lain yang berkenaan.	ICTSO, Pemilik Sistem dan Pentadbir Sistem ICT
A.18.3 PEMBATALAN ATAU PELARASAN HAK CAPAIAN	
Hak capaian pengguna dan pihak luaran/ketiga untuk maklumat atau pemprosesan maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan tugas, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam Jabatan / Agensi Sektor Awam Negeri.	ICTSO, Pemilik Sistem dan Pentadbir Sistem ICT

BIDANG A KAWALAN ORGANISASI	
A.19 KESELAMATAN MAKLUMAT BERHUBUNG DENGAN PEMBEKAL	
Objektif: Mengekalkan tahap persetujuan bagi keselamatan maklumat dalam hubungan pembekal.	
KENYATAAN	**TANGGUNGJAWAB**
A.19.1 DASAR KESELAMATAN BERHUBUNG DENGAN PEMBEKAL	
Perkara yang perlu dipatuhi termasuk yang berikut: (a) Membaca, memahami dan mematuhi Pelan Keselamatan Siber Jabatan / Agensi Sektor Awam Negeri yang berkaitan; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak pembekal; (d) Capaian kepada aset ICT Jabatan / Agensi Sektor Awam Negeri perlu berlandaskan kepada perjanjian; (e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak pembekal. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai; (i) Pelan Keselamatan Siber Jabatan / Agensi Sektor Awam Negeri; (ii) Tapisan Keselamatan (jika berkaitan); (iii) Perakuan Akta Rahsia Rasmi 1972; dan (iv) Hak Harta Intelek. (f) Menandatangani Surat Akuan Pematuhan Pelan Keselamatan Siber Jabatan / Agensi Sektor Awam Negeri dan Akta Rahsia Rasmi 1972 sebagaimana di Lampiran 2 dan 3.	ICTSO, Pentadbir Kontrak, Pentadbir Sistem ICT dan Pembekal

BIDANG A KAWALAN ORGANISASI	
A.20 MENANGANI KESELAMATAN MAKLUMAT DALAM PERJANJIAN DENGAN PEMBEKAL	
Objektif: Mengekalkan tahap persetujuan bagi keselamatan maklumat dalam hubungan pembekal.	
KENYATAAN	**TANGGUNGJAWAB**
A.20.1 MENANGANI KESELAMATAN DALAM PERJANJIAN DENGAN PEMBEKAL	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; (b) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mencapai, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan Jabatan / Agensi Sektor Awam Negeri; dan (c) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh Jabatan / Agensi Sektor Awam Negeri.	ICTSO, Pentadbir Kontrak, Pemilik Projek, Pentadbir Sistem ICT dan Pembekal

BIDANG A KAWALAN ORGANISASI	
A.21 PENGURUSAN KESELAMATAN MAKLUMAT DALAM RANTAIAN BEKALAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI	
Objektif: Mengekalkan tahap persetujuan bagi keselamatan maklumat dalam hubungan pembekal.	
KENYATAAN	**TANGGUNGJAWAB**
A.21.1 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/perkhidmatan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: (a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; (b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan (c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	ICTSO, Pentadbir Kontrak, Pemilik Projek, Pentadbir Sistem ICT dan Pembekal
A.21.2 MEKANISME KAWALAN PERALATAN SEWAAN/UJICUBA (PROOF OF CONCEPT)	
Sebarang *proof of concept* (POC) yang dijalankan perlu mendapatkan kelulusan ICTSO dengan mengambilkira perkara-perkara berikut: (a) Penerimaan dan Pembekal	ICTSO, Pemilik Projek, Pentadbir Sistem ICT dan Pembekal

(i) Peralatan/perisian yang diterima bebas daripada sebarang *malware* dan perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT Jabatan / Agensi Sektor Awam Negeri; dan (ii) Pembekal yang terlibat perlu memastikan semua syarat keselamatan dipatuhi: ● Pelan Keselamatan Siber Jabatan / Agensi Sektor Awam Negeri; ● Perakuan Akta Rahsia Rasmi 1972; dan ● Hak Harta Intelek (b) Penyelenggaraan (i) Capaian melalui rangkaian luar Jabatan / Agensi Sektor Awam Negeri adalah tidak dibenarkan; dan (ii) Aktiviti penyelenggaraan adalah di bawah pengawasan pegawai Jabatan / Agensi Sektor Awam Negeri. (c) Pemulangan (i) Maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (*secured delete*); dan (ii) Memastikan semua maklumat tidak tertinggal pada peralatan/perisian; (d) Hasil penemuan atau hasil dari POC perlu diserahkan dan dibentang kepada pihak Jabatan / Agensi Sektor Awam Negeri dan tidak dibenarkan untuk disebarkan atau dikongsi dengan mana-mana pihak luar; dan (e) Sebarang perubahan yang dilakukan perlu direkod dan dikembalikan kepada kepada asal seperti sebelum POC.	

BIDANG A KAWALAN ORGANISASI	
A.22 PENGURUSAN PEMANTAUAN, KAJIAN SEMULA DAN PERUBAHAN PERKHIDMATAN PEMBEKAL	
Objektif: Mengekalkan tahap persetujuan bagi keselamatan maklumat dan penyampaian perkhidmatan selaras dengan perjanjian pembekal.	
KENYATAAN	**TANGGUNGJAWAB**
A.22.1 MEMANTAU DAN MENGKAJI SEMULA PERKHIDMATAN PEMBEKAL	
Perkara-perkara yang perlu diambil kira adalah seperti berikut: (a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal; dan (b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa.	ICTSO, Pembekal dan Pemilik Projek
A.22.2 MENGURUSKAN PERUBAHAN KEPADA PERKHIDMATAN PEMBEKAL	
Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	ICTSO, Pembekal dan Pemilik Projek

BIDANG A KAWALAN ORGANISASI	
A.23 KESELAMATAN MAKLUMAT DALAM PENGGUNAAN PERKHIDMATAN AWAN (CLOUD SERVICES)	
Objektif: Memperinci dan menguruskan keselamatan maklumat dalam menggunakan perkhidmatan awan (*cloud services*).	
KENYATAAN	**TANGGUNGJAWAB**
A.23.1 PENGGUNAAN STORAN AWAN (CLOUD)	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan setiap maklumat rasmi hanya disimpan dalam storan awan awam (*public cloud storage*) yang dibenarkan oleh Kerajaan Negeri; (b) Memastikan pengguna tidak menyimpan dokumen tidak rasmi dan tidak berkaitan seperti yang berbentuk hiburan dan tidak bermanfaat pada storan awan yang disediakan oleh Jabatan / Agensi Sektor Awam Negeri; (c) Semua pengguna perlu memastikan kandungan storan awan yang disediakan oleh Jabatan / Agensi Sektor Awam Negeri diurus dengan baik dan sentiasa membuat kerja-kerja pengemaskinian data atau *housekeeping* dari semasa ke semasa; dan (d) Pengguna perlu memastikan perkongsian fail dan folder hanya dibuat untuk pengguna yang dibenarkan sahaja dalam tempoh yang dibenarkan.	Semua pengguna

BIDANG A KAWALAN ORGANISASI	
A.24 PERANCANGAN DAN PERSEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT	
Objektif: Memastikan tindak balas yang cepat, berkesan, konsisten dan teratur kepada insiden keselamatan maklumat termasuk komunikasi pada kejadian keselamatan maklumat.	
KENYATAAN	**TANGGUNGJAWAB**
A.24.1 TANGGUNGJAWAB DAN PROSEDUR	
Kerajaan Negeri Sabah menubuhkan sgCSIRT yang bertindak sebagai pasukan *Cyber Security Incident Response Team* (CSIRT) bagi mengendali insiden keselamatan siber. Tanggungjawab sgCSIRT meliputi semua bidang tugas pengurusan pengendalian insiden keselamatan siber agensi sektor awam negeri seperti yang dinyatakan pada **A.2.6 SABAH GOVERNMENT CYBER SECURITY INCIDENT RESPONSE TEAM (sgCSIRT)**.	ICTSO, sgCSIRT dan Pemilik Projek/Sistem

BIDANG A KAWALAN ORGANISASI	
A.25 PENILAIAN DAN KEPUTUSAN MENGENAI INSIDEN KESELAMATAN MAKLUMAT	
Objektif: Memastikan kategori dan keutamaan yang efektif dalam insiden keselamatan maklumat.	
KENYATAAN	**TANGGUNGJAWAB**
A.25.1 PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT	
Insiden keselamatan siber ialah kejadian siber yang tidak diingini apabila berlakunya kehilangan kerahsiaan maklumat, gangguan terhadap integriti data atau sistem, atau gangguan yang menyebabkan kegagalan dalam memperoleh maklumat daripada sistem komputer dan kemungkinan berlakunya kesalahan pelanggaran peraturan keselamatan maklumat, dasar-dasar tertentu atau amalan piawai keselamatan siber. Contoh jenis-jenis insiden keselamatan siber ialah: (a) Penafian Perkhidmatan (*Denial of Service, DoS*) atau Penafian Perkhidmatan Teragih (*Distributed Denial of Service, DDoS*); (b) Pencerobohan (*Intrusion*); (c) Jangkitan Perisian Hasad (*Malicious Software Malware*); (d) Pengehosan Perisian Hasad (*Malware Hosting*); (e) Percubaan Pencerobohan *(Intrusion Attempt*); dan (f) Potensi Serangan (*Potential Attack*). Tindakan ke atas insiden yang berlaku hendaklah dibuat berasaskan kepada tahap kritikal sesuatu insiden. Tahap keutamaan tindakan ke atas insiden akan ditentukan seperti berikut: **(a) Keutamaan 1**	CDO, ICTSO, sgCSIRT dan Pentadbir Sistem ICT

Insiden keselamatan siber yang memberi impak tinggi terhadap pertahanan dan keselamatan negara, kestabilan ekonomi negara, imej negara, keupayaan Kerajaan Negeri Sabah untuk berfungsi, kesihatan dan keselamatan awam serta privasi individu. **(b) Keutamaan 2** Insiden keselamatan siber yang tidak memberi impak seperti mana yang dinyatakan dalam Keutamaan 1. Bagi insiden yang dinilai dalam kategori tahap keutamaan 1, insiden perlu dimaklumkan kepada ICTSO dan CDO untuk tindakan berikut: (a) Mengurus dan mengambil tindakan ke atas insiden yang berlaku sehingga keadaan pulih; (b) Mengaktifkan Pelan Pemulihan Perkhidmatan (PKP) jika perlu; dan (c) Menentukan samada insiden ini perlu dilaporkan kepada agensi penguatkuasaan undang-undang/keselamatan (NACSA, PDRM, SKMM dan lain-lain). Sekiranya insiden yang dinilai berada di dalam tahap keutamaan 2, insiden tersebut hanya perlu diselesaikan di peringkat dalaman JTDINS/ICTSO atau/dan makluman kepada CDO (jika perlu).	

BIDANG A KAWALAN ORGANISASI	
A.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT	
Objektif: Memastikan tindak balas yang efisien dan efektif kepada insiden keselamatan maklumat.	
KENYATAAN	**TANGGUNGJAWAB**
A.26.1 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT	
Insiden keselamatan maklumat hendaklah dikendalikan menurut prosedur yang didokumenkan. Tindak balas yang dirancang dan yang diambil perlu direkodkan.	ICTSO dan sgCSIRT

BIDANG A KAWALAN ORGANISASI	
A.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT	
Objektif: Mengurangkan kebarangkalian atau kesan daripada insiden akan datang.	
KENYATAAN	**TANGGUNGJAWAB**
A.27.1 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT	
Setiap insiden keselamatan maklumat direkodkan dan dinilai untuk memastikan kawalan dan tindakan yang diambil adalah mencukupi atau perlu ditambah.	ICTSO dan sgCSIRT

BIDANG A KAWALAN ORGANISASI	
A.28 PENGUMPULAN BAHAN BUKTI	
Objektif: Memastikan pengurusan bukti insiden keselamatan maklumat yang teratur bagi tujuan rujukan sekiranya diperlukan.	
KENYATAAN	**TANGGUNGJAWAB**
A.28.1 PENGUMPULAN BAHAN BUKTI	
Jabatan / Agensi Sektor Awam Negeri hendaklah menentukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti.	ICTSO dan sgCSIRT

BIDANG A KAWALAN ORGANISASI	
A.29 KESINAMBUNGAN KESELAMATAN MAKLUMAT	
Objektif: Melindungi keselamatan maklumat dan aset ICT ketika berlakunya gangguan.	
KENYATAAN	**TANGGUNGJAWAB**
A.29.1 PERANCANGAN KESINAMBUNGAN KESELAMATAN MAKLUMAT	
Jabatan hendaklah memastikan keperluan keselamatan maklumat di dalam pelan pengurusan kesinambungan keselamatan maklumat apabila berlaku gangguan/bencana. Ini adalah bertujuan untuk memastikan ketersediaan perkhidmatan Jabatan tidak terganggu selain dapat mengenal pasti aspek keselamatan maklumat dalam pelan Pengurusan Kesinambungan Perkhidmatan (PKP). Pelan ini hendaklah diangkat untuk pengesahan CDO.	Koordinator PKP, Pasukan Tindak Balas Kecemasan, Pasukan Komunikasi Krisis dan Pasukan Pemulihan Bencana (DRP) ICT
A.29.2 PELAKSANAAN KESINAMBUNGAN KESELAMATAN MAKLUMAT	
Jabatan hendaklah memastikan aspek keselamatan maklumat dalam pelan Pengurusan Kesinambungan Perkhidmatan (PKP) diwujudkan, didokumentasi, dilaksana dan dikemas kini (proses, prosedur serta kawalan) untuk	Koordinator PKP, Pasukan Tindak Balas Kecemasan, Pasukan Komunikasi Krisis

memastikan tahap keselamatan maklumat dalam kesinambungan perkhidmatan menepati keperluan semasa berlaku gangguan/bencana. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh pihak Pengurusan Jabatan. Perkara-perkara berikut hendaklah dipatuhi: (a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan; (b) Mengenal pasti peristiwa atau ancaman yang boleh mengakibatkan gangguan terhadap perkhidmatan Jabatan serta kemungkinan dan impak gangguan tersebut terhadap keselamatan ICT; (c) Menjalankan analisis impak perkhidmatan; (d) Melaksanakan simulasi terhadap prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (e) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (f) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (g) Membuat backup mengikut prosedur yang telah ditetapkan; dan (h) Menguji, menyelenggara dan mengemas kini pelan keselamatan ICT sekurang-kurangnya setahun sekali. Pelan PKP hendaklah dibangunkan, didokumentasikan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;	dan Pasukan Pemulihan Bencana (DRP) ICT

(b) Senarai personel utama sgCSIRT, Jabatan, pembekal dan pihak ketiga berserta nombor yang boleh dihubungi (faksimili, telefon, sistem pesanan ringkas (sms), dan e-mel). Senarai personel kedua juga hendaklah disediakan sebagai menggantikan personel utama yang tidak dapat hadir untuk menangani insiden; (c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; (e) Perjanjian dengan pembekal dan pihak ketiga untuk mendapatkan keutamaan penyambungan semula perkhidmatan; (f) Salinan dokumentasi pelan PKP hendaklah disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan PKP hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi perkhidmatan untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan; (g) Ujian pelan PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan; dan (h) Jabatan hendaklah memastikan salinan dokumentasi pelan PKP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

BIDANG A KAWALAN ORGANISASI	
A.30 PERSEDIAAN ICT UNTUK KESINAMBUNGAN PERKHIDMATAN	
Objektif: Memastikan maklumat dan aset ICT Jabatan / Agensi Sektor Awam Negeri tersedia apabila berlaku gangguan.	
KENYATAAN	**TANGGUNGJAWAB**
A.30.1 MENENTUSAHKAN, MENGKAJI SEMULA DAN MENILAI KESINAMBUNGAN KESELAMATAN MAKLUMAT	
Jabatan hendaklah memastikan keperluan keselamatan maklumat di dalam pelan pengurusan kesinambungan keselamatan maklumat apabila berlaku gangguan/bencana. Ini adalah bertujuan untuk memastikan ketersediaan perkhidmatan Jabatan tidak terganggu selain dapat mengenal pasti aspek keselamatan maklumat dalam pelan Pengurusan Kesinambungan Perkhidmatan (PKP). Pelan ini hendaklah diangkat untuk pengesahan CDO. Pelan Kesinambungan Perkhidmatan (PKP) termasuk Pelan Pemulihan Bencana (DRP) hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi perkhidmatan Jabatan / Agensi Sektor Awam Negeri untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian ini hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan pegawai yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. Jabatan hendaklah mengesahkan kawalan terhadap keselamatan maklumat dalam pelan Pengurusan Kesinambungan Perkhidmatan (PKP) dilaksanakan secara berkala untuk memastikan pelan berkenaan sahih dan berkesan semasa berlaku gangguan/bencana.	Koordinator PKP, Pasukan Tindak Balas Kecemasan, Pasukan Komunikasi Krisis dan Pasukan Pemulihan Bencana (DRP) ICT, Pemilik Sistem dan Semua Pengguna

BIDANG A KAWALAN ORGANISASI	
A.31 KEPERLUAN UNDANG-UNDANG, PERATURAN DAN KONTRAK	
Objektif: Memastikan pematuhan kepada keperluan undang-undang, peraturan dan kontrak yang berkaitan dengan keselamatan maklumat.	
KENYATAAN	**TANGGUNGJAWAB**
A.31.1 KENAL PASTI KEPERLUAN UNDANG-UNDANG, PERATURAN DAN KONTRAK YANG TERPAKAI	
Setiap pengguna Jabatan / Agensi Sektor Awam Negeri, pihak luaran/ketiga dan pembekal yang mempunyai urusan dengan perkhidmatan ICT hendaklah membaca, memahami dan mematuhi Pelan Keselamatan Siber Jabatan / Agensi Sektor Awam Negeri dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa seperti di Lampiran 1.	Semua pengguna, Pembekal dan Pihak Luaran/Ketiga
A.31.2 PERATURAN KAWALAN KRIPTOGRAFI	
Kawalan kriptografi perlu digunakan bagi tujuan pematuhan kepada undang-undang, peraturan dan kontrak yang diguna pakai.	Semua pengguna, Pembekal dan Pihak Luaran/Ketiga

BIDANG A KAWALAN ORGANISASI	
A.32 HAK HARTA INTELEKTUAL	
Objektif: Memastikan pematuhan kepada keperluan undang-undang, peraturan dan kontrak yang berkaitan dengan Hak Harta intelektual dan penggunaan Hak Milik produk.	
KENYATAAN	**TANGGUNGJAWAB**
A.32.1 KAWALAN HAK HARTA INTELEKTUAL	
Memastikan pematuhan terhadap keperluan undang-undang, peraturan dan kontrak yang berkaitan Hak Harta Intelektual. Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Semua pengguna, Pembekal dan Pihak Luaran/Ketiga

BIDANG A KAWALAN ORGANISASI	
A.33 PERLINDUNGAN REKOD	
Objektif: Memastikan pematuhan kepada keperluan undang-undang, peraturan dan kontrak serta jangkaan masyarakat atau sosial berkaitan perlindungan dan ketersediaan rekod.	
KENYATAAN	**TANGGUNGJAWAB**
A.33.1 KAWALAN PERLINDUNGAN REKOD	
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas pihak yang tidak berkenaan seperti yang terkandung di dalam keperluan undang-undang, peraturan dan kontrak.	Semua pengguna, Pembekal dan Pihak Luaran/Ketiga

BIDANG A KAWALAN ORGANISASI	
A.34 PRIVASI DAN PERLINDUNGAN MAKLUMAT PENGECAMAN INDIVIDU (PII)	
Objektif: Memastikan pematuhan kepada keperluan undang-undang, peraturan dan kontrak berkaitan aspek keselamatan maklumat dalam perlindungan maklumat pengecaman individu (PII).	
KENYATAAN	**TANGGUNGJAWAB**
A.34.1 KAWALAN PRIVASI DAN PERLINDUNGAN MAKLUMAT PENGECAMAN INDIVIDU (PII)	
Jabatan / Agensi Sektor Awam Negeri hendaklah memberi jaminan dalam melindungi maklumat pengecaman individu (PII) seperti terkandung di dalam undang-undang dan peraturan Kerajaan Malaysia.	Semua pengguna, Pembekal dan Pihak Luaran/Ketiga

BIDANG A KAWALAN ORGANISASI	
A.35 KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI	
Objektif: Memastikan kesesuaian, kecekapan dan keberkesanan yang berterusan dalam pendekatan Jabatan / Agensi Sektor Awam Negeri untuk menguruskan keselamatan maklumat.	
KENYATAAN	**TANGGUNGJAWAB**
A.35.1 KEPERLUAN KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI	
Penilaian keselamatan yang dilaksanakan oleh pihak ketiga boleh dilaksanakan secara terancang apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	ICTSO dan Pentadbir Sistem

BIDANG A KAWALAN ORGANISASI	
A.36 PEMATUHAN KEPADA POLISI, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT	
Objektif: Memastikan keselamatan maklumat yang dilaksanakan dan beroperasi sesuai dengan polisi keselamatan, polisi tajuk khusus, peraturan dan piawaian yang dikaji semula secara berkala.	
KENYATAAN	**TANGGUNGJAWAB**
A.36.1 PEMATUHAN POLISI DAN PIAWAIAN KESELAMATAN MAKLUMAT	
Jabatan / Agensi Sektor Awam Negeri hendaklah membuat kajian semula secara berkala terhadap pematuhan polisi dan piawaian keselamatan maklumat.	ICTSO
A.36.2 KAJIAN SEMULA PEMATUHAN TEKNIKAL	
Jabatan / Agensi Sektor Awam Negeri hendaklah membuat kajian semula secara berkala terhadap pematuhan keselamatan maklumat dan prosedur yang terkandung di dalam polisi, piawaian dan keperluan teknikal.	ICTSO dan Pentadbir Sistem ICT

BIDANG A KAWALAN ORGANISASI	
A.37 MENDOKUMENKAN PROSEDUR OPERASI	
Objektif: Memastikan operasi di kemudahan pemprosesan maklumat tepat dan selamat.	
KENYATAAN	**TANGGUNGJAWAB**
A.37.1 KEPERLUAN MENDOKUMENKAN PROSEDUR OPERASI	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur operasi ICT yang diwujudkan perlu dikenal pasti dan sekiranya masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap; dan (c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua Pengguna

BIDANG B KAWALAN SUMBER MANUSIA	
B.1 SARINGAN	
Objektif: Memastikan semua kakitangan adalah berkelayakan dengan jawatan yang dipertimbangkan, kekal layak dan sesuai sepanjang perkhidmatan.	
KENYATAAN	**TANGGUNGJAWAB**
B.1.1 SARINGAN SEBELUM DALAM PERKHIDMATAN	
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan Jabatan / Agensi Sektor Awam Negeri serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan Jabatan / Agensi Sektor Awam Negeri serta pihak ketiga yang terlibat seperti yang termaktub dalam Arahan Keselamatan selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Semua Pengguna

BIDANG B KAWALAN SUMBER MANUSIA	
B.2 TERMA DAN SYARAT PERKHIDMATAN	
Objektif: Memastikan kakitangan faham tanggungjawab mereka dalam keselamatan maklumat untuk jawatan yang dipertimbangkan.	
KENYATAAN	**TANGGUNGJAWAB**
B.2.1 TERMA DAN SYARAT SEBELUM DALAM PERKHIDMATAN	
Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua Pengguna

BIDANG B KAWALAN SUMBER MANUSIA	
B.3 KESEDARAN, PENDIDIKAN DAN LATIHAN KESELAMATAN MAKLUMAT	
Objektif: Memastikan kakitangan dan pihak yang berkepentingan sedar dan memenuhi tanggungjawab keselamatan maklumat.	
KENYATAAN	**TANGGUNGJAWAB**
B.3.1 KESEDARAN, PENDIDIKAN DAN LATIHAN KESELAMATAN MAKLUMAT KETIKA DALAM PERKHIDMATAN	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan pegawai dan kakitangan Jabatan / Agensi Sektor Awam Negeri serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan undang-undang dan peraturan yang ditetapkan oleh Jabatan / Agensi Sektor Awam Negeri; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan maklumat diberi kepada pengguna ICT Jabatan / Agensi Sektor Awam Negeri secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan (c) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Sumber Manusia, Jabatan / Agensi Sektor Awam Negeri.	Semua Pengguna

BIDANG B KAWALAN SUMBER MANUSIA	
B.4 PROSES TINDAKAN DISIPLIN	
Objektif: Memastikan kakitangan dan pihak yang berkepentingan faham ke atas kesan perlanggaran polisi keselamatan, menghalang serta berurusan dengan kakitangan dan pihak yang berkepentingan yang terlibat dengan pelanggaran.	
KENYATAAN	**TANGGUNGJAWAB**
B.4.1 PROSES TINDAKAN DISIPLIN KETIKA DALAM PERKHIDMATAN	
Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan Jabatan / Agensi Sektor Awam Negeri serta pihak ketiga yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan ditetapkan oleh Jabatan / Agensi Sektor Awam Negeri.	Semua Pengguna

BIDANG B KAWALAN SUMBER MANUSIA	
B.5 TANGGUNGJAWAB SELEPAS PERTUKARAN ATAU PENAMATAN PERKHIDMATAN	
Objektif: Melindungi pihak berkepentingan Jabatan / Agensi Sektor Awam Negeri sebagai sebahagian proses pertukaran atau penamatan kakitangan atau kontrak.	
KENYATAAN	**TANGGUNGJAWAB**
B.5.1 TINDAKAN SELEPAS BERTUKAR ATAU TAMAT PERKHIDMATAN	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada pentadbiran Bahagian/Pusat semasa (sebelum berpindah) mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan pemprosesan maklumat mengikut peraturan yang ditetapkan oleh Jabatan / Agensi Sektor Awam Negeri dan/atau terma perkhidmatan.	Pentadbir Sistem ICT dan Semua Pengguna

BIDANG B KAWALAN SUMBER MANUSIA	
B.6 PERJANJIAN KERAHSIAAN MAKLUMAT	
Objektif: Mengekalkan kerahsiaan maklumat yang boleh dicapai oleh kakitangan dan pihak luaran/ketiga.	
KENYATAAN	**TANGGUNGJAWAB**
B.6.1 KEPERLUAN PERJANJIAN KERAHSIAAN MAKLUMAT	
Syarat-syarat dan terma perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan Jabatan / Agensi Sektor Awam Negeri dan hendaklah di semak dan di dokumentasi. Pembekal/pihak luaran/pihak ketiga hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan termasuk yang dinyatakan dalam **A.2.10 KEPERLUAN KESELAMATAN DENGAN PIHAK LUARAN/KETIGA.**	ICTSO dan Pentadbir Sistem ICT

BIDANG B KAWALAN SUMBER MANUSIA	
B.7 KERJA JARAK JAUH	
Objektif: Memastikan keselamatan maklumat bagi kakitangan yang bekerja jarak jauh.	
KENYATAAN	**TANGGUNGJAWAB**
B.7.1 KEPERLUAN PERJANJIAN KERAHSIAAN MAKLUMAT	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Capaian jarak jauh yang dimaksudkan merangkumi capaian daripada sistem rangkaian luar ke sistem rangkaian Jabatan / Agensi Sektor Awam Negeri; (b) Penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (*encryption*); (c) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan; (d) Lokasi bagi akses ke sistem ICT Jabatan / Agensi Sektor Awam Negeri hendaklah dipastikan selamat; (e) Penggunaan perkhidmatan menggunakan kaedah *Virtual Private Network* (VPN) yang disediakan oleh Jabatan / Agensi Sektor Awam Negeri hendaklah mendapat kebenaran daripada ICTSO. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini; dan (f) Kebenaran dari ICTSO adalah diperlukan bagi capaian jarak jauh oleh pihak pembekal dan perlu diteliti semula terutamanya yang melibatkan sistem-sistem kritikal. Perlu ada seliaan/pemantauan khas dari Jabatan / Agensi Sektor Awam Negeri apabila pembekal membuat capaian jarak jauh. Ia perlu mengambil kira lokasi asal capaian dan risiko-risiko serta ancaman kepada Jabatan / Agensi Sektor Awam Negeri.	ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Semua Pengguna

BIDANG B KAWALAN SUMBER MANUSIA	
B.8 PELAPORAN INSIDEN KESELAMATAN MAKLUMAT	
Objektif: Menyokong pelaporan bagi insiden keselamatan maklumat yang boleh dikenalpasti oleh kakitangan tepat pada masanya, konsisten dan berkesan.	
KENYATAAN	**TANGGUNGJAWAB**
B.8.1 KEPERLUAN PELAPORAN KEJADIAN KESELAMATAN MAKLUMAT	
Pengguna Jabatan / Agensi Sektor Awam Negeri dan pembekal yang menggunakan sistem dan perkhidmatan maklumat Jabatan / Agensi Sektor Awam Negeri dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat.	ICTSO, sgCSIRT dan Semua Pengguna

BIDANG C KAWALAN FIZIKAL	
C.1 PERIMETER KESELAMATAN FIZIKAL	
Objektif: Mencegah dari akses fizikal yang tidak sah, kerosakan dan gangguan terhadap maklumat dan aset ICT Jabatan / Agensi Sektor Awam Negeri.	
KENYATAAN	**TANGGUNGJAWAB**
C.1.1 KAWALAN PERIMETER KESELAMATAN FIZIKAL	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan dan pintu berkunci) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (c) Memasang alat penggera atau sistem pengawasan (contoh: CCTV) mengikut jenis/kategori yang bersesuaian untuk kawalan: (i) Kebakaran; (ii) Pencerobohan; (iii) Suhu; (iv) Banjir/hujan/kebocoran; (v) Kadar kelembapan; dan (vi) Pencemaran udara (dalam bangunan) (d) Mengehadkan jalan keluar masuk; (e) Mengadakan kaunter kawalan; (f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat;	CDO, ICTSO

(g) Mewujudkan perkhidmatan kawalan keselamatan; (h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan pengguna yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; (k) Memastikan butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; (l) Memastikan pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; dan (m) Memastikan lokasi premis ICT tidak berhampiran dengan kawasan pemunggahan dan laluan awam.	

BIDANG C KAWALAN FIZIKAL	
C.2 LALUAN MASUK FIZIKAL	
Objektif: Memastikan penggunaan laluan masuk fizikal kepada maklumat dan aset ICT Jabatan / Agensi Sektor Awam Negeri yang disahkan sahaja.	
KENYATAAN	**TANGGUNGJAWAB**
C.2.1 KAWALAN MASUK FIZIKAL	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Setiap pengguna Jabatan / Agensi Sektor Awam Negeri hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan semula kepada Jabatan / Agensi Sektor Awam Negeri apabila pengguna berhenti atau bersara; (c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di kaunter utama. Amalan ini juga perlu dipatuhi di semua pusat Jabatan / Agensi Sektor Awam Negeri. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (d) Kehilangan pas mestilah dilaporkan dengan segera.	Semua Pengguna
C.2.2 KAWASAN PENGHANTARAN DAN PEMUNGGAHAN	
Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Pengurus ICT dan Pentadbir Sistem ICT
C.2.3 KAWASAN LARANGAN	
Kawasan Larangan bermaksud mana-mana kawasan yang diisytiharkan sebagai Kawasan Larangan mengikut Seksyen 4 Akta Kawasan Larangan dan Tempat Larangan 1959 (Akta 298).	Pengurus ICT, Pentadbir Sistem ICT dan Semua Pengguna

Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	

BIDANG C **KAWALAN FIZIKAL**	
C.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN	
Objektif: Mencegah dari akses fizikal yang tidak sah, kerosakan dan gangguan terhadap maklumat dan aset ICT Jabatan / Agensi Sektor Awam Negeri di pejabat, bilik dan kemudahan.	
KENYATAAN	**TANGGUNGJAWAB**
C.3.1 KAWALAN KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawasan tempat kerja, bilik mesyuarat, bilik perbincangan, bilik fail, bilik kawalan CCTV, pusat data dan bilik *server* perlu dihadkan daripada diakses tanpa kebenaran; (b) Kawasan tempat kerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh pihak luar; (c) Petunjuk lokasi bilik operasi dan Kawasan larangan hendaklah mematuhi arahan keselamatan; dan (d) Fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk **KECUALI** dengan kebenaran CDO, ICTSO atau Pegawai Mengawal Pusat.	CDO, ICTSO, Pengurus ICT dan Pentadbir Sistem ICT
C.3.2 KESELAMATAN PUSAT DATA	
Pusat Data adalah lokasi yang menjadi tempat pengumpulan atau penyimpanan suatu jenis data.	Pengurus ICT dan Pentadbir Sistem ICT

Pusat Data menyimpan komputer/*server* untuk tujuan pengumpulan data dan menukarkannya kepada bentuk yang sesuai bagi kegunaan pengguna atau komputer lain. Pusat Data Kerajaan Negeri adalah di bawah kelolaan Bahagian Infrastruktur Pusat Data, JTDINS. Untuk memastikan semua *server* sentiasa selamat daripada pencerobohan atau sebarang ancaman dan membolehkan ia dicapai sepanjang masa, semua *server* hendaklah diletakkan di dalam Pusat Data yang mempunyai kemudahan keselamatan, penyaman udara khas dan kemudahan perlindungan suhu dan kebakaran. Pusat Data juga seharusnya dilengkapkan dengan ciri-ciri keselamatan lain seperti CCTV dan UPS. Berikut beberapa langkah untuk melindungi *server* tersebut: (a) Memantau dan mengawal keluar masuk pengguna ke pusat data melalui sistem *Security Access Door* atau berkunci dan CCTV; (b) Memastikan hanya pegawai-pegawai yang mempunyai kebenaran sahaja yang dibenarkan memasuki Pusat Data; (c) Semua akses yang dibenarkan ke kawasan persekitaran pusat data/bilik *server* hendaklah diiringi oleh Pentadbir Sistem atau kakitangan teknikal yang dilantik bagi menentukan dan mengawal selia penugasan yang diperlukan; (d) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; (e) Menyediakan buku log untuk tujuan merekodkan maklumat dan aktiviti yang dilaksanakan oleh Pentadbir Sistem ICT atau Pihak Ketiga;	

(f) Sebarang pemindahan maklumat daripada pusat data/bilik *server* hendaklah dipohon dan mendapat kebenaran daripada pemilik data (*data owne*r) dan Ketua Jabatan masing-masing; (g) Memastikan Pusat Data sentiasa bersih dan peralatan ICT tidak terdedah kepada habuk; (h) Memastikan penyaman udara berfungsi dengan baik dan suhunya adalah bersesuaian dengan Pusat Data; (i) Memastikan semua peralatan keselamatan, UPS dan penyaman udara mestilah diselenggarakan secara berkala; (j) Memastikan Pusat Data juga dilengkapi dengan Sistem Pencegahan dan Penggera Kebakaran yang diselenggara secara berkala; dan (k) Memastikan tiada sebarang foto dan video diambil di Pusat Data.	
C.3.3 KESELAMATAN BILIK SERVER DAN RAK RANGKAIAN	
Bilik *Server* adalah bilik yang menempatkan *server* dan peralatan rangkaian serta keselamatan dengan skala dan saiz yang lebih kecil dari Pusat Data. Rak rangkaian (mengandungi peralatan rangkaian) sama ada *wall standing* atau *wall mounted* (digantung). Diantara beberapa langkah keselamatan yang perlu diambil termasuk: (a) Memastikan sistem penyaman udara untuk perlindungan suhu disediakan dalam Bilik *Server*/Rangkaian berkenaan. Bagi bilik yang memuatkan peralatan rangkaian *wall mounted* perlu mempunyai kitar pengudaraan yang bersesuaian;	Pengurus ICT dan Pentadbir Sistem ICT

(b) Memastikan sistem pencegahan kebakaran disediakan di bangunan yang mana Bilik *Server* ditempatkan; (c) Memastikan keperluan UPS sekurang-kurangnya mampu melindungi *Server* dan peralatan rangkaian yang utama; (d) Memantau dan mengawal keluar masuk pengguna ke Bilik *Server* dengan menyediakan Buku Log Pelawat; (e) Memastikan hanya pegawai-pegawai yang mempunyai kebenaran sahaja yang dibenarkan memasuki Bilik *Server;* (f) Memastikan Bilik *Server* sentiasa bersih dan peralatan ICT tidak terdedah kepada habuk; (g) Memastikan penyaman udara mestilah berfungsi dengan baik, di mana suhunya adalah bersesuaian dengan Bilik *Server;* (h) Memastikan semua peralatan diselenggarakan secara berkala; (i) Memastikan rak peralatan *server* dan rangkaian tidak diletakkan di bawah penyaman udara, kotak suis agihan (DB) elektrik, tingkap atau ruang-ruang terbuka pada persekitaran luar; (j) Memastikan tiada sebarang peralatan luar diletakkan di bawah rak *wall mounted* bagi memastikan rak tersebut boleh dicapai pada bila-bila masa; (k) Memastikan setiap rak peralatan *server* dan rangkaian dikunci dan kunci disimpan di tempat yang selamat; dan (l) Mempunyai sistem pencegahan kebakaran yang sewajarnya dan bersesuaian.	

BIDANG C KAWALAN FIZIKAL	
C.4 PEMANTAUAN KESELAMATAN FIZIKAL	
Objektif: Mengesan dan menghalang akses fizikal yang tidak sah.	
KENYATAAN	**TANGGUNGJAWAB**
C.4.1 KAWALAN PEMANTAUAN KESELAMATAN FIZIKAL	
Premis fizikal perlu dipantau menggunakan sistem pengawasan (contoh: pengawal, penggera pencerobohan, sistem pemantauan video seperti CCTV, sistem aplikasi pengurusan maklumat keselamatan fizikal atau mana-mana yang bersesuaian). Akses ke lokasi kritikal perlu dipantau secara berterusan bagi mengesan akses yang tidak sah atau tingkah laku yang mencurigakan.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

BIDANG C KAWALAN FIZIKAL	
C.5 PERLINDUNGAN DARIPADA ANCAMAN FIZIKAL DAN PERSEKITARAN	
Objektif: Mencegah atau mengurangkan kesan dari kejadian yang berpunca dari ancaman fizikal dan persekitaran.	
KENYATAAN	**TANGGUNGJAWAB**
C.5.1 KEPERLUAN PERLINDUNGAN DARIPADA ANCAMAN FIZIKAL DAN PERSEKITARAN	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada pihak Jabatan/Agensi/Bahagian yang berkenaan. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: (a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

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

BIDANG C KAWALAN FIZIKAL	
C.6 BEKERJA DI KAWASAN SELAMAT	
Objektif: Mencegah maklumat dan aset ICT di dalam kawasan yang selamat dari kerosakan dan gangguan oleh kakitangan yang tidak sah yang bekerja di kawasan tersebut.	
KENYATAAN	**TANGGUNGJAWAB**
C.6.1 BEKERJA DI KAWASAN SELAMAT	
Menyediakan prosedur dan garis panduan untuk keperluan bekerja di dalam kawasan yang dihadkan kepada pihak tertentu sahaja. Perkara-perkara berikut hendaklah dipatuhi: (a) Akses ke kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan (b) Pembekal adalah dilarang untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Semua Pengguna

BIDANG C KAWALAN FIZIKAL	
C.7 CLEAR DESK DAN CLEAR SCREEN	
Objektif: Mengurangkan risiko capaian tidak sah, kehilangan dan kerosakan kepada maklumat di meja, skrin dan mana mana lokasi yang boleh dimasuki sewaktu dan selepas waktu bekerja.	
KENYATAAN	**TANGGUNGJAWAB**
C.7.1 KAWALAN CLEAR DESK DAN CLEAR SCREEN	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau logout apabila meninggalkan komputer ; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Semua Pengguna

BIDANG C KAWALAN FIZIKAL	
C.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN	
Objektif: Mengurangkan risiko dari ancaman fizikal dan persekitaran serta dari akses tidak sah dan kerosakan.	
KENYATAAN	**TANGGUNGJAWAB**
C.8.1 PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (b) Pengguna bertanggungjawab sepenuhnya ke atas peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran peralatan dan konfigurasi yang telah ditetapkan; (c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang peralatan ICT yang telah ditetapkan; (d) Pengguna tidak dibenarkan mengubah kedudukan peralatan ICT dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT; (e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (f) 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; (g) Setiap komputer yang mempunyai akses LAN perlu *Join Domain* untuk membolehkan akaun	Pengurus ICT, Pentadbir Sistem ICT dan Semua Pengguna

pada *Active Directory* Jabatan / Agensi Sektor Awam Negeri digunakan sebagai log masuk manakala komputer *standalone*, penggunaan kata laluan adalah diwajibkan; (h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; (i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); (j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; (k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan/atau mempunyai pengudaraan (*air ventilation*) yang sesuai; (l) Pengendalian bagi peralatan ICT yang hilang hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa dari semasa ke semasa; (m) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa; (n) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih; (o) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;	

(p) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem ICT; (q) Pengguna bertanggungjawab terhadap peralatan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (r) Pengguna hendaklah memastikan semua peralatan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; (s) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; (t) Memastikan plug dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan peralatan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya; dan (u) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik.	

BIDANG C KAWALAN FIZIKAL	
C.9 KESELAMATAN ASET DI LUAR PREMIS	
Objektif: Mencegah peralatan di luar premis dari hilang, rosak dan dikompromi dan gangguan kepada operasi Jabatan / Agensi Sektor Awam Negeri.	
KENYATAAN	**TANGGUNGJAWAB**
C.9.1 KESELAMATAN PERALATAN DAN ASET DI LUAR PREMIS	
Peralatan yang dibawa keluar dari premis Jabatan / Agensi Sektor Awam Negeri adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; (c) Sebarang sambungan ke rangkaian dan Internet di tempat awam perlu mengambil kira faktor keselamatan rangkaian terutamanya melibatkan urusan kerja rasmi; (d) Peralatan perlu dipastikan tidak digunakan oleh mana-mana pihak ketiga; (e) Pergerakan peralatan perlu melalui prosedur yang ditetapkan berserta borang yang berkaitan dan direkodkan bagi tujuan pemantauan; dan (f) Sebarang laporan kehilangan peralatan hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa dari semasa ke semasa.	Pengurus ICT, Pentadbir Sistem ICT dan Semua Pengguna

BIDANG C KAWALAN FIZIKAL	
C.10 MEDIA STORAN	
Objektif: Memastikan pendedahan, pengubahsuaian, penghapusan dan pemusnahan yang sah pada media storan.	
KENYATAAN	**TANGGUNGJAWAB**
C.10.1 PENGURUSAN MEDIA MUDAH ALIH	
Media mudah alih merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat dan media storan yang boleh alih. Peraturan yang perlu dipatuhi dalam pengurusan media mudah alih adalah berdasarkan Arahan Keselamatan seperti berikut: (a) Menyimpan media mudah alih dalam bekas penyimpanan yang selamat dan dibenarkan; (b) Memastikan capaian untuk memasuki kawasan penyimpanan media mudah alih hendaklah terhad kepada Pentadbir dan pegawai yang dibenarkan sahaja; (c) Mengawal media mudah alih bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Menyimpan media mudah alih yang mengandungi data rahsia rasmi di dalam bekas keselamatan yang mempunyai ciri-ciri keselamatan; (e) Memastikan capaian dan pergerakan media mudah alih direkodkan; (f) Meletakkan peralatan *backup* bagi media mudah alih di tempat yang terkawal; (g) Mengadakan salinan atau pendua pada media mudah alih bagi tujuan keselamatan dan bagi mengelakkan kehilangan data;	Semua Pengguna

(h) Menyimpan maklumat rasmi sahaja dalam media mudah alih yang dibekalkan oleh Jabatan / Agensi Sektor Awam Negeri; dan (i) Lesen perisian (*registration code, serials, CD-keys*) perlu direkod dengan tepat dan disimpan berasingan daripada disk atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak.	
C.10.2 PELUPUSAN MEDIA	
Pelupusan media mudah alih perlu mendapat kelulusan dan mengikut prosedur Jabatan / Agensi Sektor Awam Negeri yang berkenaan. Peraturan yang perlu dipatuhi dalam pelupusan media adalah seperti berikut: (a) Memastikan media mudah alih yang mengandungi maklumat rahsia rasmi yang hendak dihapuskan atau dimusnahkan dilupuskan mengikut Pekeliling Pengurusan Aset Alih Jabatan / Agensi Sektor Awam Negeri dan peraturan yang berkuat kuasa berkaitan sanitasi media; (b) Memastikan media mudah alih yang hendak dilupuskan yang mengandungi data rahsia rasmi/sensitif dihapuskan (*wipe data*) dengan teratur dan selamat; (c) Melaksanakan pelupusan media mudah alih dalam aset ICT mengikut Pekeliling Pengurusan Aset Alih Jabatan / Agensi Sektor Awam Negeri yang berkuat kuasa; dan (d) Memberi makluman kepada pemilik maklumat terlebih dahulu sebelum menghapuskan maklumat atau kandungan media mudah alih.	Semua Pengguna
C.10.3 PENGHANTARAN DAN PEMINDAHAN MEDIA	
Peraturan yang perlu dipatuhi dalam penghantaran dan pemindahan media adalah berdasarkan Arahan Keselamatan dengan mematuhi perkara berikut:	ICTSO dan Semua Pengguna

(a) Memastikan penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik data terlebih dahulu dengan menandatangani Surat Perakuan Pelan Keselamatan Siber di Lampiran 2 dan perakuan Akta Rahsia Rasmi seperti di Lampiran 3; (b) Memastikan penghantaran atau pemindahan media yang mengandungi maklumat rahsia rasmi ke luar pejabat hendaklah mendapatkan kebenaran daripada ICTSO terlebih dahulu; (c) Memastikan penghantaran atau pemindahan media ke luar pejabat mempunyai rekod; (d) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; dan (e) Mengehadkan peredaran data atau media untuk tujuan yang dibenarkan sahaja.	
C.10.4 PENGALIHAN ASET	
Aset ICT seperti peralatan, perisian dan maklumat tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Bagi peralatan ICT yang dipinjam perlulah mengikut prosedur berikut: (a) Memastikan maklumat peminjam dan peralatan dipinjam direkodkan ketika peminjaman dan pemulangan dibuat; (b) Memastikan tempoh pinjaman dihadkan kepada tempoh masa yang dipersetujui; (c) Melaporkan sebarang kerosakan dan kegagalan peralatan berfungsi dengan baik kepada *Helpdesk*/Pentadbir Sistem ICT dengan kadar segera; dan (d) Sebarang laporan kehilangan peralatan pinjaman hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa dari semasa ke semasa.	Pegawai Mengawal Pusat, Pegawai aset, Pentadbir Sistem ICT dan Semua Pengguna

Peralatan ICT yang hendak dibawa keluar dari premis Jabatan / Agensi Sektor Awam Negeri, perlulah mendapat kelulusan Pegawai Mengawal Pusat (PMP)/Pegawai Aset atau Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan.	

BIDANG C KAWALAN FIZIKAL	
C.11 UTILITI SOKONGAN	
Objektif: Mencegah maklumat dan aset ICT dari hilang, rosak dan dikompromi atau gangguan kepada operasi Jabatan / Agensi Sektor Awam Negeri akibat dari kegagalan dan gangguan utiliti sokongan.	
KENYATAAN	**TANGGUNGJAWAB**
C.11.1 KAWALAN UTILITI SOKONGAN	
Peralatan ICT perlu dilindungi daripada kegagalan bekalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; (b) Peralatan sokongan seperti *Uninterruptible Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data/Bilik *Server* supaya mendapat bekalan kuasa berterusan; (c) Perancangan untuk keperluan bekalan kuasa untuk semua peralatan hendaklah dibuat sebelum perolehan bagi memastikan bekalan kuasa mencukupi untuk operasi; dan (d) Kesemua utiliti sokongan perlu diselenggara secara berkala.	Pengurus ICT, Pentadbir Sistem ICT dan Semua Pengguna

BIDANG C KAWALAN FIZIKAL	
C.12 KESELAMATAN KABEL	
Objektif: Mencegah maklumat dan aset ICT dari hilang, rosak dan dikompromi atau gangguan kepada operasi Jabatan / Agensi Sektor Awam Negeri berkaitan dengan punca kuasa dan kabel komunikasi.	
KENYATAAN	**TANGGUNGJAWAB**
C.12.1 KESELAMATAN KABEL	
Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: (a) Memastikan hanya pengguna Jabatan / Agensi Sektor Awam Negeri atau pihak ketiga yang dibenarkan boleh melaksanakan pemasangan atau penyelenggaraan kabel; (b) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (c) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (d) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wiretapping*; dan (e) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Pengurus ICT, Pentadbir Sistem ICT dan Semua Pengguna

BIDANG C KAWALAN FIZIKAL	
C.13 PENYELENGGARAAN PERALATAN	
Objektif: Mencegah maklumat dan aset ICT dari hilang, rosak dan dikompromi atau gangguan kepada operasi Jabatan / Agensi Sektor Awam Negeri berpunca dari kekurangan penyelenggaran.	
KENYATAAN	**TANGGUNGJAWAB**
C.13.1 KAWALAN PENYELENGGARAAN PERALATAN	
Peralatan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan; (b) Memastikan peralatan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap peralatan bagi penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; (f) Penyelenggaraan peralatan oleh pembekal perlu dilakukan secara *on-site* dengan pengawasan oleh pihak yang berkenaan. *Remote access* oleh pihak luaran/ketiga dan pembekal hanyalah dengan kebenaran daripada ICTSO; dan (g) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT dan dimaklumkan kepada Pemilik Sistem.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

BIDANG C KAWALAN FIZIKAL	
C.14 PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN	
Objektif: Mencegah ketirisan maklumat dari peralatan yang perlu dilupuskan atau diguna semula.	
KENYATAAN	**TANGGUNGJAWAB**
C.14.1 PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh Jabatan / Agensi Sektor Awam Negeri dan ditempatkan di Jabatan / Agensi Sektor Awam Negeri. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Jabatan / Agensi Sektor Awam Negeri. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- (a) Semua pemusnahan peralatan khususnya yang mengandungi maklumat rahsia rasmi hendaklah mengikut peraturan yang ditetapkan oleh Kerajaan sepertimana yang disebutkan dalam Arahan Keselamatan. Prosedur pemusnahan tersebut boleh merujuk kepada Tatacara dan Garis Panduan pelupusan dan sanitasi yang digunapakai; (b) Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; (c) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (d) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;	Pegawai Aset, Pengurus ICT, Pentadbir Sistem ICT dan Semua Pengguna

(e) Pegawai aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Harta Jabatan / Agensi Sektor Awam Negeri; (f) Pelupusan peralatan ICT hendaklah dilakukan mengikut tatacara pelupusan semasa yang berkuat kuasa; (g) Peralatan ICT yang dihapus kira hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara selamat; dan (h) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara perkara seperti berikut: (i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan peralatan tambahan dalaman *CPU* seperti *RAM*, *hardisk*, *motherboard* dan sebagainya; (ii) Menyimpan dan memindahkan peralatan luaran komputer seperti *AVR*, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di Jabatan / Agensi Sektor Awam Negeri; (iii) Memindah keluar dari Jabatan / Agensi Sektor Awam Negeri mana-mana peralatan ICT yang hendak dilupuskan; (iv) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Jabatan / Agensi Sektor Awam Negeri; dan (v) Pengguna ICT bertanggungjawab memastikan segala maklumat rahsia rasmi di dalam komputer disalin pada media storan kedua sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	

BIDANG D KAWALAN TEKNOLOGI	
D.1 PERALATAN PENGGUNA	
Objektif: Melindungi maklumat daripada risiko yang didapati dari penggunaan peralatan oleh pengguna.	
KENYATAAN	**TANGGUNGJAWAB**
D.1.1 PERALATAN MUDAH ALIH	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan mudah alih yang dibekalkan oleh Jabatan / Agensi Sektor Awam Negeri seperti telefon pintar, tablet dan yang seumpamanya hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; (b) Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih; (c) Ketika menggunakan rangkaian komputer awam (*public wi-fi*), capaian kepada dokumen mengandungi maklumat rahsia rasmi hendaklah dihadkan. Sekiranya masih ada keperluan untuk berbuat demikian, maka langkah-langkah keselamatan hendaklah diambil supaya maklumat tersebut tidak boleh dilihat oleh pihak yang tidak berkenaan; (d) Peralatan mudah alih hendaklah dilengkapkan dengan sistem pengoperasian dan perisian antivirus yang diselenggarakan dengan baik; (e) Maklumat rahsia rasmi tidak dibenarkan untuk disimpan di dalam peralatan mudah alih. Pengendalian Rahsia Rasmi dalam persekitaran ICT perlu mengikut Arahan Keselamatan; dan (f) Proses *backup* perlu dilaksanakan bagi menjamin keselamatan data.	CDO, ICTSO, Pentadbir Sistem ICT dan Semua Pengguna

D.1.2 BRING YOUR OWN DEVICE (BYOD)	
Pengguna BYOD perlu mematuhi tatacara penggunaan BYOD: (a) Memastikan keselamatan maklumat semasa menggunakan peralatan BYOD; (b) Dilarang memasang perisian yang tidak dibenarkan untuk melaksanakan tugasan rasmi Jabatan / Agensi Sektor Awam Negeri; (c) Dilarang memasang perisian yang mengganggu sistem rangkaian Jabatan / Agensi Sektor Awam Negeri; (d) Mengaktifkan fungsi keselamatan kata laluan di setiap komputer riba/peranti. Sekiranya *Active Directory* wujud, komputer berkenaan perlu sambung ke *Domain Server;* (e) Peralatan BYOD hendaklah dilindungi oleh perisian *Endpoint Security* bagi mengelak penyebaran virus/malware/trojan dan lain-lain ke atas pengguna Jabatan / Agensi Sektor Awam Negeri yang lain; (f) Memastikan peranti yang digunakan menggunakan teknologi penyulitan (*encryption*), tandatangan digital atau sebarang mekanisme bagi melindungi maklumat elektronik semasa ianya digunakan; (g) Dilarang menyalin dan membawa keluar maklumat organisasi dengan menggunakan peranti mudah alih dan media storan seperti *external hardisk* dan sebagainya tanpa kebenaran; (h) Memadam dokumen elektronik dengan merincih secara elektronik/'*secure deletion*' selepas dokumen tidak lagi digunapakai; (i) Dilarang meninggalkan komputer riba/peranti di ruang pejabat yang terbuka tanpa menguncikannya;	Semua Pengguna

(j) Peralatan BYOD yang membuat sambungan ke rangkaian Jabatan / Agensi Sektor Awam Negeri adalah tidak dibenarkan membuat capaian menggunakan proksi luar, VPN atau yang seumpama dengannya; (k) Mengaktifkan fungsi *screen saver* secara automatik apabila peralatan BYOD tidak digunakan; (l) Dilarang menjadikan peralatan BYOD sebagai *access point* kepada aset ICT Jabatan / Agensi Sektor Awam Negeri untuk capaian ke Internet tanpa kebenaran; (m) Memadamkan segala maklumat yang berkaitan dengan urusan rasmi jabatan sekiranya bertukar/ditamatkan perkhidmatan/bersara atau sewaktu dihantar ke pusat servis luar untuk penyelenggaraan; dan (n) Membenarkan pihak Jabatan / Agensi Sektor Awam Negeri untuk membuat semakan bagi tujuan pengauditan, semakan atau analisis risiko ke atas peralatan BYOD yang digunakan.	
D.1.3 PERALATAN PENGGUNA YANG TIADA PENGAWASAN	
Peralatan yang tiada pengawasan perlu dilindungi dengan cara berikut: (a) Menamatkan sesi penggunaan selepas digunakan; (b) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; dan (c) Memastikan peralatan tidak digunakan oleh pihak yang tidak berkaitan.	Semua Pengguna

BIDANG D KAWALAN TEKNOLOGI	
D.2 HAK CAPAIAN ISTIMEWA	
Objektif: Memastikan pengguna, komponen perisian dan perkhidmatan yang sah sahaja diberi hak capaian istimewa.	
KENYATAAN	**TANGGUNGJAWAB**
D.2.1 PENGURUSAN HAK CAPAIAN ISTIMEWA	
Peruntukan dan penggunaan hak capaian istimewa hendaklah dikenalpasti, dihadkan, dikawal dan diselia berdasarkan keperluan skop tugas merujuk kepada Prosedur Pendaftaran dan Penamatan Pengguna. Identiti bagi hak capaian istimewa digunakan hanya untuk kerja-kerja pentadbiran dan bukan tugasan seharian seperti menyemak e-mel dan capaian Internet.	ICTSO, Pemilik Sistem dan Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.3 SEKATAN CAPAIAN MAKLUMAT	
Objektif: Memastikan hanya capaian sah dan mengelakkan capaian tidak sah kepada maklumat dan aset ICT.	
KENYATAAN	**TANGGUNGJAWAB**
D.3.1 SEKATAN CAPAIAN MAKLUMAT	
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 keselamatan maklumat yang telah ditentukan; (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log/jejak audit); (c) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; (d) Capaian sistem maklumat dan aplikasi melalui jarak jauh hanya dibenarkan mengikut keperluan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; (e) Mengehadkan capaian sistem dan aplikasi kepada lima kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; (f) Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; (g) Maklumat tarikh *login* terakhir hendaklah dipamerkan; dan (h) *Session timeout* hendaklah dilaksanakan.	ICTSO dan Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.4 CAPAIAN KEPADA KOD SUMBER	
Objektif: Mengelakkan kemunculan fungsian yang tidak sah, mengelakkan perubahan yang tidak sengaja atau berniat jahat dan mengekalkan kerahsiaan harta intelek yang berharga.	
KENYATAAN	**TANGGUNGJAWAB**
D.4.1 KAWALAN CAPAIAN KEPADA KOD SUMBER PROGRAM	
Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Pegawai yang bertanggungjawab perlu memastikan kod sumber versi terkini disimpan sebagai backup ditempat yang selamat; (b) Pegawai yang bertanggungjawab perlu memastikan kod sumber yang disimpan adalah bukan *object code*; (c) *Log audit* perlu dibuat ke atas capaian kod sumber; (d) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan (e) Kod sumber bagi semua aplikasi yang dibangunkan hendaklah menjadi hak milik Jabatan / Agensi Sektor Awam Negeri.	Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.5 PENGESAHAN RAHSIA	
Objektif: Memastikan pengguna atau entiti telah disahkan selamat, apabila membuat capaian sistem aplikasi dan perkhidmatan yang dibenarkan.	
KENYATAAN	**TANGGUNGJAWAB**
D.5.1 PROSEDUR LOG MASUK YANG SELAMAT	
Kawalan log masuk yang selamat perlu mengambil kira perkara berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Mengehadkan dan mengawal penggunaan program; (d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi; dan (e) Memastikan sistem pengurusan kata laluan secara interaktif dan kata laluan adalah berkualiti.	ICTSO dan Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.6 PENGURUSAN KAPASITI	
Objektif: Memastikan kapasiti yang diperlukan oleh kemudahan pemprosesan maklumat, sumber manusia, pejabat dan kemudahan lain.	
KENYATAAN	**TANGGUNGJAWAB**
D.6.1 PENGURUSAN KAPASITI PEMPROSESAN MAKLUMAT	
Perkara-perkara berikut perlu diambil kira dalam pengurusan kapasiti: (a) Kapasiti suatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan (b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan maklumat bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	ICTSO dan Pentadbir Sistem ICT
D.6.2 PENGURUSAN KAPASITI SUMBER MANUSIA, PEJABAT DAN KEMUDAHAN LAIN	
Melaksanakan pengurusan kapasiti sumber manusia, pejabat dan kemudahan lain dengan mendapatkan kakitangan serta kemudahan dan ruang baharu/tambahan mengikut kesesuaian.	Pegawai Mengawal Pusat

BIDANG D KAWALAN TEKNOLOGI	
D.7 PERLINDUNGAN DARIPADA *MALWARE*	
Objektif: Memastikan maklumat dan aset ICT dilindungi dari *malware*.	
KENYATAAN	**TANGGUNGJAWAB**
D.7.1 KAWALAN DARIPADA *MALWARE*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program *malware* seperti *endpoint*, Intrusion *Detection System* (*IDS*) dan *Intrusion Prevention System* (*IPS*) serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; (c) Mengimbas semua perisian atau sistem dengan *endpoint* sebelum menggunakannya; (d) Mengemaskini *endpoint* dengan pattern/signature *endpoint* yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri sesi kesedaran mengenai ancaman *malware* dan cara mengendalikannya; (g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;	ICTSO, Pegawai Mengawal Pusat, Pentadbir Sistem ICT dan Semua Pengguna

(h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; (i) Memberi amaran mengenai ancaman keselamatan maklumat seperti serangan *malware*; (j) Memastikan setiap pemasangan perisian yang bukan standard Jabatan / Agensi Sektor Awam Negeri telah mendapat kelulusan ICTSO dengan sokongan Pegawai Mengawal Pusat dan direkodkan; dan (k) Penggunaan mobile code terutamanya dari Internet dan emel seperti *JavaScript*, *VBScript* dan *ActiveX Controls*, yang boleh mendatangkan ancaman keselamatan siber adalah tidak dibenarkan.	

BIDANG D KAWALAN TEKNOLOGI	
D.8 PENGURUSAN KERENTANAN (*VULNERABILITIES*) TEKNIKAL	
Objektif: Mencegah eksploitasi dari kerentanan (*vulnerabilities*) teknikal.	
KENYATAAN	**TANGGUNGJAWAB**
D.8.1 KAWALAN PENGURUSAN MENGURUSKAN KERENTANAN (*VULNERABILITIES*) TEKNIKAL	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memperoleh maklumat kerentanan (*vulnerabilities*) teknikal yang tepat pada masanya ke atas sistem maklumat yang digunakan. Diantara kaedah yang digunakan termasuklah pelaksanaan *Security Penetration Assessment*, *Vulnerability Test* atau maklumat umum kerentanan. Sebagai contoh ialah *Common Vulnerabilities and Exposures* (*CVE*); (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi;dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan ancaman keselamatan siber adalah tidak dibenarkan.	ICTSO dan Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.9 PENGURUSAN KONFIGURASI	
Objektif: Memastikan peralatan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul dengan aturan keselamatan yang diperlukan dan konfigurasi tidak diubah oleh perubahan yang tidak sah dan tidak betul.	
KENYATAAN	**TANGGUNGJAWAB**
D.9.1 KAWALAN PENGURUSAN KONFIGURASI	
Perkara yang perlu dipatuhi termasuk mewujudkan, mendokumentasi, melaksana, memantau dan mengkaji semula konfigurasi keselamatan bagi peralatan, perisian, perkhidmatan dan rangkaian.	ICTSO dan Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.10 PENGHAPUSAN MAKLUMAT	
Objektif: Mencegah pendedahan maklumat sensitif yang tidak sewajarnya dan mematuhi undang-undang, peraturan dan keperluan kontrak dalam penghapusan maklumat.	
KENYATAAN	**TANGGUNGJAWAB**
D.10.1 KAWALAN PENGHAPUSAN MAKLUMAT	
Maklumat yang disimpan di dalam sistem informasi, peralatan dan mana-mana storan media perlu dihapuskan apabila tidak diperlukan. Kaedah penghapusan secara *secure deletion*. Kawalan **C.14.1 PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN** boleh digunakan bagi pemusnahan secara fizikal disamping menghapuskan maklumat yang terkandung di dalamnya.	Pentadbir Sistem ICT dan Semua Pengguna.

BIDANG D KAWALAN TEKNOLOGI	
D.11 *DATA MASKING*	
Objektif: Mengehadkan pendedahan maklumat sensitif termasuk *PII* dan mematuhi undang-undang, peraturan dan keperluan kontrak.	
KENYATAAN	**TANGGUNGJAWAB**
D.11.1 KAWALAN *DATA MASKING*	
Data Masking perlu digunakan selaras dengan polisi tajuk khusus dalam kawalan capaian dan polisi tajuk khusus lain yang berkaitan serta keperluan perkhidmatan dengan mengambil kira pertimbangan undang-undang.	Pentadbir Sistem ICT dan Semua Pengguna.

BIDANG D KAWALAN TEKNOLOGI	
D.12 PERLINDUNGAN KETIRISAN DATA	
Objektif: Mengesan dan mencegah pendedahan yang tidak sah dan maklumat yang diambil oleh individu atau sistem.	
KENYATAAN	**TANGGUNGJAWAB**
D.12.1 PERLINDUNGAN KETIRISAN DATA	
Langkah-langkah perlindungan ketirisan data perlu diguna pakai untuk sistem, rangkaian dan peralatan yang melakukan proses, menyimpan dan menghantar maklumat sensitif.	Pentadbir Sistem ICT dan Semua Pengguna.

BIDANG D KAWALAN TEKNOLOGI	
D.13 *BACKUP* MAKLUMAT	
Objektif: Membolehkan salinan maklumat, perisian dan sistem diselenggara dan diuji secara berkala berdasarkan polisi tajuk khusus berkaitan *backup*.	
KENYATAAN	**TANGGUNGJAWAB**
D.13.1 KAWALAN *BACKUP* MAKLUMAT	
Bagi memastikan kesinambungan penyampaian perkhidmatan, perkara perkara seperti berikut hendaklah dipatuhi dan dipantau untuk memenuhi keperluan perlindungan data digital dan sistem aplikasi ICT Kerajaan Negeri yang terkandung dalam Surat Pekeliling Kementerian Kewangan Bil. 12 Tahun 2008 bertajuk “Dasar Perolehan dan Pelaksanaan Sistem Aplikasi ICT, serta Penyimpanan Data dan Sistem Aplikasi ICT Ke Pusat Data Kerajaan Negeri” bertarikh 30 Disember 2008. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua sistem aplikasi ICT yang dibangunkan dan digunapakai oleh semua Kementerian/Jabatan/Pihak Berkuasa Tempatan/Badan Berkanun di bawah Kerajaan Negeri hendaklah disimpan dan ditempatkan di Pusat Data Kerajaan Negeri; (b) Sebarang sistem aplikasi ICT yang dicapai melalui sistem rangkaian Sabah Net oleh Ibu Pejabat dan Cawangan Agensi di seluruh negeri hendaklah disimpan dan ditempatkan di Pusat Data Kerajaan Negeri; (c) Menyimpan semua salinan data digital Jabatan/Agensi di Pusat Data Kerajaan Negeri sebagai tempat penyimpanan data secara *offsite*; (d) Menyerahkan dua (2) salinan untuk simpanan sokongan penuh data mingguan (*Weekly Full data backup*) dan sokongan penuh sistem mingguan	ICTSO, Pentadbir Sistem ICT dan Semua Pengguna.

(*Weekly Full system backup*) kepada Pusat Data Kerajaan Negeri; (e) Melaksanakan prosedur *backup* mengikut amalan terbaik industri dan piawaian keselamatan ICT semasa bagi memastikan kelangsungan data yang optimum; (f) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi setelah mendapat versi terbaru; (g) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat; (h) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu; dan (i) Menyimpan sekurang-kurangnya tiga generasi *backup*.	

BIDANG D KAWALAN TEKNOLOGI	
D.14 *REDUNDANCY* PADA KEMUDAHAN PEMPROSESAN MAKLUMAT	
Objektif: Memastikan operasi berterusan pada kemudahan pemprosesan maklumat.	
KENYATAAN	**TANGGUNGJAWAB**
D.14.1 KETERSEDIAAN KEMUDAHAN PEMPROSESAN MAKLUMAT	
Kemudahan pemprosesan maklumat perlu mempunyai *redundancy* yang mencukupi untuk memenuhi keperluan ketersediaan. Ia perlu diuji *(failover*) keberkesanannya dari semasa ke semasa.	ICTSO, Pentadbir Sistem ICT dan Pemilik Sistem.

BIDANG D KAWALAN TEKNOLOGI	
D.15 *LOGGING*	
Objektif: Merekod kejadian, menjana pembuktian, memastikan integriti maklumat log, mencegah capaian tidak sah, mengenal pasti kejadian keselamatan maklumat yang membawa kepada insiden keselamatan maklumat dan menyokong penyiasatan.	
KENYATAAN	**TANGGUNGJAWAB**
D.15.1 EVENT LOGGING	
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat, pencerobohan, perubahan yang tidak dibenarkan dalam	Pentadbir Sistem ICT

sistem/infrastruktur. Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO; dan (d) Fail log hendaklah disimpan untuk tempoh sekurang-kurangnya enam bulan. Jenis fail log bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti berikut: (i) Fail log sistem pengoperasian; (ii) Fail log servis (contoh: web, e-mel); (iii) Fail log aplikasi (jejak audit); dan (iv) Fail log rangkaian (contoh: switch, firewall, IPS) Setiap sistem aplikasi mestilah mempunyai jejak audit (*audit trail*). Jejak audit ini merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu peristiwa (*event*). 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; dan (e) Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal.	

D.15.2 PERLINDUNGAN MAKLUMAT LOG	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; (b) Kemudahan merekod dan maklumat log perlu dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan; dan (c) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya.	Pentadbir Sistem ICT
D.15.3 LOG PENTADBIR DAN OPERATOR	
Aktiviti pentadbiran dan operator sistem perlu direkodkan dan dipantau secara kerap.	Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.16 AKTIVITI PEMANTAUAN	
Objektif: Mengesan tingkah laku anomali dan potensi kepada insiden keselamatan maklumat.	
KENYATAAN	**TANGGUNGJAWAB**
D.16.1 PEMANTAUAN BERTERUSAN	
Pemantauan kepada rangkaian, sistem dan aplikasi perlu dilaksanakan secara berterusan mengikut tempoh yang bersesuaian. Perkara-perkara yang memerlukan pemantauan termasuklah tetapi tidak terhad kepada: (a) Trafik keluar masuk rangkaian, sistem dan aplikasi; (b) Capaian kepada sistem, server, perkakasan rangkaian, sistem pemantauan, sistem aplikasi yang kritikal dan lain-lain; (c) Tahap pentadbir sistem dan fail konfigurasi rangkaian; (d) Log dari peralatan/perisian keselamatan (contoh: *Antivirus*, *IDS*, *IPS*, *firewall* dan lain-lain); (e) Log kejadian berkaitan aktiviti sistem dan rangkaian; (f) Penggunaan kod yang disahkan tidak disalah guna; dan (g) Penggunaan sumber (contoh: *CPU*, *hard disks*, *memory* dan *bandwidth*).	Pentadbir Sistem ICT
D.16.2 SEMAKAN DAN FORENSIK ICT	
ICTSO mestilah bertanggungjawab menyemak, merekod dan menganalisis perkara perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT Jabatan / Agensi Sektor Awam Negeri;	ICTSO, Pentadbir Sistem ICT

(b) Aktiviti yang boleh menjadi punca serangan *malicious code*; (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesuatu sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan *bandwidth* rangkaian; (g) Aktiviti penyalahgunaan akaun e-mel; (h) Aktiviti penukaran alamat IP (*IP address*) dan segmen IP selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT; dan (i) Sebarang aktiviti yang menyebabkan terdapat keperluan untuk semakan dan forensik ICT dijalankan di bawah arahan CDO dan ICTSO.	

BIDANG D KAWALAN TEKNOLOGI	
D.17 PENYERAGAMAN WAKTU	
Objektif: Membolehkan korelasi dan analisis kejadian berkaitan keselamatan dan lain-lain data yang direkodkan dan untuk menyokong siasatan kepada insiden keselamatan maklumat.	
KENYATAAN	**TANGGUNGJAWAB**
D.17.1 KEPERLUAN PENYERAGAMAN WAKTU	
Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Jabatan / Agensi Sektor Awam Negeri atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.18 PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA	
Objektif: Memastikan penggunaan program utiliti tidak mendatangkan mudarat kepada keselamatan maklumat bagi kawalan sistem dan aplikasi.	
KENYATAAN	**TANGGUNGJAWAB**
D.18.1 KAWALAN PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA	
Penggunaan program utiliti yang berkemungkinan mengakibatkan keperluan *overriding* pada kawalan sistem dan aplikasi perlu dihadkan dan dikawal.	ICTSO dan Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI	
Objektif: Memastikan integriti pada sistem operasi dan mengelakkan eksploitasi kepada kerentanan (*vulnerabilities*) teknikal.	
KENYATAAN	**TANGGUNGJAWAB**
D.19.1 KAWALAN PEMASANGAN PERISIAN PADA SISTEM OPERASI	
Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan ICTSO adalah seperti berikut: (a) Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; (b) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian dilaksanakan dan diperaku berjaya; dan (c) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.	ICTSO dan Pentadbir Sistem ICT
D.19.2 SEKATAN KE ATAS INTALASI PERISIAN	
Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran ICTSO.	ICTSO, Pentadbir Sistem ICT dan Semua Pengguna

BIDANG D KAWALAN TEKNOLOGI	
D.20 KESELAMATAN RANGKAIAN	
Objektif: Melindungi maklumat dalam rangkaian dan menyokong kemudahan pemprosesan maklumat dari dikompromi melalui rangkaian.	
KENYATAAN	**TANGGUNGJAWAB**
D.20.1 KAWALAN RANGKAIAN	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan rangkaian hendaklah diletakkan di lokasi yang selamat dan bebas dari sebarang ancaman keselamatan, kerosakan, haiwan perosak dan bencana alam; (b) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (c) Semua peralatan mestilah melalui proses *User Acceptance Test* (*UAT*) selepas pemasangan dan konfigurasi; (d) Semua peralatan rangkaian yang dipasang, dikonfigurasi dan diselenggarakan oleh pembekal hendaklah dipantau oleh Pentadbir Sistem ICT; (e) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan Jabatan / Agensi Sektor Awam Negeri; (f) Memasang perisian *Intrusion Prevention System* (*IPS*) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat Jabatan / Agensi Sektor Awam Negeri;	ICTSO dan Pentadbir Sistem ICT

(g) Sebarang penyambungan rangkaian yang bukan di bawah kawalan Jabatan / Agensi Sektor Awam Negeri adalah tidak dibenarkan; (h) Semua pengguna hanya dibenarkan menggunakan rangkaian Jabatan / Agensi Sektor Awam Negeri. Penggunaan modem/*Wireless Broadband* adalah dilarang sama sekali kecuali mendapat kebenaran ICTSO; (i) Kemudahan bagi *wireless* LAN perlu mematuhi kawalan keselamatan; (j) Sebarang peralatan capaian yang disambungkan ke rangkaian Jabatan / Agensi Sektor Awam Negeri adalah tidak dibenarkan membuat capaian menggunakan kaedah/*tools bypass proxy* yang tidak dibenarkan atau seumpama dengannya; (k) Konfigurasi semua peralatan rangkaian dan keselamatan ICT hendaklah sentiasa dikemas kini berdasarkan keperluan semasa. Salinan konfigurasi hendaklah disimpan oleh Pentadbir Sistem ICT pada storan pendua sebagai *backup*; dan (l) Konfigurasi rangkaian daripada LAN ke WAN perlu *transparent* (tanpa NAT).	

BIDANG D KAWALAN TEKNOLOGI	
D.21 KESELAMATAN PADA PERKHIDMATAN RANGKAIAN	
Objektif: Memastikan keselamatan dalam penggunaan perkhidmatan rangkaian.	
KENYATAAN	**TANGGUNGJAWAB**
D.21.1 KAWALAN PERKHIDMATAN RANGKAIAN	
Pengurusan bagi semua perkhidmatan rangkaian yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian. Semua peralatan rangkaian yang dibekalkan oleh JTDINS bagi sistem rangkaian Sabah Net tidak dibenarkan dialih dan dipinda konfigurasinya tanpa kebenaran ICTSO.	ICTSO dan Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.22 PENGASINGAN DALAM RANGKAIAN	
Objektif: Memisahkan rangkaian dalam sempadan keselamatan dan mengawal trafik di kalangan rangkaian tersebut berdasarkan keperluan perkhidmatan Jabatan / Agensi Sektor Awam Negeri.	
KENYATAAN	**TANGGUNGJAWAB**
D.22.1 KAWALAN PENGASINGAN RANGKAIAN	
Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian Jabatan / Agensi Sektor Awam Negeri. Perkhidmatan *Wireless* untuk kegunaan awam hendaklah diasingkan daripada rangkaian dalaman Jabatan / Agensi Sektor Awam Negeri.	Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.23 *WEB FILTERING*	
Objektif: Untuk melindungi sistem daripada dikompromi oleh perisian hasad dan untuk menghalang akses kepada laman web yang tidak dibenarkan.	
KENYATAAN	**TANGGUNGJAWAB**
D.23.1 KAWALAN *WEB FILTERING*	
Memasang *Web Content Filtering* pada *Internet Gateway* atau kawalan capaian Internet yang bersesuaian untuk menyekat aktiviti/capaian laman web yang dilarang.	Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.24 PENGGUNAAN KRIPTOGRAFI	
Objektif: Memastikan penggunaan kriptografi yang betul dan efektif untuk melindungi kerahsiaan, keaslian atau integriti maklumat berdasarkan perkhidmatan Jabatan / Agensi Sektor Awam Negeri dan keperluan keselamatan serta mengambil kira undang-undang, peraturan dan keperluan kontrak yang berkaitan dengan kriptografi.	
KENYATAAN	**TANGGUNGJAWAB**
D.24.1 POLISI PENGGUNAAN KAWALAN KRIPTOGRAFI	
Kriptografi merangkumi kaedah-kaedah seperti yang berikut: (a) Enkripsi - Sistem aplikasi yang melibatkan maklumat rahsia rasmi hendaklah dibuat enkripsi (*encryption*); dan (b) Tandatangan Digital - Maklumat rahsia rasmi yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media yang mengandungi tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan (c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Pentadbir Sistem ICT dan Semua Pengguna

BIDANG D KAWALAN TEKNOLOGI	
D.25 KESELAMATAN KITAR HAYAT PEMBANGUNAN	
Objektif: Memastikan keselamatan maklumat direka bentuk dan dilaksanakan pada kitar hayat pembangunan perisian dan sistem aplikasi.	
KENYATAAN	**TANGGUNGJAWAB**
D.25.1 DASAR KESELAMATAN PEMBANGUNAN	
Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Keselamatan persekitaran pembangunan; (b) Keselamatan pangkalan data; (i) Pemantauan Capaian Pangkalan Data di Pelayan Produksi secara berkala; (ii) Permohonan Capaian Pangkalan Data di Pelayan Produksi; dan (iii) Pewujudan Pangkalan Data Baharu/Peningkatan direkodkan dengan permohonan perlu disertakan dengan dokumen yang berkaitan. (c) Keperluan keselamatan dalam fasa reka bentuk; (d) Keperluan check point keselamatan dalam carta perbatuan projek; (e) Keperluan pengetahuan ke atas keselamatan aplikasi; (f) Keselamatan dalam kawalan versi; dan (g) Bagi pembangunan secara penyumberluaran (*outsource*), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	ICTSO dan Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.26 KEPERLUAN KESELAMATAN APLIKASI	
Objektif: Memastikan keperluan keselamatan maklumat dikenal pasti dan ditangani ketika membangunkan dan perolehan aplikasi.	
KENYATAAN	**TANGGUNGJAWAB**
D.26.1 PERLINDUNGAN PERKHIDMATAN APLIKASI DALAM RANGKAIAN AWAM	
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: (a) Semua perkhidmatan sumber luaran hendaklah dikenal pasti dan direkodkan. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi Jabatan / Agensi Sektor Awam Negeri. Contoh perkhidmatan sumber luaran ialah: (i) Perisian Sebagai Satu Perkhidmatan (SaaS); (ii) Platform Sebagai Satu Perkhidmatan (PaaS); (iii) Infrastruktur Sebagai Satu Perkhidmatan; (iv) Storan Pengkomputeran Awan; dan (v) Pemantauan Keselamatan. (b) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji secara berkala; (c) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*); (d) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan	ICTSO dan Pentadbir Sistem ICT

(e) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	
D.26.2 PERLINDUNGAN TRANSAKSI PERKHIDMATAN APLIKASI	
Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulangan mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Penggunaan tanda tangan digital oleh setiap pihak yang terlibat dalam transaksi; (b) Memastikan semua aspek transaksi dipatuhi: (i) Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan; (ii) Mengekalkan kerahsiaan maklumat; (iii) Mengekalkan privasi pihak yang terlibat; dan (iv) Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi. (c) Pihak yang mengeluarkan tanda tangan digital ialah yang dilantik oleh Jabatan / Agensi Sektor Awam Negeri.	ICTSO dan Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.27 PRINSIP KESELAMATAN ARKITEKTUR DAN KEJURUTERAAN SISTEM	
Objektif: Memastikan keselamatan maklumat direka bentuk, dilaksana dan beroperasi dengan selamat dalam kitar hayat pembangunan.	
KENYATAAN	**TANGGUNGJAWAB**
D.27.1 PRINSIP KESELAMATAN KEJURUTERAAN SISTEM	
Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumentasi, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan sistem hendaklah sentiasa dikaji dari semasa ke semasa mengikut keperluan dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat.	Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.28 *SECURE CODING*	
Objektif: Prinsip *secure coding* hendaklah digunakan semasa pembangunan sistem aplikasi.	
KENYATAAN	**TANGGUNGJAWAB**
D.28.1 KAWALAN *SECURE CODING*	
Prinsip bagi sistem keselamatan pengaturcaraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan dalam usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan sistem hendaklah sentiasa dikaji dari semasa ke semasa mengikut keperluan dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat.	Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.29 PENGUJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN	
Objektif: Mengesahkan keperluan keselamatan maklumat direkodkan ketika aplikasi atau kod diserahkan (*deploy*) ke persekitaran produksi.	
KENYATAAN	**TANGGUNGJAWAB**
D.29.1 PENGUJIAN KESELAMATAN SISTEM	
Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; (b) Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan (c) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan. Maklumat lanjut berkaitan pengujian keselamatan sistem boleh merujuk kepada dokumen ISO/IEC/IEEE 29119 *Software Testing Standard.*	ICTSO dan Pentadbir Sistem ICT
D.29.2 PENGUJIAN PENERIMAAN SISTEM	
Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat **A.8.2 ANALISIS DAN SPESIFIKASI KEPERLUAN KESELAMATAN MAKLUMAT** dan	ICTSO, Pentadbir Sistem ICT dan Semua Pengguna

kepatuhan kepada **D.25.1 DASAR KESELAMATAN PEMBANGUNAN**; (b) Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai dan didokumentasikan; dan (c) Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan (*vulnerability scanner*). Maklumat lanjut berkaitan boleh merujuk kepada dokumen *ISO/IEC/IEEE 29119 Software Testing Standard.*	

BIDANG D KAWALAN TEKNOLOGI	
D.30 PEMBANGUNAN OLEH SUMBER LUAR (*OUTSOURCED*)	
Objektif: Memastikan langkah-langkah keselamatan maklumat yang diperlukan oleh Jabatan / Agensi Sektor Awam Negeri dilaksanakan oleh pembangun sistem dari sumber luar (*outsourced*).	
KENYATAAN	**TANGGUNGJAWAB**
D.30.1 KAWALAN PEMBANGUNAN OLEH SUMBER LUAR (OUTSOURCED)	
Jabatan / Agensi Sektor Awam Negeri hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Kod sumber (*source code*) adalah menjadi HAK MILIK Jabatan / Agensi Sektor Awam Negeri. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Perkiraan perlesenan, kod sumber adalah HAK MILIK Jabatan / Agensi Sektor Awam Negeri dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara outsource; (b) Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori “Pembekal hendaklah membenar Jabatan / Agensi Sektor Awam Negeri hak mencapai kod sumber dan melaksanakan pengolahan risiko”; (c) Keperluan dalam kontrak syarat kriteria untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik; (d) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem; (e) Mengguna pakai prinsip dan tatacara *escrow*;	ICTSO dan Pentadbir Sistem ICT

(f) Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian; dan (g) Kerja-kerja pembangunan sistem perlu dilakukan di premis Jabatan / Agensi Sektor Awam Negeri atau lokasi yang dibenarkan oleh ICTSO sahaja dengan mengambil kira persekitaran pembangunan yang selamat.	

BIDANG D KAWALAN TEKNOLOGI	
D.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PRODUKSI.	
Objektif: Melindungi persekitaran produksi dan data daripada dikompromi semasa aktiviti pembangunan dan pengujian.	
KENYATAAN	**TANGGUNGJAWAB**
D.31.1 KEPERLUAN PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PRODUKSI	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan dan perisian yang diperlukan bagi tugas membangun, mengemaskini, 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.	ICTSO dan Pentadbir Sistem ICT
D.31.2 PERSEKITARAN PEMBANGUNAN YANG SELAMAT	
Mewujudkan dan melindungi persekitaran pembangunan supaya selamat untuk pembangunan sistem dan integrasi yang meliputi seluruh kitar hayat pembangunan sistem.	ICTSO dan Pentadbir Sistem ICT

Jabatan / Agensi Sektor Awam Negeri perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: (a) Sensitiviti data yang akan diproses, disimpan dan dihantar/diterima dari/ke sistem; (b) Terpakai untuk 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.	

BIDANG D KAWALAN TEKNOLOGI	
D.32 PENGURUSAN KAWALAN PERUBAHAN	
Objektif: Memelihara keselamatan maklumat ketika melaksanakan perubahan.	
KENYATAAN	**TANGGUNGJAWAB**
D.32.1 KAWALAN PERUBAHAN	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan peralatan, sistem untuk pemprosesan maklumat,perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;	Semua Pengguna

(c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak; dan (e) Makluman kepada pengguna perlu dilakukan sekiranya perubahan mengakibatkan gangguan kepada perkhidmatan ICT.	
D.32.2 PROSEDUR KAWALAN PERUBAHAN SISTEM	
Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan Jabatan / Agensi Sektor Awam Negeri. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal; (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; (d) Capaian kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja; dan (e) Sebarang perubahan perlu direkodkan dan diuji.	Pentadbir Sistem ICT

D.32.3 KAJIAN SEMULA TEKNIKAL BAGI APLIKASI SELEPAS PERUBAHAN PLATFORM OPERASI	
Apabila platform operasi berubah, aplikasi bagi perkhidmatan kritikal hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan Jabatan / Agensi Sektor Awam Negeri. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; (b) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan (c) Memastikan perubahan yang sesuai dibuat kepada Pelan Kesinambungan Perkhidmatan (PKP) Jabatan / Agensi Sektor Awam Negeri dan Pelan Pemulihan Bencana Sistem (DRP) yang berkaitan.	ICTSO dan Pentadbir Sistem ICT
D.32.4 SEKATAN KE ATAS PERUBAHAN DALAM PAKEJ PERISIAN	
Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.	Pentadbir Sistem ICT

BIDANG D KAWALAN TEKNOLOGI	
D.33 MAKLUMAT UNTUK AKTIVITI PENGUJIAN	
Objektif: Memastikan pengurusan maklumat pengujian adalah dikawal.	
KENYATAAN	**TANGGUNGJAWAB**
D.33.1 PERLINDUNGAN MAKLUMAT UNTUK AKTIVITI PENGUJIAN	
Maklumat yang digunakan untuk aktiviti pengujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; (b) Pentadbir Sistem ICT yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; (c) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan (d) Permohonan penyalinan dan penggunaan data sebenar sebagai data pengujian hendaklah direkodkan.	ICTSO, Pentadbir Sistem ICT dan Semua Pengguna

BIDANG D KAWALAN TEKNOLOGI	
D.34 PERLINDUNGAN KESELAMATAN MAKLUMAT KETIKA PENGUJIAN AUDIT	
Objektif: Meminimumkan kesan audit dan lain-lain aktiviti sebagai jaminan terhadap sistem operasi dan proses dalam perkhidmatan Jabatan / Agensi Sektor Awam Negeri.	
KENYATAAN	**TANGGUNGJAWAB**
D.34.1 KAWALAN AUDIT SISTEM MAKLUMAT	
Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dan dipersetujui bagi meminimumkan gangguan ke atas perkhidmatan Jabatan / Agensi Sektor Awam Negeri. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	ICTSO dan Pentadbir Sistem ICT

GLOSARI

Access Point	Perkakasan yang digunakan untuk mengwujudkan rangkaian tanpa wayar (*wireless*) pada sesuatu tempat.
AKNS	Agensi Kerajaan Negeri Sabah
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, cakera keras, pita magnetik, *optical disk, flash disk, thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk peralatan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses salinan sesuatu dokumen atau maklumat.
Bandwidth	Jalur Lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
Browser	Pelayar atau penjelajah media
BYOD	*Bring Your Own Device* Merujuk kepada pekerja yang membawa peranti pengkomputeran mereka sendiri - seperti telefon pintar, komputer riba dan tablet PC - untuk bekerja dengan mereka dan menggunakannya sebagai tambahan kepada atau bukan peranti yang disediakan oleh majikan.
Bypass proxy	Capaian Internet atau rangkaian dengan menggunakan perkhidmatan proxy server dari pihak ketiga bagi tujuan pemintasan.
CDO	*Chief Digital Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Content Filtering	Proses yang mengurus atau menyaring capaian kepada laman web tertentu.
COTS	*Commercial off-the-shelf*

	Produk sedia ada yang disesuaikan dengan keperluan organisasi pembeli.
Data masking	Teknik yang digunakan untuk mewujudkan versi data yang kelihatan secara struktur adalah sama dengan data asal tetapi menyembunyikan maklumat sensitif.
Denial of service	Halangan pemberian perkhidmatan.
Domain Server	Komputer yang mengandungi pangkalan data alamat IP yang mengaitkannya dengan nama domain.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Escrow	Deposit kod sumber perisian dengan pihak ketiga.
Failover	Keupayaan untuk menukar secara automatik dan lancar kepada sistem sandaran (*backup*) yang boleh dipercayai.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Hub	Hab (hub) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	ICT Security Officer Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi

	pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code.* Contohnya: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
Malware	Perisian Hasad “Perisian hasad” merujuk kepada sebarang jenis perisian yang direka untuk membahayakan komputer.
NC4	*National Cyber Coordination and Command Centre.* Pusat yang dibangunkan untuk tujuan pengurusan krisis siber termasuk pemantauan ancaman siber terhadap sistem kritikal negara.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pegawai Aset	Pegawai yang dilantik untuk menjaga aset di Jabatan/Agensi Kerajaan Negeri.
Pelanggan	Pengguna awam dan pengguna Jabatan/Agensi Kerajaan Negeri

Pemilik Projek	Pemilik Projek adalah pihak yang bertanggungjawab ke atas keseluruhan proses bisnes di dalam projek.
Pemilik Sistem	Pihak yang bertanggungjawab yang merupakan pemilik bisnes dan mengatur peruntukan sedia ada untuk menentukan keutamaan pengurusan sistem.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi.
Personal Identifiable Information (PII)	Maklumat Pengecaman Individu Maklumat yang apabila digunakan secara bersendirian atau dengan data lain yang berkaitan mampu mengenal pasti seseorang individu.
PKP	Pelan Kesinambungan Perkhidmatan Proses pengurusan menyeluruh yang mengenal pasti potensi kesan yang mengancam organisasi, dan menyediakan rangka kerja untuk membangun daya tahan dan keupayaan untuk bertindak balas yang berkesan yang melindungi kepentingan pemegang taruh, reputasi, jenama dan penciptaan nilai aktiviti.
Proxy	Aplikasi pelayan atau peralatan yang bertindak sebagai perantara untuk permohonan daripada pelanggan yang menjangkau sumber dari pelayan yang membekalkan sumber ini.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Public Wi-fi	Wi-fi awam yang telah disediakan oleh pihak tertentu (seperti di restoran) secara percuma.
Redundancy	Juga dikenali sebagai lewahan. Penyelesaian bagi penyediaan peralatan pendua, sandaran atau pautan yang segera mengambil alih fungsi peralatan atau talian penghantaran yang gagal.
Remote Access	Kawalan jauh komputer dengan menggunakan peranti lain yang disambungkan melalui internet atau rangkaian lain.

Rollback	Tindakan mengembalikan sesuatu kepada keadaan asalnya kesan daripada sesuatu aktiviti.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Secure Deletion	Proses yang mengelakkan dari berlakunya proses pemulihan (*recovery*) fail yang telah dipadam dengan menggantikan data fail tersebut dengan data yang tidak bermakna.
Server	Pelayan komputer.
Session Time-out	Waktu tamat sesi mewakili peristiwa yang berlaku apabila pengguna tidak melakukan apa-apa tindakan di laman web/sistem aplikasi pada sela waktu yang ditetapkan.
Source Code	Kod Sumber Program komputer dalam bahasa pengaturcaraan asalnya (seperti *FORTRAN* atau *C*) sebelum terjemahan ke kod objek biasanya oleh pengkompil.
Storan Awan (*Cloud Storage*)	Media penyimpanan online yang membolehkan pengguna menyimpan data/maklumat di pelayan mata (*server virtual*) yang tersedia.
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (*CSMA/CD*) yang merupakan satu protokol penghantaran dengan mengurangkan pelanggaran yang berlaku.
Tandatangan Digital	Tandatangan khusus yang bersandarkan sijil digital, memberikan bukti identiti anda. Tandatangan digital diiktiraf sebagai sejenis e-tandatangan yang lebih selamat kerana ia terikat secara kriptografi kepada dokumen yang telah ditandatangani dan boleh disahkan.
Telecommuting	Pengaturan kerja di mana pekerja bekerja di luar pejabat, sering bekerja dari rumah atau lokasi yang

	dekat dengan rumah (termasuk kedai kopi, perpustakaan, dan pelbagai tempat lain).
Two-level authentication (2FA)	Kaedah pengesahan yang memerlukan pengguna menggunakan dua faktor pengesahan untuk membuat capaian ke aplikasi, akaun dalam talian dan sebagainya.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virtual Private Network	Rangkaian Peribadi Maya Rangkaian yang menggunakan infrastruktur telekomunikasi awam, seperti Internet, untuk membekalkan pejabat-pejabat jarak jauh atau pengguna persendirian dengan capaian selamat/tidak selamat terhadap rangkaian organisasi mereka.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
WAN	*Wide Area Network* atau Rangkaian Kawalan Luas Rangkaian yang wujud di kawasan geografi berskala besar menghubungkan rangkaian yang lebih kecil.
Web Filtering	Tapisan web adalah seperti pengawal keselamatan digital yang memeriksa laman web yang orang ingin layari. Ia menilai laman web ini dan memutuskan sama ada mereka selamat atau tidak.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran 1

UNDANG-UNDANG ATAU PERATURAN-PERATURAN LAIN YANG BERKAITAN DAN BERKUAT KUASA

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di Jabatan/Agensi Awam Negeri:

1	Akta Rahsia Rasmi 1972;
2	Akta Tandatangan Digital 1997;
3	Akta Jenayah Komputer 1997;
4	Akta Hak Cipta (Pindaan) Tahun 2012;
5	Akta Komunikasi dan Multimedia 1998;
6	Akta Aktiviti Kerajaan Elektronik 2007;
7	Akta Perlindungan Data Peribadi 2010;
8	Akta Keselamatan Siber 2024 (Akta 854);
9	Akta Perkongsian Data 2025 (Akta 864);
10	Akta Keselamatan Dalam Talian 2025 (Akta 866);
11	Electronic Government Activities Enactment 2014;
12	Perintah-Perintah Am;
13	Arahan Keselamatan (Semakan dan Pindaan 2017);
14	Arahan Perbendaharaan;
15	Arahan Teknologi Maklumat 2007;
16	Surat Arahan Ketua Setiausaha Negara- Penamaan Ketua Pegawai Maklumat Sektor Awam bertarikh 22 Mac 2000;
17	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;
18	Surat Arahan Ketua Pengarah MAMPU - Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-Agensi Kerajaan bertarikh 23 Mac 2009;

19	Surat Arahan Ketua Pengarah - Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 dalam Sektor Awam Bertarikh 24 November 2010;
20	Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam bertarikh 22 Jan 2010;
21	Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
22	Surat Pekeliling Perbendaharaan Bil. 3/1995 – Peraturan Perolehan Perkhidmatan Perundingan;
23	Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
24	Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
25	Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
26	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
27	Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
28	Surat Pekeliling Am Bil. 3 Tahun 2015 – Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Agensi Sektor Awam;
29	Pekeliling Transformasi Pentadbiran Awam Bil. 3 Tahun 2018 – Panduan Pengurusan Projek ICT Sektor Awam (PPrISA);
30	Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
31	Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2021 – Dasar Perkongsian Data Sektor Awam;
32	Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2021 – Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam;
33	Surat Pekeliling Am Bil. 3 Tahun 2022 – Garis Panduan Pengurusan Keselamatan Penggunaan Persidangan Video (Video Conferencing) dalam Perkhidmatan Awam;
34	Surat Pekeliling Am Bil. 3 Tahun 2022 - Garis Panduan Sanitasi Media Elektronik dalam Perkhidmatan Awam;
35	Pekeliling Am Bil. 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam;
36	Pekeliling Kementerian Pembangunan Sumber dan Kemajuan Teknologi Maklumat Bil.1 Tahun 2018 - Pemantauan dan Penyalahgunaan Kemudahan Rangkaian Sabah.Net;
37	Pekeliling Jabatan Ketua Menteri, Rujukan: JKM 100-4/62 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 19 Jun 2024;

38	Surat Pekeliling Kementerian Sains, Teknologi dan Inovasi Bilangan 1/2025 - Garis Panduan Perolehan, Pengagihan Dan Penyelenggaraan Peralatan ICT;
39	Surat Pekeliling Kementerian Sains, Teknologi dan Inovasi Bilangan 2/2025 - Garis Panduan Pemasangan Sistem Rangkaian Komputer (Dalaman);
40	Surat Pekeliling Kementerian Sains, Teknologi dan Inovasi Bilangan 3/2025 - Garis Panduan Mengenai Tatacara Penggunaan Internet;
41	Surat Pekeliling Kementerian Sains, Teknologi dan Inovasi Bilangan 4/2025 - Garis Panduan Penggunaan *Bring Your Own Device* (BYOD);
42	Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSA), April 2016;
43	Lampiran C Pekeliling Perkhidmatan Bilangan 15 Tahun 2006;
44	Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam;
45	Pemantapan Penggunaan Dan Pengurusan E-Mel Di Agensi-Agensi Kerajaan Bertarikh 1 Julai 2010;
46	Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam oleh NACSA bertarikh 28 Februari 2019;
47	Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) oleh NACSA bertarikh 28 Januari 2019;
48	Surat Edaran Ketua Pengarah Keselamatan Bil 2/2022 bertajuk Garis Panduan Pengurusan Keselamatan Perlindungan Dalam Mengurus dan Menghadapi Bencana;
49	Garis Panduan Perolehan ICT Kerajaan;
50	Garis Panduan Pengurusan Pusat Data MAMPU;
51	The National Guidelines on AI Governance & Ethics 2024; dan
52	Polisi Pendigitalan Data Sektor Awam.

Lampiran 2

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN SIBER SEKTOR AWAM SABAH

Nama (Huruf Besar) :

No. Kad Pengenalan : ----------

Jawatan/Gred : ----------

Jabatan/Agensi : ----------

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

1. Saya telah membaca, memahami dan akur peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan Siber Sektor Awam Sabah.
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : ----------

Tarikh : ----------

Pengesahan Pegawai Keselamatan ICT

(Nama Pegawai Keselamatan ICT)

b.p Ketua Jabatan/Agensi

Tarikh:

Lampiran 3

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 satu 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 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/Agensi :.....
Tarikh :.....

Cop Jabatan/Organisasi

Lampiran 4

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

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 satu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

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

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

Tandatangan : .....
Nama (huruf besar) : .....
No. Kad Pengenalan : .....
Jawatan : .....
Jabatan/Organisasi : .....
Tarikh :

Disaksikan oleh
Tandatangan : .....
Nama (huruf besar) : .....
Jawatan : .....
Jabatan/Agensi : .....
Tarikh : .....
Cop Jabatan/Organisasi :