JABATAN KOMUNIKASI KOMUNITI

DASAR KESELAMATAN ICT (DKICT)

VERSI 1.0
MEI 2022

REKOD PINDAAN DOKUMEN

TARIKH	VERSI	KETERANGAN PINDAAN
30 Mei 2022	1.0	Dokumen Baharu

KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT (DKICT) Jabatan Komunikasi Komuniti (J-KOM) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset *Information and Communication Technology* (ICT) di J-KOM. Dasar ini juga menerangkan kepada semua pengguna di Jabatan mengenai tanggungjawab dan peranan pengguna dalam melindungi aset ICT J-KOM. Polisi ini adalah terpakai kepada semua warga J-KOM dan pihak ketiga yang berurusan dengan J-KOM.

OBJEKTIF

Objektif utama DKICT J-KOM ialah seperti berikut :

a. Memastikan kelancaran pengoperasian Jabatan berlandaskan ICT dengan meminimumkan kerosakan atau kemusnahan aset ICT Jabatan;

b. Melindungi kepentingan pihak-pihak yang bergantung kepada operasi ICT Jabatan dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

c. Mencegah penyalahgunaan, penyelewengan atau kecurian aset ICT Kerajaan; dan

d. Meningkatkan tahap kesedaran keselamatan ICT kepada pengguna aset ICT Jabatan.

PERNYATAAN DASAR

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

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

a. Melindungi maklumat terperingkat Kerajaan dari capaian tanpa kuasa yang sah;

b. Menjamin setiap maklumat adalah tepat dan sempurna;

c. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

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

DKICT J-KOM merangkumi perlindungan atas semua bentuk maklumat elektronik dan bukan 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 terkini. 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 itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul, dan langkah-langkah pencegahan yang boleh diambil untuk menangani risiko berkenaan.

SKOP

Aset ICT Jabatan terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat, manusia dan premis. DKICT J-KOM 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 Jabatan terjamin keselamatannya sepanjang masa, DKICT J-KOM merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut :

a. Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan Jabatan. Contoh: komputer, pencetak, pengimbas, pelayan, peralatan komunikasi dan sebagainya.

b. Perisian

Semua jenis perisian yang digunakan untuk mengendali, memproses, menyimpan dan menghantar data atau maklumat. Ini termasuklah sistem aplikasi, perisian sistem operasi seperti Windows dan LINUX serta perisian utiliti, perisian komunikasi, sistem pengurusan pangkalan data, fail program, fail data dan lain-lain.

c. Perkhidmatan

Perkhidmatan yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:

i. Perkhidmatan rangkaian seperti *Local Area Network* (LAN), *Wide Area Network* (WAN) dan lain-lain;

ii. Sistem halangan akses seperti sistem kad akses; dan

iii. Perkhidmatan sokongan seperti kemudahan bekalan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

d. Data atau Maklumat

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

e. Manusia

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

f. Premis

Semua kemudahan yang digunakan untuk menempatkan Perkara **(a) hinga (e)** yang dinyatakan di atas.

Setiap perkara di atas perlu diberi perlindungan yang rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT J-KOM dan perlu dipatuhi adalah seperti berikut:

a. Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT J-KOM hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan;

b. Hak akses minimum

Hak akses 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 akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

c. Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah :

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

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

iii. Menentukan maklumat sedia untuk digunakan;

iv. Menjaga kerahsiaan kata laluan;

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

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

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

d. Pengasingan

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

e. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dan dikonfigurasi supaya dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit yang bersesuaian.

f. Pematuhan

DKICT Jabatan hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

g. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan Pelan Pemulihan Bencana/Pengurusan Kesinambungan Perkhidmatan.

h. 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 optimum.

PENILAIAN RISIKO KESELAMATAN ICT

Jabatan hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan kelemahan yang semakin meningkat pada masa ini. Sehubungan itu, Jabatan perlu mengambil tindakan dan langkah proaktif, munasabah dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

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

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

Jabatan bertanggungjawab melaksana dan menguruskan risiko keselamatan ICT selaras dengan Surat Pekeliling Am Bilangan 6 Tahun 2005 : Garis Panduan Penilaian Risiko Keselamatan ICT Keselamatan Maklumat Sektor Awam.

Jabatan 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 Jabatan;

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

d. Memindahkan risiko kepada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

PERKARA 01 – PEMBANGUNAN DAN PENYELENGGARAAN DASAR

Objektif	
Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Jabatan serta perundangan yang berkaitan.	
KENYATAAN	**TINDAKAN**

0101 Dasar Keselamatan ICT

010101 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah (KP) dibantu oleh Ketua Pegawai Maklumat (CIO), Pengurus ICT, Pegawai Keselamatan ICT (ICTSO) dan semua Pengarah Bahagian/Unit.	KP

010102 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua pengguna aset ICT Jabatan merangkumi warga J-KOM, pembekal, perunding dan lain-lain yang bertugas dan/atau berurusan dengan Jabatan.	ICTSO

010103 Penyelenggaraan Dasar

DKICT J-KOM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan DKICT J-KOM: a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Kemukakan cadangan pindaan kepada peringkat tertinggi Jabatan iaitu Mesyuarat Pengurusan J-KOM yang dipengerusikan oleh KP untuk pertimbangan dan persetujuan ahli mesyuarat; c. Perubahan yang telah dipersetujui mestilah dimaklumkan kepada semua pengguna; dan	ICTSO

d. Dasar ini hendaklah dikaji semula mengikut keperluan semasa.	

010104 Pemakaian Dasar

DKICT J-KOM adalah terpakai kepada semua pengguna aset ICT Jabatan dan tiada pengecualian diberikan.	Pengguna

PERKARA 02 – ORGANISASI KESELAMATAN

Objektif	
Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT J-KOM.	
KENYATAAN	**TINDAKAN**

0201 Infrastruktur Organisasi Dalaman

020101 Ketua Pengarah (KP)

Peranan dan tanggungjawab KP adalah seperti berikut: a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah DKICT J-KOM; b. Memastikan semua pengguna mematuhi DKICT J-KOM; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT J-KOM; dan e. Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT), J-KOM.	KP

020102 Ketua Pegawai Maklumat (CIO)

Ketua Pegawai Maklumat (CIO) adalah Timbalan Ketua Pengarah J-KOM. Peranan dan tanggung jawab CIO adalah seperti berikut : a. Membantu KP dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT J-KOM; b. Menentukan keperluan keselamatan ICT J-KOM; c. Menyelaras dan mengurus pelan pelaksanaan bagi program kesedaran keselamatan ICT seperti penyediaan DKICT J-KOM, latihan, kesedaran pengguna, pengurusan risiko serta pengauditan; dan d. Bertanggungjawab atas perkara-perkara yang berkaitan dengan keselamatan ICT J-KOM.	TKP

020103 Pengurus ICT

Pengurus ICT ialah Pengarah Bahagian Teknologi Maklumat, J-KOM. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut : a. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan J-KOM; b. Menentukan kawalan akses semua pengguna terhadap aset ICT; c. Memaklumkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO dan CIO; dan d. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT J-KOM.	Pengurus ICT

020104 Pegawai Keselamatan ICT (ICTSO)

ICTSO J-KOM adalah Penolong Pengarah Bahagian Teknologi Maklumat (BTM) J-KOM. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Mengurus keseluruhan program keselamatan ICT Jabatan; b. Menguatkuasakan pelaksanaan DKICT J-KOM; c. Memberi penerangan, taklimat dan pendedahan berkenaan DKICT J-KOM kepada semua warga Jabatan; d. Mewujud dan melaksanakan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT J-KOM; e. Menjalankan pengurusan risiko; f. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan Bahagian/Unit berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g. Memberi dan menyebarkan amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h. Melaporkan insiden keselamatan ICT kepada Pasukan Pengendali Insiden Keselamatan ICT (CERT) J-KOM, CIO dan Agensi Keselamatan Siber Negara (NACSA); i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; j. Melaporkan sebarang salah laku pengguna yang melanggar DKICT J-KOM kepada CIO; k. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar DKICT J-KOM; l. Menyedia, melaksanakan dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT;	ICTSO

m. Menyedia, melaksanakan dan menyelaras penilaian risiko dan program keselamatan ICT sepertimana yang ditetapkan dalam DKICT J-KOM; dan n. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	

020105 Pentadbir ICT

Pentadbir ICT ialah Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat, Juruteknik Komputer dan Pegawai yang berkelayakan di Jabatan. Peranan dan tanggungjawab Pentadbir ICT adalah seperti berikut : a. Mengambil tindakan segera yang bersesuaian dengan pengurusan aset ICT apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat atau Pengurus ICT; c. Mengurus dan memantau aset ICT; d. Memastikan setiap aset ICT J-KOM yang disediakan bagi keperluan jabatan digunakan dengan baik; e. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; f. Melaporkan sebarang insiden keselamatan ICT kepada ICTSO; g. Menyimpan dan menganalisis rekod jejak audit; dan h. Menyediakan laporan pengurusan aset ICT secara berkala atau mengikut keperluan.	Pentadbir ICT

020106 Pengguna

Pengguna adalah semua warga J-KOM atau Pihak Ketiga yang bertugas dan/atau berurusan dengan J-KOM . Peranan dan tanggungjawab pengguna adalah seperti berikut : a. Membaca, memahami dan mematuhi DKICT J-KOM; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat terperingkat; d. Melaksanakan prinsip-prinsip DKICT J-KOM dan menjaga kerahsiaan maklumat J-KOM; e. Melaksanakan langkah-langkah perlindungan seperti berikut :- i. Menghalang pendedahan atau ketirisan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi prosedur dan garis panduan keselamatan yang ditetapkan; vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f. Melaporkan segera sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO; g. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan	Pengguna

h. Menandatangani Akuan Pematuhan Dasar Keselamatan ICT Jabatan Komunikasi Komuniti (J-KOM) seperti di **LAMPIRAN A**.	

020107 Pasukan Pengendali Insiden Keselamatan ICT (CERT)

Keanggotaan CERT adalah seperti berikut : **Pengarah CERT:** Pengurus ICT (Pengarah BTM) **Pengurus CERT:** Pegawai Keselamatan ICT (ICTSO) **Ahli :** a. Pegawai Teknologi Maklumat b. Penolong Pegawai Teknologi Maklumat **Urusetia** bagi CERT Jabatan adalah BTM. Peranan dan tanggungjawab CERT adalah seperti berikut: a. Menerima dan mengesan aduan keselamatan ICT Jabatan dan menilai tahap dan jenis insiden; b. Merekodkan dan menjalankan siasatan awal insiden yang diterima; c. Menangani tindak balas (response) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d. Menghubungi dan melaporkan insiden yang berlaku kepada NACSA sama ada sebagai input atau untuk tindakan seterusnya; e. Memberi khidmat nasihat kepada CIO mengenai tindakan pemulihan dan pengukuhan; f. Menyebarkan makluman berkaitan pemulihan dan pengukuhan kepada semua pengguna J-KOM; dan g. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	CERT

020108 Pegawai Aset

Peranan dan tanggungjawab Pegawai Aset adalah seperti berikut: a. Mengetuai Bahagian/Cawangan/Unit Pengurusan Aset dengan memastikan Pengurusan Aset Alih Kerajaan dijalankan selaras dengan peraturan yang ditetapkan dalam Pekeliling Perbendaharaan; b. Menyelaras pelantikan Pegawai Aset, Pegawai Pemeriksa Aset dan Lembaga Pemeriksa Pelupusan Aset bagi PTJ-PTJ di bawah seliaannya termasuk Penolong Pegawai Aset; c. Menjadi urusetia Mesyuarat Jawatankuasa Pengurusan Aset Kerajaan (JKPAK) peringkat Jabatan; d. Memastikan Tatacara Pengurusan Aset Alih Kerajaan diurus secara baik meliputi Penerimaan, Pendaftaran, Penggunaan, Penyimpanan, Pemeriksaan, Penyelenggaraan, Pindahan, Pelupusan, Kehilangan dan Hapus Kira.	Pegawai Aset

0202 Pihak Ketiga

020201 Keperluan Keselamatan Dalam Perkhidmatan ICT

Pihak Ketiga terdiri daripada pembekal, pakar runding dan pihak lain yang terlibat dalam penggunaan atau capaian kepada aset ICT jabatan atas urusan rasmi. Perkara yang perlu dipatuhi termasuk adalah seperti berikut : a. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; b. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan Pihak Ketiga; c. Akses kepada aset ICT jabatan perlu berlandaskan kepada perjanjian dan peraturan yang ditetapkan iaitu: i. DKICT J-KOM; ii. Tapisan Keselamatan; iii. Akta Rahsia Rasmi 1972; iv. Hak Harta Intelek; dan v. Arahan Teknologi Maklumat 2007. d. Menandatangani Akta Rahsia Rasmi 1972 seperti di **LAMPIRAN B;** dan e. Menandatangani Akuan Pematuhan Dasar Keselamatan ICT Jabatan Komunikasi Komuniti (J-KOM) seperti **di LAMPIRAN A**.	Pihak Ketiga

PERKARA 03 – PENGURUSAN ASET

Objektif	
Menyediakan dan menyokong perlindungan keselamatan yang bersesuaian atas semua aset ICT J-KOM.	
KENYATAAN	**TINDAKAN**

0301 Akauntabiliti Aset

030101 Inventori Aset

Ini bertujuan memastikan aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Peranan yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset ICT diurus berdasarkan Pekeliling Perbendaharaan AM Bil. 2 Tahun 2018 - Tatacara Pengurusan Aset Alih Kerajaan; b. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di J-KOM; d. Setiap pengguna bertanggungjawab atas aset ICT yang di bawah kawalannya; dan e. Peraturan, prosedur dan tatacara bagi pengendalian dan pengurusan aset ICT hendaklah dikenal pasti, didokumenkan dan dilaksanakan.	Pentadbir ICT Pengguna

0302 Pengelasan dan Pengendalian Maklumat

030201 Pengelasan Maklumat

Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad	Semua

030202 Pengendalian Maklumat

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan 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 prosedur dan garis panduan keselamatan yang ditetapkan; f. Memberi perhatian aktiviti pengendalian maklumat terperingkat; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT J-KOM dari diketahui umum.	Semua

PERKARA 04 – KESELAMATAN SUMBER MANUSIA

Objektif	
Memastikan pihak yang terlibat memahami tanggungjawab dan peranan bagi meningkatkan pengetahuan dalam keselamatan aset ICT.	
KENYATAAN	**TINDAKAN**

0401 Keselamatan Aset ICT dalam Tugas Harian

040101 Sebelum Perkhidmatan

Pengguna mestilah memahami tanggungjawab masing-masing atas keselamatan aset ICT J-KOM bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi adalah seperti berikut : a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab semua pengguna yang berkepentingan atas keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk semua pengguna yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Pengguna

040102 Semasa Perkhidmatan

Memastikan semua pengguna hendaklah faham dan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong DKICT J-KOM dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi adalah seperti berikut :	Pengurus ICT ICTSO

a. Memastikan pengguna menguruskan keselamatan berdasarkan perundangan dan peraturan yang ditetapkan oleh Kerajaan atau melalui kawalan dalaman/ garis panduan J-KOM; b. Memastikan latihan atau program kesedaran yang berkaitan mengenai pengurusan keselamatan ICT J-KOM diberi kepada pengguna dari semasa ke semasa; c. Memastikan adanya proses tindakan tatatertib atas pengguna, sekiranya berlaku perlanggaran dengan perundangan dan peraturan berkaitan ICT yang ditetapkan oleh Kerajaan atau melalui kawalan dalaman/ garis panduan J-KOM; dan d. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul bagi menjamin kepentingan keselamatan ICT J-KOM.	

040103 Bertukar atau Tamat Perkhidmatan

Memastikan semua pengguna diuruskan dengan teratur apabila bertukar atau tamat perkhidmatan dari J-KOM. Perkara yang perlu dipatuhi adalah seperti berikut :- a. Memastikan semua aset ICT Kerajaan dikembalikan kepada Jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; b. Meminda atau membatalkan semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan dan/atau terma perkhidmatan; dan c. Memastikan semua maklumat terperingkat dipulangkan atau dihapuskan secara selamat mengikut prosedur yang ditetapkan.	Pengurus ICT ICTSO

PERKARA 05 – KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif	
Melindungi aset ICT daripada sebarang bentuk pencerobohan, kerosakan atau ancaman.	
KENYATAAN	**TINDAKAN**

0501 Keselamatan Kawasan

050101 Kawalan Kawasan

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat Jabatan. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; d. Memperkukuhkan dinding dan siling; e. Memasang alat penggera atau kamera; f. Menghadkan jalan keluar masuk; g. Mengadakan kaunter kawalan; h. Menyediakan tempat atau bilik khas untuk pelawat-pelawat;	CIO ICTSO

i. Mewujudkan perkhidmatan kawalan keselamatan; j. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja dibenarkan melalui pintu masuk; k. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; l. Mereka bentuk dan melaksanakan keselamatan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; m. Menyediakan garis panduan bagi pengguna J-KOM yang bekerja di dalam kawasan terhad; dan n. Memastikan kawasan-kawasan penghantaran dan pemunggahan serta tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	

050102 Kawalan Masuk Fizikal

Perkara yang perlu dipatuhi adalah seperti berikut: a. Warga J-KOM hendaklah memakai atau mengenakan Pas Keselamatan Pekerja sepanjang waktu bertugas; b. Pihak Ketiga perlu mendapatkan Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; c. Semua pas keselamatan hendaklah diserahkan balik kepada bahagian berkenaan apabila pengguna bertukar atau tamat perkhidmatan; d. Kehilangan pas keselamatan mestilah dilaporkan dengan segera; dan e. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai dan/atau menggunakan aset ICT J-KOM.	Pengguna

050103 Kawasan Larangan

Pengguna dilarang berada di Pusat Data (*Data Centre*) atau Bilik *Server* J-KOM kecuali dengan kebenaran dan/atau diiringi oleh pegawai yang diberi kuasa. Akses kepada kawasan larangan hanyalah kepada pengguna yang dibenarkan sahaja. Pusat Data atau Bilik *Server* J-KOM merupakan kawasan larangan yang dihadkan kemasukannya bagi melindungi aset ICT yang terdapat di dalam kawasan tersebut. Pengguna dilarang merakam sebarang foto atau video dikawasan ini, kecuali mendapat kelulusan bertulis ICTSO terlebih dahulu.	Pengurus ICT ICTSO Pentadbir ICT

0502 Keselamatan Peralatan

050201 Peralatan ICT

Pengguna perlu mematuhi langkah-langkah keselamatan seperti berikut: a. Menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Bertanggungjawab terhadap peralatan ICT di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; c. Penggunaan kata laluan untuk akses ke peralatan ICT adalah diwajibkan; d. Bertanggungjawab sepenuhnya ke atas peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran peralatan dan konfigurasi yang telah ditetapkan; e. Dilarang sama sekali menambah, menanggalkan, mengganti atau memindahkan sebarang peralatan ICT yang telah ditetapkan; f. Dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir ICT; g. Memastikan perisian *antivirus* sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;	Pengguna

h. Melindungi semua peralatan ICT daripada sebarang isu seperti kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna. Sekiranya isu ini berlaku, hendaklah dilaporkan kepada ICTSO J-KOM; i. Bertanggungjawab atas kerosakan atau kehilangan peralatan ICT di bawah jagaan dan/atau kawalannya; j. Peralatan ICT yang kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); k. 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; l. Sebarang pelekat hiasan atau contengan yang meninggalkan kesan yang lama pada peralatan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; m. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; n. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir ICT untuk dibaik pulih; o. Memastikan semua komputer, pencetak dan pengimbas berkeadaan "*SLEEP*" apabila tidak digunakan/ditinggalkan sementara dan berkeadaan "*OFF*" apabila pengguna meninggalkan pejabat; p. Memastikan palam (plug) ditanggalkan dari soket pendawaian elektrik bagi mengelakkan kerosakkan peralatan apabila meninggalkan pejabat atau sekiranya peralatan tidak digunakan dalam tempoh yang lama; dan q. Sebarang bentuk kehilangan, penyelewengan atau salah guna peralatan hendaklah dilaporkan kepada ICTSO J-KOM.	

050202 Media Storan

Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti *optical disk*, *flash drive*, *external hard disk, public cloud storage* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan dan integriti serta kebolehsediaan untuk digunakan. Pengguna perlu mengambil langkah-langkah berikut bagi menjamin keselamatan media storan: a. Media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; b. Media storan perlu dipastikan keselamatannya sebelum disambungkan kepada peralatan ICT; c. Maklumat dalam media storan perlu dihapuskan secara selamat terlebih dahulu sebelum media storan dilupuskan; d. Media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk ketahanan dari dipecahkan serta dari api, air dan medan magnet; e. Media storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan dan dikategorikan selamat serta akses hendaklah terhad kepada pengguna yang dibenarkan sahaja; f. Akses dan pergerakan kepada media storan yang mengandungi maklumat terperingkat perlu direkodkan; g. Hanya maklumat terbuka sahaja boleh disimpan di dalam *public cloud storage*. *Public cloud storage client* hendaklah diputuskan dari talian selepas digunakan; dan h. Menyediakan salinan atau penduaan pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data.	Pengguna

050203 Media Perisian dan Sistem Aplikasi

Perkara yang perlu dipatuhi adalah seperti berikut: a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan di Jabatan; b. Sistem aplikasi dalaman tidak dibenarkan diagih atau didemontrasi kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c. Lesen perisian (*registration code, serials, Compact Disc Keys (CD-keys)*) perlu disimpan berasingan daripada media storan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; d. Perisian dan aplikasi milik Kerajaan adalah tidak dibenarkan dipasang pada peralatan milik peribadi kecuali dengan kelulusan; dan e. Kod sumber sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Pengurus ICT Pengguna

050204 Media Sijil Tandatangan Digital

Perkara yang perlu dipatuhi adalah seperti berikut: a. Semua pengguna hendaklah bertanggungjawab sepenuhnya ke atas media atau sijil tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b. Media ini tidak boleh dipindah milik atau dipinjamkan kepada pengguna lain; dan c. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan segera kepada ICTSO untuk tindakan selanjutnya.	ICTSO Pengguna

050205 Penyelenggaraan Peralatan

Peralatan hendaklah diselenggarakan dengan baik bagi memastikan kebolehsediaan dan integriti. Perkara yang perlu dipatuhi adalah seperti berikut: a. Bertanggungjawab terhadap setiap peralatan ICT bagi penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; b. Peralatan yang diselenggarakan hendaklah mematuhi prosedur yang telah ditetapkan; c. Peralatan hanya boleh diselenggara oleh pihak yang dibenarkan sahaja; d. Peralatan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; e. Pengguna dimaklumkan sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f. Aktiviti penyelenggaraan mestilah mendapat kebenaran dari Pengurus ICT atau Pentadbir ICT yang bertanggungjawab.	Pengurus ICT Pentadbir ICT Pengguna Pihak Ketiga

050206 Pergerakan Peralatan

Peralatan yang dibawa masuk atau dibawa ke luar premis adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mendapatkan kelulusan Pengurus ICT/Pegawai Aset/Pentadbir ICT bagi pergerakan peralatan; b. Peralatan yang digunakan perlu dilindungi dan dikawal sepanjang masa; c. Pergerakan, penyimpanan atau penempatan peralatan hendaklah mengambil kira ciri-ciri keselamatan yang bersesuaian; d. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan bagi tujuan pemantauan; dan e. Melengkapkan Borang Pergerakan Aset seperti di **LAMPIRAN D**.	Pengurus ICT Pentadbir ICT Pegawai Aset Pengguna

050207 Pelupusan Peralatan

Peralatan ICT yang hendak dilupuskan perlu melalui proses pelupusan terkini. Langkah-langkah berikut perlu diambil dalam memastikan peralatan ICT dilupuskan dengan teratur iaitu: a. Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data dan maklumat dalam storan telah dihapuskan dengan cara yang selamat; b. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; c. Peralatan ICT yang hendak dilupuskan perlu disimpan di tempat yang telah dikhaskan dengan ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;	Pentadbir ICT Pegawai Aset

d. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset (SPA); e. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; f. Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; ii. Mencabut, menanggalkan dan menyimpan komponen dalaman CPU seperti RAM, *Hard Disk*, *Motherboard* dan sebagainya; iii. Menyimpan dan memindahkan peralatan tambahan komputer seperti UPS, *speaker* atau mana-mana peralatan yang berkaitan ke mana-mana lokasi lain; iv. Membawa keluar dari pejabat mana-mana peralatan ICT yang hendak dilupuskan; dan v. Melupuskan sendiri peralatan ICT tanpa melalui prosedur pelupusan yang ditetapkan. g. Sekiranya maklumat perlu disimpan, pengguna boleh membuat salinan.	Pengguna

0503 Keselamatan Persekitaran

050301 Kawalan Persekitaran

Bagi mengelakkan kerosakan terhadap aset ICT Jabatan, semua cadangan berkaitan urusan perolehan, penyewaan atau pengubahsuaian premis dan aset ICT hendaklah dirujuk terlebih dahulu kepada pegawai yang bertanggungjawab. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: a. Merancang dan menyediakan pelan keseluruhan susun atur ruang pejabat yang menempatkan pusat data, bilik percetakan, peralatan komputer dan sebagainya dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dilihat dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran aset ICT yang berkaitan; dan g. Semua peralatan perlindungan keselamatan hendaklah diurus, diselenggara dan dipantau secara berkala bagi memastikan ia dapat berfungsi dengan baik. Aktiviti ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	Pengguna

050302 Pendawaian

Pendawaian komputer hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada sebarang kerosakan yang disengajakan atau tidak disengajakan; dan c. Membuat pelabelan kabel dengan jelas dan mestilah melalui laluan *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Pengurus ICT Pentadbir ICT

050303 Bekalan Kuasa

Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.	Pengurus ICT Pentadbir ICT

050304 Prosedur Kecemasan

Bagi menjamin keselamatan, pengguna perlu mengambil langkah-langkah berikut: a. Hendaklah membaca, memahami dan mematuhi prosedur kecemasan sedia ada yang berkuatkuasa; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada pegawai yang berkenaan.	Pengguna

0504 Keselamatan Dokumen dan Sistem Dokumentasi

050401 Dokumen

Bagi memastikan integriti maklumat, pengguna perlu mengambil langkah-langkah berikut: a. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b. Mengawal dan merekodkan aktiviti capaian dokumen sedia ada; c. Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; d. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur Arahan Keselamatan; e. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; f. Pelupusan dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Arkib Negara Malaysia; dan g. Menggunakan penyulitan (*encryption*) atas dokumen terperingkat yang disediakan dan dihantar secara elektronik.	Pengguna

PERKARA 06 – PENGURUSAN OPERASI DAN KOMUNIKASI

Objektif	
Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan tepat, lancar dan selamat daripada sebarang ancaman dan gangguan.	
KENYATAAN	**TINDAKAN**

0601 Pengurusan Prosedur Operasi

060101 Pengendalian Prosedur

Perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur keselamatan ICT Jabatan yang di wujudkan hendaklah didokumenkan, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.	ICTSO

060102 Kawalan Perubahan

Perkara yang perlu dipatuhi adalah seperti berikut: a. Pengubahsuaian yang melibatkan peralatan, sistem aplikasi, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai yang berkenaan atau pemilik aset ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyenggara, menghapus dan mengemas kini mana-mana komponen ICT hendaklah dikendalikan oleh pegawai yang berkelayakan dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;	Pengguna

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

060103 Pengasingan Tugas dan Tanggungjawab

Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahan yang tidak dibenarkan atas aset ICT. Perkara yang perlu dipatuhi adalah seperti berikut: a. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan b. Platform yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari peralatan yang digunakan sebagai platform pelaksanaan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan pembangun, operasi dan rangkaian.	Pengurus ICT

0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

060201 Perkhidmatan Penyampaian

Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh Pihak Ketiga; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh Pihak Ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan	Pengguna

c. Pengurusan perubahan dasar perlu mengambilkira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risko.	

0603 Perancangan dan Penerimaan Sistem Aplikasi

060301 Perancangan Kapasiti

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

060302 Penerimaan Sistem Aplikasi

Perkara yang perlu dipatuhi adalah seperti berikut: a. Semua sistem aplikasi baharu (termasuk sistem aplikasi yang dinaik taraf) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui; b. Sebarang penyerahan atau penerimaan sistem aplikasi baharu perlu mendapat pengesahan/kelulusan pemilik sistem; dan c. Penyelenggaraan sistem adalah berdasarkan manual operasi dan prosedur yang ditetapkan.	Pentadbir ICT

0604 Perisian Berbahaya

060401 Perlindungan dari Perisian Berbahaya

Perkara yang perlu dipatuhi adalah seperti berikut: a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti *anti-virus, anti-spyware, anti-spam, content filtering, web reputation dan Intrusion Prevention System* (IPS) dan sebagainya serta mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang tulen; c. Mengimbas semua data, perisian, sistem aplikasi dan media storan dengan perisian keselamatan yang bersesuaian sebelum menggunakannya; d. Mengemaskini perisian keselamatan dari semasa ke semasa; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua sistem aplikasi yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	ICTSO Pentadbir ICT Pengguna

060402 Perlindungan dari Medium Mudah Alih

Penggunaan Medium Mudah Alih hendaklah dirancang, diuji dan dikawal. Pengunaan Medium Mudah Alih yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pengguna

0605 Pengemasan (*Housekeeping*)

060501 Sistem Sandar (*Backup*)

Bagi memastikan sistem aplikasi beroperasi semula setelah berlakunya bencana, salinan penduaan hendaklah dilakukan setiap kali konfigurasi berubah. Rekod salinan penduaan hendaklah disimpan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat salinan keselamatan atas semua konfigurasi dan tetapan pada sistem aplikasi dan perisian sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan; c. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d. Penduaan hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan penduaan bergantung pada tahap kritikal maklumat; e. Menyimpan sekurang-kurangnya tiga (3) generasi data penduaan; dan f. Merekod dan menyimpan salinan penduaan di lokasi yang berlainan dan selamat selaras dengan peraturan semasa.	Pentadbir ICT

0606 Pengurusan Rangkaian

060601 Kawalan Infrastruktur Rangkaian

Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin bagi melindungi ancaman kepada perisian dan sistem aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan: a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran, habuk dan lain-lain; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. Semua peralatan rangkaian hendaklah dipastikan lulus piawaian yang ditetapkan oleh SIRIM atau agensi piawaian antarabangsa semasa dikeluarkan serta melalui proses ujian penerimaan selepas pemasangan dan konfigurasi; e. Peralatan rangkaian harus diselenggara secara berkala oleh kakitangan atau pihak yang dibenarkan sahaja; f. Semua capaian kepada internet dan sistem aplikasi hendaklah melalui *firewall*; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO Jabatan; h. Memasang dan mengkonfigurasi secara optimum *Intrusion Intrusion Detection System* (IDS) dan *Prevention System* (IPS) bagi mengesan serta menghalang sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem aplikasi dan maklumat Jabatan; i. Memasang *Web Content Filtering* pada *Internet Gateway* untuk memantau dan/atau menyekat aktiviti yang dilarang;	ICTSO Pentadbir ICT

j. Semua pengguna hanya dibenarkan menggunakan rangkaian Jabatan sahaja dan sebarang penyambungan rangkaian yang bukan di bawah kawalan Jabatan hendaklah mendapat kebenaran ICTSO; k. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan yang bersesuaian dengannya; dan l. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	

0607 Pengurusan Media

060701 Penghantaran dan Pemindahan

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Pengarah/CIO/pegawai yang diberi kuasa terlebih dahulu.	Pengguna

060702 Prosedur Pengendalian Media

Perkara yang perlu dipatuhi adalah seperti berikut: a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Mengehadkan dan menentukan capaian media kepada pengguna yang sah sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat terperingkat dan rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang ditetapkan.	Pentadbir ICT

060703 Keselamatan Sistem Dokumentasi

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan aktiviti capaian ke atas dokumentasi.	Pentadbir ICT

0608 Pengurusan Mel Elektronik (E-mel)

060801 Kawalan Pengendalian E-mel

Penggunaan e-mel Jabatan hendaklah dipantau secara berterusan untuk memenuhi keperluan etika penggunaan e-mel dan Internet. Antara prosedur-prosedur pengendalian e-mel termasuk: a. Mengehadkan jenis fail lampiran bagi tujuan mengelakkan serangan virus atau *scammer*; b. Menetapkan had minimum kuota mailbox di mana saiz e-mel (mailbox) setiap pengguna adalah bergantung kepada kapasiti yang telah ditetapkan oleh MyGovUC MAMPU; c. Memantau penggunaan e-mel Jabatan secara berterusan; d. Menyediakan akaun e-mel kepada warga Jabatan sahaja melalui prosedur yang ditetapkan; e. Bahagian Sumber Manusia dan Pentadbiran Jabatan perlu memaklumkan sebarang status pengguna (bertukar Jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke Jabatan bagi tujuan pengemaskinian e-mel yang terlibat atau mengikut keperluan Jabatan; f. Menyekat atau membatalkan capaian penggunaan e-mel bagi aktiviti *spamming*, penyebaran virus, bahan-bahan negatif dan surat berantai yang dilakukan oleh pengguna akaun e-mel Jabatan;	Pentadbir ICT

g. Capaian e-mel pengguna yang tidak lagi berkhidmat di Jabatan akan dihentikan; dan h. Pentadbir ICT berhak memasang sebarang jenis perisian atau peralatan penapisan e-mel dan virus yang difikirkan sesuai dan boleh menggunakannya untuk mencegah, menapis, menyekat atau menghapuskan mana-mana e-mel yang disyaki mengandungi virus atau berunsur *spamming* daripada memasuki komputer.	

060802 Penggunaan E-mel

Penggunaan e-mel Jabatan hendaklah memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan” dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut : a. Akaun atau alamat e-mel yang diperuntukkan oleh Jabatan sahaja boleh digunakan untuk kegunaan rasmi. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. Penggunaan e-mel rasmi bagi tujuan peribadi adalah tidak dibenarkan; c. Setiap e-mel yang disediakan perlu mematuhi format yang telah ditetapkan oleh Jabatan; d. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perbincangan yang sama, sebelum penghantaran dilakukan; e. Penghantar hendaklah memastikan alamat e-mel penerima adalah betul; f. Dokumen terperingkat yang diterima melalui e-mel hendaklah segera dipindahkan ke storan kedua dan diberikan perlindungan yang sewajarnya;	Pengguna

g. Penggunaan fail kepilan (*attachment*) dibuat sekiranya perlu, tidak melebihi yang ditetapkan oleh Pentadbir ICT semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; h. Penghantaran lampiran dalam format/*extension* "*.exe, *.bat, *.hta, *.cmd dan *.com" tidak dibenarkan; i. Mengelak dari membuka e-mel dan fail kepilan daripada penghantar yang tidak diketahui atau diragui; j. Mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; k. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; l. E-mel yang tidak penting dan dan tidak diperlukan lagi bolehlah dihapuskan; m. Pengguna adalah bertanggungjawab untuk mengurus dan memastikan saiz e-mel yang disimpan di dalam peti mail (*mailbox*) masing-masing tidak melebihi kuota yang telah ditetapkan; n. Memastikan tarikh dan masa sistem komputer adalah tepat berdasarkan *Malaysian Standard Time* oleh SIRIM; o. Fungsi *Auto-Reply* adalah tidak dibenarkan kecuali pengguna yang bercuti atau bertugas di luar pejabat iaitu dengan menggunakan mesej *Out-of-Office*; dan p. Pengguna adalah mewakili dirinya sendiri dan bertanggungjawab ke atas maklumat yang dikeluarkan dalam setiap perhubungan yang dibuat secara elektronik.	

0609 Pemantauan

060901 Pengauditan dan Forensik ICT

ICTSO mestilah bertanggungjawab merekod dan menganalisis: a. Sebarang percubaan pencerobohan kepada sistem Jabatan; b. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery*, *phising*), pencerobohan (*intrusion*) ancaman (*threats*) dan kehilangan fizikal (*physical loss*); c. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sistem aplikasi 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 lebar jalur (*bandwidth)* rangkaian; g. Aktiviti penyalahgunaan akaun e-mel; dan h. Aktiviti penukaran Alamat IP *(IP address)* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir ICT. Langkah-langkah yang perlu diambil adalah seperti berikut: a. ICTSO akan menentukan prosedur pengumpulan bahan bukti daripada media storan yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan; b. Proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat; dan c. Sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, laporan khas perlu disediakan. Semua proses dan hasil siasatan adalah SULIT.	ICTSO

060902 Jejak Audit

Jejak audit akan merekodkan semua aktiviti sistem aplikasi. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi perkara berikut: a. Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; b. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; c. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan; Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Akta Arkib Negara. Pentadbir ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir ICT

060903 Sistem Log

Perkara yang perlu dipatuhi adalah seperti berikut: a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO Jabatan.	Pentadbir ICT

060904 Pemantauan Log

Pemantauan log merupakan aktiviti untuk mengesan kesalahan atau penyalahgunaan dalam pemprosesan maklumat. Tindakan yang perlu bagi pemantauan log ialah: a. Merekodkan semua aktiviti yang dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian (log audit); b. Mewujudkan prosedur untuk memantau penggunaan kemudahan memproses maklumat dan hasilnya perlu dipantau secara berkala; c. Maklumat log perlu direkodkan dan dilindungi daripada diubah suai dari sebarang capaian yang tidak dibenarkan; d. Merekod aktiviti pentadbiran dan operator sistem; e. Merekod, menganalisis dan mengambil tindakan bagi kesalahan, kesilapan dan/atau penyalahgunaan; dan f. Menyelaras masa yang berkaitan dengan sistem pemprosesan maklumat dalam Jabatan dengan satu sumber masa yang dipersetujui.	Pentadbir ICT

PERKARA 07 – KAWALAN CAPAIAN

Objektif	
Memahami, mematuhi dan melindungi keperluan keselamatan dalam mencapai dan menggunakan aset ICT Jabatan.	
KENYATAAN	**TINDAKAN**

0701 Dasar Kawalan Capaian

070101 Keperluan Dasar

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	Pentadbir ICT

0702 Pengurusan Capaian Pengguna

070201 Akaun Pengguna

Pengguna adalah bertanggungjawab ke atas aset ICT yang digunakan. Pengguna dan aktiviti yang dilakukan perlu dikenal pasti berdasarkan perkara berikut: a. Akaun yang diperuntukkan sahaja boleh digunakan; b. Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian yang paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan terlebih dahulu; c. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan yang ditetapkan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan	Pentadbir ICT Pengguna

f. Pentadbir ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut : i. Pengguna bercuti panjang; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	

070202 Hak Capaian

Penetapan dan penggunaan atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir ICT

070203 Pengurusan Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai aset ICT mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan 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 secara berkala dan mengikut ketetapan prosedur pengurusan kata laluan yang berkuat kuasa; c. Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara. Kata laluan yang terbaik adalah gabungan antara huruf nombor (alphanumerik) dan aksara khas di mana penggunaan gabungan ini adalah digalakkan; d. Kata laluan hendaklah diingat, disimpan serta tidak boleh dicatat atau didedahkan dengan apa cara sekalipun; e. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;	Pengguna

g. Penukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula hendaklah dikuatkuasakan mengikut kesesuaian sistem; h. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; dan i. Penggunaan semula kata laluan yang telah digunakan sebelumnya hendaklah dielakkan.	

070204 *Clear Desk* dan *Clear Screen*

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Maksud bagi: a. *Clear Desk* iaitu tidak meninggalkan sebarang maklumat penting di atas meja apabila pengguna tidak berada di tempatnya atau tidak meninggalkan sebarang maklumat penting pada peranti lain seperti pengimbas, mesin faksimili, mesin fotostat atau sebagainya; dan b. *Clear Screen* iaitu tidak memaparkan sebarang maklumat penting di paparan skrin apabila pengguna tidak berada di tempatnya. Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut: a. Menggunakan kemudahan *password screen saver* atau mengamalkan amalan log keluar atau *sign out* apabila meninggalkan komputer; b. Maklumat-maklumat penting hendaklah disimpan di dalam laci atau kabinet fail yang berkunci; dan c. Semua dokumen hendaklah diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat atau medium output yang lain sebaik sahaja dokumen tersebut dijana, diterima atau digunakan.	Pengguna

0703 Kawalan Capaian

070301 Capaian Rangkaian

Perkara yang perlu dipatuhi adalah seperti berikut: a. Membenarkan pengguna membuat capaian rangkaian untuk kegunaan rasmi sahaja; b. Hanya warga Jabatan sahaja yang dibenarkan mengguna rangkaian Jabatan. Pengguna luar yang ingin menggunakan kemudahan rangkaian hendaklah mendapat kebenaran Pentadbir ICT; c. Mewujudkan mekanisme pengesahan yang sesuai untuk mengawal capaian pengguna; d. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; dan e. Mewujud dan melaksanakan kawalan pengalihan laluan (*routing control*) untuk memastikan rangkaian boleh diakses oleh pengguna.	Pentadbir ICT

070302 Capaian Jarak Jauh

Perkara yang perlu dipatuhi adalah seperti berikut: a. Penghantaran maklumat yang menggunakan capaian jarak jauh menggunakan kaedah *remote access* perlu dikawal dan dipantau; b. Capaian yang dibuat bagi kerja jarak jauh hendaklah melalui medium atau antara muka yang dibenarkan sahaja; c. Lokasi bagi akses ke aset ICT Jabatan hendaklah dipastikan selamat; d. Tindakan perlindungan hendaklah diambil bagi menghalang pendedahan maklumat dan capaian tidak sah serta penyalahgunaan; e. Pengguna hendaklah memastikan keselamatan maklumat teperingkat terjamin semasa menjalankan kerja secara jarak jauh, terutamanya kerja dilaksanakan melalui rangkaian awam atau komputer guna sama ditempat awam;	Pengguna

f. Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pengurus ICT. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini; g. Untuk mengelakkan capaian terus secara fizikal kepada *server* yang berada di Pusat Data, capaian sistem aplikasi melalui jarak jauh (*remote*) adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada pegawai berkenaan dan perkhidmatan yang dibenarkan sahaja; dan h. Memastikan capaian jarak jauh diputuskan *(log out)*, setelah melaksanakan kerja.	

070303 Capaian Internet

Pengurusan capaian internet merangkumi: a. Penggunaan Internet 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 dalam rangkaian Jabatan; b. Penggunaan Internet hanyalah untuk kegunaan rasmi dan secara berhemah. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; c. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; d. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing*, *video streaming, chat, downloading*) perlu dipertimbangkan bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan; dan e. Jabatan hendaklah mempertimbangkan rangkaian berasingan untuk capaian Internet antara warga dan capaian Internet bagi orang awam melalui kaedah *Virtual LAN* (VLAN) atau lain-lain, termasuk bagi rangkaian tanpa wayar (*wireless*).	Pengurus ICT Pentadbir ICT ICTSO

Perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan apa jua modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; b. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang ditetapkan mengikut senarai tugas; c. Bahan yang diperoleh dari Internet hendaklah ditentukan kesahihan dan ketepatannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; d. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Bahagian sebelum dimuat naik ke Internet atau dihantar secara meluas melalui e-mel; e. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh Jabatan sahaja. f. Pengguna yang dibenarkan dan diberi kuasa sahaja dibenarkan membuat sebaran media berkaitan Jabatan melalui e-mel dan Internet; g. Perisian atau aplikasi yang boleh menyebabkan kesesakan dan mengganggu prestasi capaian Internet seperti perisian/aplikasi perkongsian *peer-to-peer (P2P)* atau lain-lain yang seumpamanya, atau aktiviti seperti memuat naik/turun fail dan aktiviti *media streaming* yang dilaksanakan secara berterusan tanpa kelulusan adalah tidak dibenarkan. Pentadbir Rangkaian boleh memutus dan menyekat aktiviti ini bagi memastikan kelancaran operasi Jabatan.	Pengguna

h. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut : i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik dan video/audio/multimedia yang boleh menjejaskan tahap capaian Internet dan prestasi peralatan ICT; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan kandungan serta melibatkan diri secara sosial melalui teks ucapan, komen atau apa jua cara/bahan yang mengandungi unsur-unsur fitnah, hasutan, lucah dan/atau melanggar dasar-dasar semasa Kerajaan. i. Pengguna hendaklah berhenti, menutup aplikasi dan memutuskan talian dengan serta merta sekiranya menerima dan/atau disambungkan ke laman Internet yang mengandungi unsur-unsur tidak menyenangkan atau tidak dibenarkan.	

070304 Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan b. Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Jabatan; b. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;*	Pentadbir ICT ICTSO

c. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; dan d. Menyediakan tempoh penggunaan mengikut kesesuaian. Perkara yang perlu dipatuhi termasuk 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 dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna; c. Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; d. Mengehadkan dan mengawal penggunaan program utiliti yang berkemampuan bagi satu tempoh yang ditetapkan; dan e. Menghadkan tempoh sambungan ke aplikasi berisiko tinggi.	

070305 Capaian Sistem Aplikasi

Capaian sistem aplikasi di Jabatan adalah terhad kepada pengguna dan tujuan yang dibenarkan. Ini bagi memastikan kawalan capaian sistem aplikasi adalah kukuh. Perkara yang perlu dipatuhi adalah seperti berikut : a. Pengguna hanya boleh menggunakan sistem aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem aplikasi pengguna hendaklah direkodkan (*log*) bagi mengesan aktiviti-aktiviti yang tidak diingini;	Pentadbir ICT ICTSO

c. Menghadkan tiga (3) kali percubaan sahaja bagi capaian sistem aplikasi. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; d. Melaksanakan *time out* secara automatik bagi situasi tertentu dalam penggunaan sistem aplikasi; dan e. Memastikan kawalan sistem aplikasi adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah.	

0704 Peralatan Mudah Alih

070401 Penggunaan Peralatan Mudah Alih

Perkara yang perlu dilaksanakan adalah seperti berikut: a. Mengambil kira dan mempertimbangkan peralatan berasaskan *Trusted Platform Module* (TPM), dikonfigurasi secara optimum dan diaktifkan semasa membuat perolehan ICT; b. Pentadbir ICT hanya menyediakan sokongan terhad ('reasonable endeavors') kepada pengguna bagi tujuan konfigurasi, tetapan dan penggunaan peralatan mudah alih bagi capaian ke sistem aplikasi yang dibenarkan untuk urusan rasmi sahaja; c. Memasang dan menggunakan kata laluan bagi mengelakkan akses yang tidak dibenarkan; d. Memasang dan menggunakan perisian keselamatan ICT seperti anti-virus pada peralatan mudah alih; e. Merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan pergerakan perkakasan tersebut daripada kehilangan atau kerosakan; dan f. Mengaktifkan kemudahan 'remote wipe' (sekiranya ada) bagi memadam maklumat Kerajaan dari peralatan mudah alih sekiranya berlaku perkara tidak diingini.	Pentadbir ICT ICTSO
Perkara yang perlu dilaksanakan adalah seperti berikut : a. Melaporkan kehilangan peralatan mudah alih kepada ICTSO; dan b. Menyimpan dan mengunci peralatan mudah alih di tempat yang selamat apabila tidak digunakan;	Pengguna

PERKARA 08 – PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM APLIKASI

Objektif	
Memastikan sistem aplikasi yang dibangunkan sendiri atau oleh pihak luar mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
KENYATAAN	**TINDAKAN**

0801 Keselamatan Dalam Membangunkan Sistem Aplikasi

080101 Keperluan Keselamatan

Perkara yang perlu dipatuhi adalah seperti berikut: a. Pembangunan sistem aplikasi harus mengambil kira keperluan aspek keselamatan yang ditetapkan pada setiap peringkat perolehan, pembangunan dan penyelenggaraan bagi memastikan tidak wujud sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan seperti berikut: i. Sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan; ii. Sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna; dan iii. Sistem output untuk memastikan data yang telah diproses adalah tepat. c. Semua sistem aplikasi yang dibangunkan sama ada secara dalaman (*inhouse*) atau luaran (*outsource*) hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan mematuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan. Ujian tahap keselamatan harus merangkumi Penilaian Keterdedahan (Vulnerability Assessment) oleh pihak berkenaan sebelum pengaktifan sistem.	Pentadbir ICT ICTSO

0802 Kriptografi

080201 Penyulitan *(Encryption)*

Pengguna hendaklah membuat penyulitan (*encryption*) atas maklumat terperingkat pada setiap masa berdasarkan kepada prosedur, tatacara dan Arahan Keselamatan.	Pengguna

080202 Pengurusan Infrastruktur Kunci Awam (PKI)

a. Pengurusan PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut. b. Penggunaan sijil atau tandatangan digital adalah mengikut keperluan khususnya yang menguruskan transaksi maklumat terperingkat secara elektronik.	Pengguna

0803 Fail Sistem

080301 Kawalan Fail Sistem

Perkara yang perlu dipatuhi adalah seperti berikut : a. Proses pengemas kini fail sistem hanya boleh dilakukan oleh Pentadbir ICT atau pegawai yang dibenarkan dan mengikut prosedur yang telah ditetapkan; b. Kod atau atur cara sistem aplikasi yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian atas kod atau atur cara program bagi mengelakkan kerosakan, pengubah suaian tanpa kebenaran, penghapusan dan kecurian; d. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan e. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir ICT

0804 Keselamatan Dalam Proses Pembangunan dan Sokongan

080401 Pengurusan Kawalan Perubahan

Perkara yang perlu dipatuhi adalah seperti berikut : a. Perubahan atau pengubahsuaian pada sistem aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b. Aplikasi kritikal perlu dikaji semula apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan buruk terhadap operasi dan keselamatan Jabatan; c. Pegawai yang dilantik atau Jawatankuasa tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilaksanakan sama ada secara dalaman atau oleh Pihak Luar; d. Mengawal perubahan dan/atau pindaan atas sistem aplikasi dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; e. Akses kepada kod sumber *(Source Code)* sistem aplikasi adalah dihadkan kepada pengguna yang dibenarkan sahaja; dan f. Menghalang sebarang peluang untuk membocorkan maklumat.	Pentadbir ICT

080402 Pembangunan Secara *Outsource*

a. Pembangunan sistem aplikasi secara *outsource* perlu dipantau oleh pemilik sistem. b. *Source code* adalah hak milik Jabatan.	Pengurus ICT Pentadbir ICT

0805 Kawalan Keterdedahan Teknikal

080501 Kawalan Dari Ancaman Teknikal

Kawalan keterdedahan teknikal perlu dilaksanakan atas sistem pengoperasian dan sistem aplikasi. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b. Menilai tahap pendedahan bagi mengenalpasti tahap risiko yang bakal dihadapi; dan c. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	ICTSO Pentadbir ICT

PERKARA 09 – PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

Objektif
Memastikan insiden dikendalikan dengan cepat, tepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT

KENYATAAN	TINDAKAN

0901 Pengurusan Insiden Keselamatan ICT

090101 Insiden Keselamatan ICT

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan seterusnya kepada CERT Jabatan dengan kadar segera: a. Maklumat didapati hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Aset ICT digunakan tanpa kebenaran; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.	Pengguna

090102 Mekanisme Pelaporan Insiden Keselamatan ICT

Sekiranya berlaku insiden keselamatan ICT, maka mekanisme pelaporan adalah berdasarkan prosedur berikut: a. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi”; dan b. Surat Pekeliling Am Bilangan 4 Tahun 2006 bertajuk “Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam”. Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT adalah seperti di **LAMPIRAN C**.	ICTSO CERT

090103 Pengurusan Maklumat Insiden Keselamatan ICT

Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran. Ini untuk mengawal kekerapan, kerosakan dan kos kejadian insiden yang berlaku. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada Jabatan. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan maklumat insiden adalah seperti berikut: a. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; b. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c. Menyediakan pelan kontigensi dan mengaktifkan pelan Pengurusan Kesinambungan Perkhidmatan (PKP); d. Menyediakan tindakan pemulihan segera; dan e. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO CERT

PERKARA 10 – PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Objektif	
Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
KENYATAAN	**TINDAKAN**

1001 Dasar Kesinambungan Perkhidmatan

100101 Pelan Pengurusan Kesinambungan Perkhidmatan

Pelan Pengurusan Kesinambungan Perkhidmatan (PKP) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT atau jawatankuasa berkaitan. Perkara berikut yang perlu diberi perhatian : a. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap perkhidmatan atau proses kerja, kemungkinan serta impak gangguan, penilaian kegagalan keselamatan dan kerugian dalam perkhidmatan akibat gangguan harus dianalisa; c. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; d. Mendokumentasikan proses dan prosedur yang telah dipersetujui; e. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; f. Membuat penduaan; dan	CIO

g. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. Jabatan bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT Jabatan.	

PERKARA 11 – PEMATUHAN

Objektif	
Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran DKICT J-KOM, memastikan kelancaran operasi.	
KENYATAAN	**TINDAKAN**

1101 Pematuhan dan Keperluan Perundangan

110101 Pematuhan Dasar, Piawaian dan Keperluan Teknikal

ICTSO perlu memastikan: a. Semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. b. Aset ICT perlu melalui pemeriksaan secara berkala bagi mematuhi piawaian pelaksanaan keselamatan dan amalan terbaik industri.	ICTSO
Pematuhan dasar, piawaian dan keperluan teknikal penting dalam memastikan keselamatan ICT terjamin. Beberapa perkara yang perlu diberi perhatian oleh Pengguna iaitu: a. Pengguna di Jabatan hendaklah membaca, memahami dan mematuhi DKICT J-KOM dan undang-undang atau peraturan lain berkaitan ICT yang berkuat kuasa. b. Aset ICT Jabatan termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. c. Sebarang penggunaan aset ICT Jabatan selain daripada maksud dan tujuan yang ditetapkan adalah merupakan satu penyalahgunaan sumber ICT Jabatan serta merupakan suatu pelanggaran dasar.	Pengguna

110102 Pematuhan Keperluan Audit

Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit aset ICT. Keperluan audit dan sebarang aktiviti pemeriksaan atas Aset ICT perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian atas aset ICT yang diaudit perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Pengguna

110103 Keperluan Perundangan

Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi adalah seperti di **LAMPIRAN E.**	Pengguna

1102 Tindakan Tatatertib

110201 Pelanggaran Dasar / Perundangan

Pelanggaran DKICT J-KOM akan dikenakan tindakan undang-undang dan tatatertib di bawah Akta Rahsia Rasmi 1972 dan Perintah-Perintah Am Bab D – Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib).	Pengguna

GLOSARI

Anti-Spam	Perisian yang bertujuan untuk mengesan dan menyekat e-mel yang berpotensi berbahaya daripada peti masuk pengguna.
Anti Spyware	Berkaitan dengan perisian yang direka untuk mengesan dan mengalih keluar perisian pengintip.
Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, Compact Disc Read-Only Memory (CDROM) untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Auto Reply	Fungsi perisian emel yang secara automatik menghantar respon penghantar dengan mengikut konfigurasi yang ditetapkan.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur - Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CD-Keys	Nombor siri atau kod produk yang merupakan gabungan huruf dan nombor bagi mengaktifkan produk.
CERT J-KOM	Organisasi yang ditubuhkan untuk membantu Jabatan mengurus pengendalian insiden keselamatan ICT di J-KOM.
Chat	Istilah rasmi untuk sembang dalam talian
CIO	*Chief Information Officer* - Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Content Filtering	Dikenali sebagai penapisan maklumat bag menyaring dan mengecualikan daripada akses atau ketersediaan halaman web atau emel yang dianggap tidak menyenangkan.
Denial of Service	Halangan pemberian perkhidmatan.

DKICT J-KOM	Dasar Keselamatan ICT J-KOM dan terpakai kepada Jabatan.
Downloading	Aktiviti muat-turun data.
Encryption	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft / espionage*), penipuan(*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Pengendali Insiden Keselamatan ICT Kerajaan.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab 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.
Inhouse	Pembangunan Sistem yang dibangun dengan menggunakan kepakaran dan tenaga kerja dalaman.
Instant Messaging	Perisian pada peranti yang membenarkan komunikasi dua hala menggunakan perkhidmatan Internet sebagai medium penghantaran data.

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)	Peranti atau aplikasi perisian yang memantau rangkaian atau sistem untuk aktiviti berniat jahat atau pelanggaran dasar.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan - Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian atau aktiviti yang berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan. Contohnya, *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
J-KOM	Jabatan Komunikasi Komuniti
LAN	*Local Area Network* - Rangkaian Kawasan Setempat yang menghubungkan komputer.
Linux	Perisian yang mempunyai sumber terbuka di mana kodnya adalah bebas.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
Media Sosial	Media dalam talian yang membenarkan pengguna bersosial, bersembang dan berhubung. Contohnya *Facebook*, *Twitter*, *Instagram* dan lain-lain.
Modem	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.

Motherboard	Papan litar utama yang menempatkan komponen elektronik unit sistem temasuk kadar *adapters*, pemproses dan cip memori.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Peer-to-peer	Satu koleksi peralatan (komputer) yang berfungsi bersama menggunakan saluran komunikasi tanpa komputer utama.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau Jabatan.
Phishing	Sejenis kejuruteraan sosial di mana penyerang menghantar mesej penipuan yang direka untuk menipu seseorang supaya mendedahkan maklumat senstif kepada pemangsa.
Pihak Ketiga	Kontraktor, Pembekal, Pakar Runding dan pihak-pihak lain yang berkepentingan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Public Cloud Storage	Perkhidmatan storan data dalam talian sama ada yang disediakan secara percuma atau berbayar. Lazimnya digunakan untuk menyimpan data untuk membolehkan ia dicapai dengan mudah melalui peranti yang mempunyai sambungan Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Scam	Helah atau penipuan bagi mencuri maklumat atau data.
Sreen saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.

Server	Pelayan komputer
Smartphone	Telefon pintar yang mempunyai ciri-ciri kalendar, buku telefon, kamera, storan, pelbagai aplikasi dan kebolehan untuk mencapai maklumat dan perkhidmatan di Internet.
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 perlanggaran yang berlaku.
Tablet	Peranti pintar yang menyamai rupa dan fungsi *Smartphone.*
Threats	Gangguan dan ancaman secara aktif atau pasif melalui pelbagai cara termasuk pesanan ringkas, e-mel dan surat yang bermotif peribadi dan atas sebab tertentu atau tindakan-tindakan zahir yang membawa maksud yang sama.
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 Conferencing	Media yang menerima serta memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

LAMPIRAN A

JABATAN PERDANA MENTERI
JABATAN KOMUNIKASI KOMUNITI

AKUAN PEMATUHAN DASAR KESELAMATAN ICT JABATAN KOMUNIKASI KOMUNITI (J-KOM)

Nama : …….....
(Huruf Besar)

No. Kad Pengenalan : …….....

Jawatan : …….....
(Huruf Besar)

Bahagian / Syarikat : …….....
(Huruf Besar)

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya juga telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT J-KOM; dan

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

.....
(Tandatangan)

Tarikh : .....

Pengesahan Ketua Jabatan

.....
(**DATO' DR. ZURAIDI BIN ISHAK**)
Ketua Pengarah
Jabatan Komunikasi Komuniti

Tarikh : .....

*Sekiranya Syarikat sila lampirkan satu (1) salinan MyKAD.

LAMPIRAN B

AKTA RAHSIA RASMI
[Akta 88]

PERAKUAN UNTUK DITANDATANGANI OLEH MEREKA YANG BUKAN PENJAWAT AWAM/PAKAR PERUNDING BERKENAAN 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, sesuatu benda rahsia Kerajaan, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkah laku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

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

Tandatangan : .....

Nama : .....

No.Kad Pengenalan : .....

Jawatan : .....

Jabatan/Organisasi : .....

Tarikh : .....

Disaksikan Oleh : .....
(Tandatangan)

Nama : .....

No. Kad Pengenalan : .....

Jawatan : .....

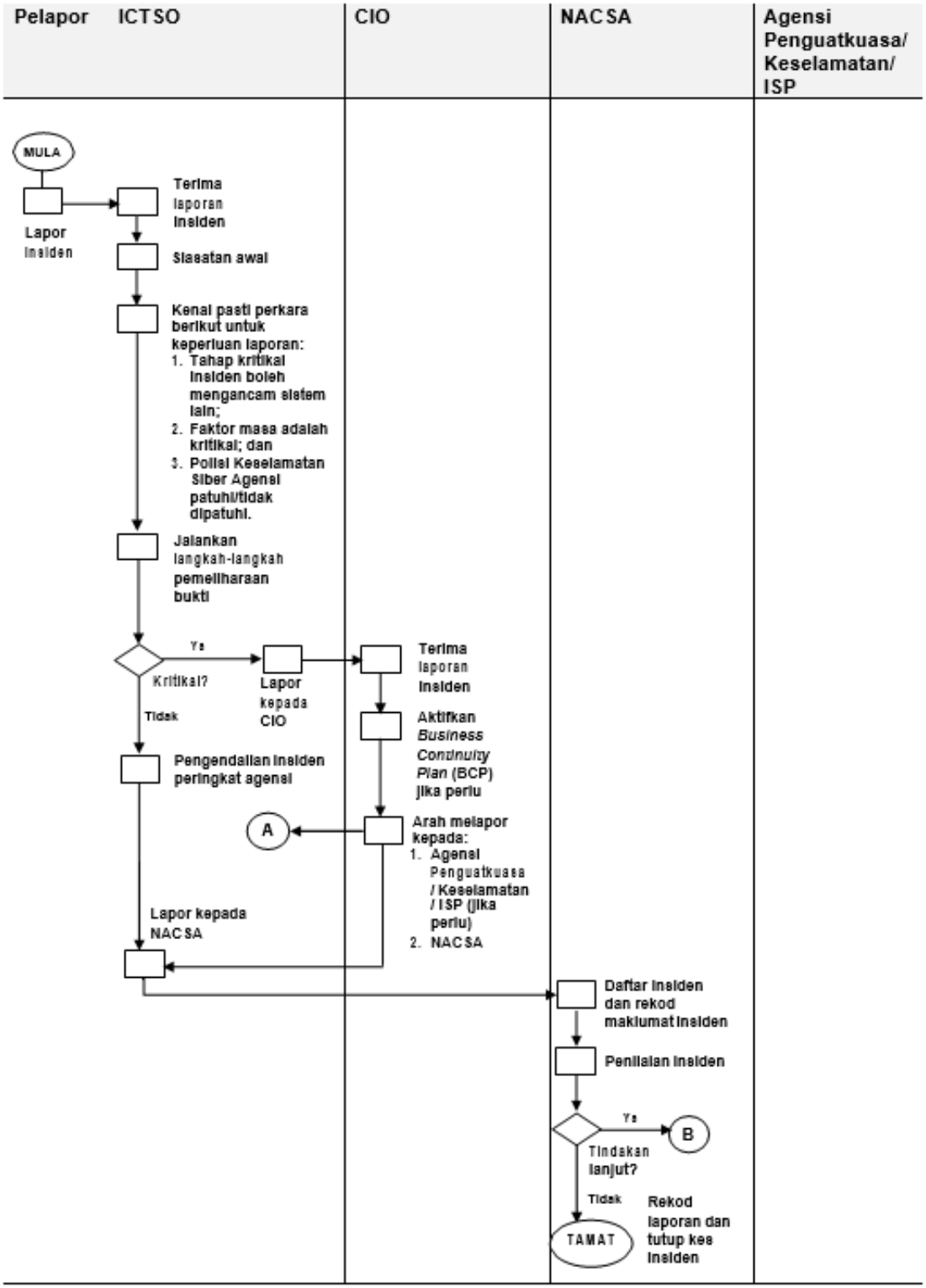
Jabatan/Organisasi : .....

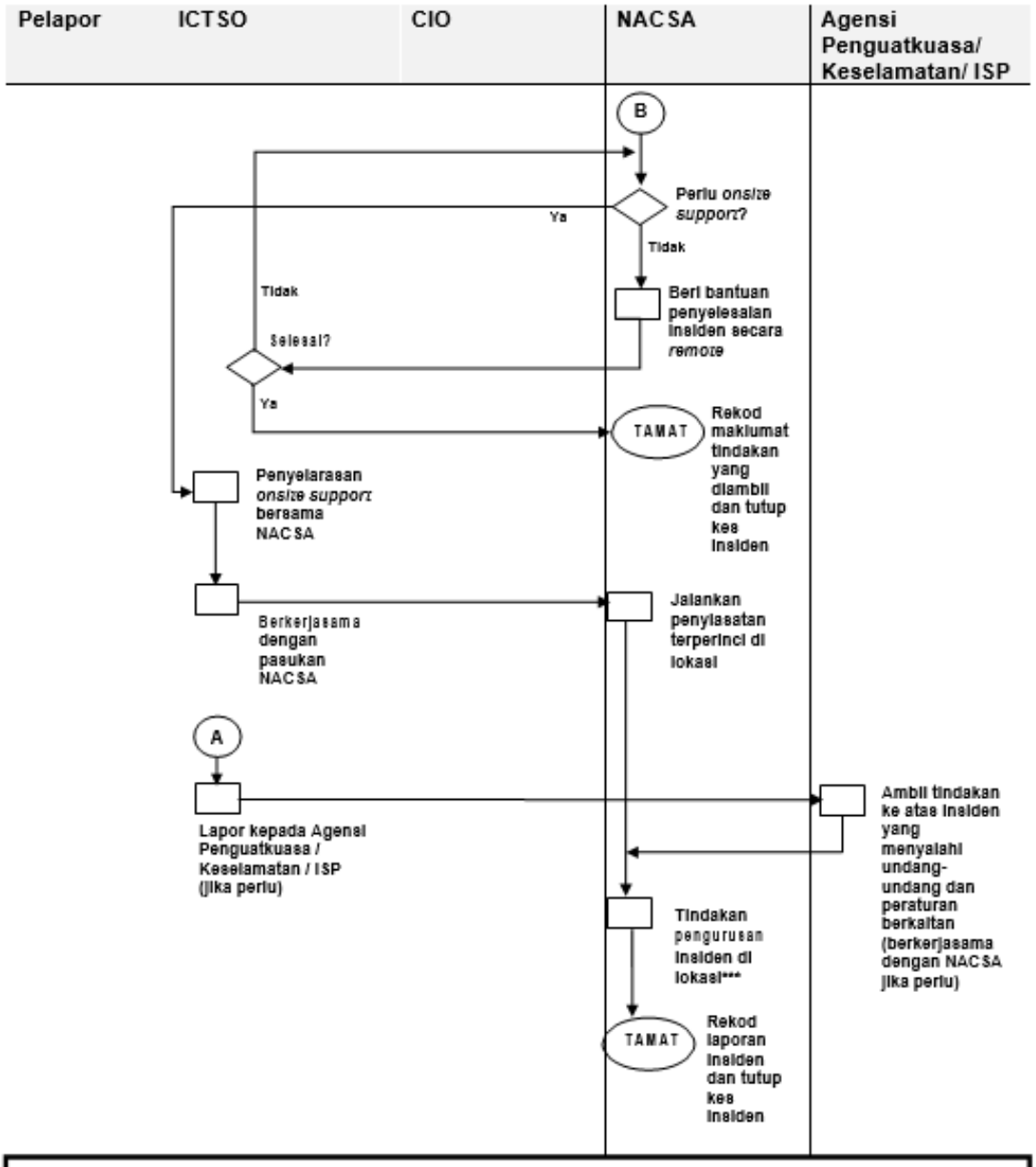
Tarikh : .....

Cop Jabatan/Organisasi: .....

LAMPIRAN C

CARTA ALIR
RINGKASAN PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT





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

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

LAMPIRAN D

BORANG PERGERAKAN ASET

JABATAN PERDANA MENTERI
JABATAN KOMUNIKASI KOMUNITI

JABATAN KOMUNIKASI KOMUNITI (J-KOM)
Bahagian Teknologi Maklumat
Aras 7, Setia Perdana 3, Kompleks Setia Perdana
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya

Nama: .....

Jabatan/Syarikat: .....

No. Kenderaan: . .....

Tujuan: .....

SENARAI BARANG YANG DIBAWA KELUAR

No. Siri Pendaftaran	Keterangan Aset	Tarikh

…….....
Tandatangan Pihak Pembekal

…….....
Tandatangan Pengawal Keselamatan

Disahkan oleh:

……
Nama:
Jab./Bhg./Unit:
Tarikh:

***Nota :**
Pihak Tuan hendaklah menentukan dan memastikan barangan yang dikeluarkan mempunyai kebenaran bertulis. Sekiranya tiada, ia boleh dianggap barangan curi dan boleh dirampas.

LAMPIRAN E

SENARAI PERUNDANGAN DAN PERATURAN

1. Arahan Keselamatan;

2. Surat Pekeliling Am Bilangan 2 Tahun 2000 bertajuk "Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK)" dan pindaannya;

3. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";

4. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)";

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

6. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi- agensi Kerajaan";

7. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam";

8. Surat Pekeliling Am Bilangan 4 Tahun 2006 bertajuk "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam";

9. Surat Pekeliling Perbendaharaan Bilangan 8 Tahun 2006 bertajuk "Peraturan Perolehan Perkhidmatan Perunding";

10. Pekeliling Am Bilangan 1 Tahun 2006 bertajuk "Pengurusan Laman Web/Portal Sektor Awam";

11. Surat Arahan Ketua Setiausaha Negara dengan rujukan UPTM(S)159/338/8 Jilid 30 (84) bertajuk "Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-Agensi Kerajaan" bertarikh 20 Oktober 2006;

12. Surat Arahan MAMPU bertajuk "Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan" bertarikh 1 Jun 2007;

13. Surat Arahan MAMPU bertajuk "Langkah-langkah Pemantapan Pelaksanaan Mel Elektronik di Agensi-Agensi Kerajaan" bertarikh 23 November 2007;

14. Surat Pekekliling Am Bilangan 3 Tahun 2009 bertajuk “Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam” bertarikh 17 November 2009;

15. Surat Arahan Ketua Pengarah MAMPU bertajuk “Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam” bertarikh 22 Januari 2010;

16. Akta Rahsia Rasmi 1972;

17. Akta Tandatangan Digital 1997;

18. Akta Jenayah Komputer 1997 (Akta 563);

19. Akta Hak Cipta (Pindaan) Tahun 1997;

20. Akta Komunikasi dan Multimedia 1998 (Akta 588) ;

21. Arahan Teknologi Maklumat 2007;

22. Akta-Akta dan Garis Panduan berkaitan Jabatan;

23. Perintah-Perintah Am;

24. Arahan Perbendaharaan; dan

25. *Standard Operating Procedure* (SOP) ICT J-KOM.

DASAR KESELAMATAN ICT
J-KOM

Jabatan Komunikasi Komuniti (J-KOM)
Aras 7, Setia Perdana 3, Kompleks Setia Perdana
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA