KEMENTERIAN PEMBANGUNAN
USAHAWAN DAN KOPERASI
MINISTRY OF ENTREPRENEUR DEVELOPMENT AND COOPERATIVES

DASAR KESELAMATAN ICT (DKICT)

KEMENTERIAN PEMBANGUNAN USAHAWAN DAN KOPERASI (KUSKOP)

25 MAC 2022

PENGESAHAN DOKUMEN			
DILULUSKAN OLEH:			
NAMA	**JAWATAN**	**TARIKH**	**TANDATANGAN**
YBhg. Dato' Suriani binti Dato' Ahmad	**Ketua Setiausaha**		

SEJARAH DOKUMEN

VERSI	KELULUSAN	TARIKH KUATKUASA
1.0	KSU	JANUARI 2020
2.0	KSU	MAC 2022

ISI KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT (DKICT) Kementerian Pembangunan Usahawan dan Koperasi (KUSKOP) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) KUSKOP. Dasar ini juga menerangkan kepada semua pengguna di KUSKOP mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT KUSKOP. Dasar ini disediakan berpandu kepada piawaian antarabangsa iaitu MS ISO/IEC 27001:2013.

OBJEKTIF

DKICT ini diwujudkan untuk:

a) menjamin kesinambungan perkhidmatan ICT sekiranya berlaku insiden keselamatan;
b) menghalang dan meminimumkan kesan sebarang insiden keselamatan yang berlaku;
c) memastikan ketersediaan, kerahsiaan dan integriti dokumen dan maklumat elektronik bagi melindungi kepentingan pihak-pihak berkepentingan;
d) memastikan akses hanya kepada pengguna yang sah; dan
e) mencegah penyalahgunaan atau kecurian aset ICT KUSKOP.

PERNYATAAN DASAR

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

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyediakan dan membekalkan perkhidmatan yang berasaskan kepada sistem 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 rahsia rasmi dan maklumat rasmi Kerajaan dari capaian tanpa kuasa yang sah;

b) menjamin setiap maklumat adalah tepat dan sempurna;
c) memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
d) memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

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

a) **Kerahsiaan**
Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.
b) **Integriti**
Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan.
c) **Tidak Boleh Disangkal**
Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.
d) **Kesahihan**
Data dan maklumat hendaklah dijamin kesahihannya.
e) **Ketersediaan**
Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

Aset ICT KUSKOP terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. DKICT KUSKOP menetapkan keperluan-keperluan asas berikut:

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

b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan Kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, DKICT KUSKOP ini merangkumi perlindungan semua bentuk maklumat Kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

a) **Perkakasan ICT**

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

b) **Perisian**

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

c) **Perkhidmatan**

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

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

d) **Data atau Maklumat**

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

e) **Manusia**

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

f) **Premis Komputer dan Komunikasi**

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

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

PRINSIP-PRINSIP

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

A. **AKSES ATAS DASAR PERLU MENGETAHUI**

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

B. **HAK AKSES MINIMUM**

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

C. **AKAUNTABILITI**

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

D. **PENGASINGAN**

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

E. **PENGAUDITAN**

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

F. **PEMATUHAN**

DKICT KUSKOP hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelangaran 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 ketidaksedian. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/ kesinambungan perkhidmatan.

H. **SALING BERGANTUNGAN**

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

PENILAIAN RISIKO KESELAMATAN ICT

KUSKOP hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu KUSKOP perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

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

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

KUSKOP bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam. KUSKOP perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a) mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

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

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

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

PERKARA 1
PEMBANGUNAN DAN PENYELENGGARAAN DASAR

1.1 DASAR KESELAMATAN ICT

Objektif:

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

1.1.1 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Ketua Setiausaha (KSU) KUSKOP selaku Pengerusi Jawatankuasa Pemandu ICT (JPICT) KUSKOP, yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Pengarah Bahagian.	KSU

1.1.2 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua pengguna KUSKOP (termasuk kakitangan, pembekal, pakar runding dll.)	ICTSO

1.1.3 Penyelenggaraan Dasar

DKICT KUSKOP 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 KUSKOP: a) kenal pasti dan tentukan perubahan yang diperlukan; b) kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT); c) perubahan yang telah dipersetujui oleh JPICT dimaklumkan kepada semua pengguna; dan d) dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	ICTSO

1.1.4 Pengecualian Dasar

DKICT KUSKOP adalah terpakai kepada semua pengguna ICT KUSKOP dan tiada pengecualian diberikan.	Semua Pengguna

PERKARA 2
ORGANISASI KESELAMATAN

2.1 INFRASTRUKTUR ORGANISASI DALAMAN

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.

2.1.1 Ketua Setiausaha (KSU)

Peranan dan tanggungjawab KSU adalah seperti berikut: a) memastikan semua pengguna memahami peruntukan-peruntukan di bawah DKICT KUSKOP; b) memastikan semua pengguna mematuhi DKICT KUSKOP; c) memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi ; dan d) memastikan penilaian risiko dan program keselamatan ICT dilaksanakan berpandukan kepada garis panduan, prosedur dan langkah keselamatan ICT.	KSU

2.1.2 Ketua Pegawai Maklumat (*Chief Information Officer* – CIO)

Setiausaha Bahagian Kanan (Pengurusan) adalah CIO yang dilantik. Peranan dan tanggungjawab ICTSO adalah seperti berikut : a) melaksanakan tanggungjawab menjaga keselamatan aset ICT berdasarkan Dasar Keselamatan ICT KUSKOP; b) menentukan keperluan keselamatan ICT; dan c) membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT.	Setiausaha Bahagian Kanan (Pengurusan)

2.1.3 Pegawai Keselamatan ICT *(ICT Security Officer - ICTSO)*

Setiausaha Bahagian Pengurusan Teknologi Maklumat (BPTM) adalah ICTSO yang dilantik. Peranan dan tanggungjawab ICTSO adalah seperti berikut : a) menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT KUSKOP; b) menguatkuasakan DKICT KUSKOP; c) memberi penerangan dan pendedahan berkenaan DKICT KUSKOP semua pengguna; d) mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT KUSKOP; e) menjalankan pengurusan risiko; f) menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g) memberi amaran terhadap kemungkinan berlakunya ancaman merbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h) Melaporkan insiden keselamatan ICT kepada NACSA dan memaklumkannya kepada CIO, i) menyelaras atau membantu siasatan berkenaan dengan ancaman atau sebarang serangan lain ke atas aset ICT, j) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan, k) bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera, l) memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar DKICT KUSKOP; dan m) memberikan kebenaran hak akses yang berkaitan keselamatan ICT kepada Warga KUSKOP.	Setiausaha Bahagian BPTM

2.1.4 Pengurus ICT	
Peranan dan tanggungjawab beliau adalah seperti berikut : a) memastikan semua pengguna memahami dan mematuhi DKICT KUSKOP, tatacara dan garis panduan yang dikeluarkan; b) mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan KUSKOP; c) menentukan kawalan akses semua pengguna terhadap aset ICT KUSKOP dan membuat semakan berkala berkenaan hak akses; d) merangka dan menyemak pelan kontingensi KUSKOP; e) melaporkan sebarang masalah berkaitan dengan keselamatan ICT kepada CIO; dan f) menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KUSKOP.	Setiausaha Bahagian BPTM
2.1.5 Pentadbir Sistem ICT	
Pentadbir Sistem ICT terdiri daripada berikut: a) Pentadbir Rangkaian dan Keselamatan; b) Pentadbir Pusat Data; c) Pentadbir Pangkalan Data; d) Pentadbir Laman Web; e) Pentadbir Sistem Aplikasi; dan f) Pentadbir E-mel. **Pentadbir Rangkaian dan Keselamatan** Peranan dan tanggungjawab seperti berikut: a) memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di KUSKOP beroperasi sepanjang masa;	BPTM/BLESS

b) memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna;

c) merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada;

d) mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil;

e) memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian;

f) memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian KUSKOP secara tidak sah seperti melalui peralatan model dan *dial-up;*

g) menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian; dan

h) melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT *(Security Posture Assessment)* serta penilaian risiko keselamatan maklumat.

Pentadbir Pusat Data

Peranan dan tanggungjawab seperti berikut:

a) memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat;

b) memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data;

c) menjadual dan melaksanakan proses *backup* dan *restoration* ke atas pangkalan data dan sistem secara berkala;

d) menyediakan perancangan bencana mengikut prinsip Pengurusan Kesinambungan Perkhidmatan dalam DKICT;

e) melaksanakan prinsip-prinsip DKICT; dan

f) memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan.

Pentadbir Pangkalan Data

Peranan dan tanggungjawab seperti berikut:

a) melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data;

b) memastikan pangkalan data boleh digunakan pada setiap masa;

c) melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data;

d) melaksanakan data *masking* dalam menyediakan data latihan;

e) memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur;

f) melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip DKICT;

g) melaksanakan proses pembersihan data *(housekeeping)* di dalam pangkalan data; dan

h) melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.

Pentadbir Laman Web

Peranan dan tanggungjawab seperti berikut:

a) menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah;

b) memantau prestasi capaian dan menjalankan penilaian prestasi untuk memastikan akses yang lancar;

c) memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman;

d) menghadkan capaian Pentadbir Laman Web bahagian ke *web server*;

e) mengasingkan kandungan dan aplikasi atas talian untuk capaian secara Intranet dan Internet ke portal KUSKOP;

f) memastikan data-data SULIT tidak boleh disalin atau dicetak oleh orang yang tidak berhak;

g) memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi;

h) melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*;

i) melaksanakan proses *backup* dan *restoration* secara berkala; dan

j) melaporkan sebarang pelanggaran keselamatan laman web kepada ICTSO.

Pentadbir Sistem Aplikasi

Peranan dan tanggungjawab seperti berikut:

a) mengkaji cadangan pembangunan atau penyelarasan sistem di KUSKOP;

b) membuat kajian semula serta memperbaiki sistem sedia ada di KUSKOP;

c) membuat pertimbangan dan mengusulkan cadangan pelaksanaan sistem di KUSKOP;

d) membuat pemantauan dan penyelenggaraan terhadap sistem dari semasa ke semasa;

e) bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem;

f) menyediakan dokumentasi sistem dan manual pengguna;

g) memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas;

h) memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya;

i) memastikan *virus pattern, hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemaskini supaya terhindar daripada ancaman virus dan penggodam;

j) mematuhi dan melaksanakan prinsip-prinsip DKICT dalam pewujudan akaun pengguna ke atas setiap sistem aplikasi; k) menghadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan dari penyalahgunaannya; dan l) melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya; **Pentadbir E-mel** Peranan dan tanggungjawab seperti berikut: a) menentukan setiap akaun yang diwujudkan atau dibatalkan mempunyai permohonan dari Bahagian bertanggungjawab. Pembatalan akaun pengguna yang bertukar keluar akan diberi tempoh masa sehingga 14 hari (jika tiada permohonan lanjutan penggunaan). Bagi pengguna yang berhenti dan melanggar dasar dan tatacara KUSKOP perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; b) pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; c) mengesah dan memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan melalui saluran rasmi; d) memastikan kemudahan membuat capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi; dan e) memastikan pengguna e-mel KUSKOP berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel dan internet KUSKOP serta pelaksanaan Kursus Pembudayaan ICT secara berterusan.	
2.1.6 Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti berikut : a) membaca, memahami dan mematuhi DKICT KUSKOP; b) mengetahui dan memahami implikasi keselamatan ICT serta kesan daripada tindakan ketidakpatuhan terhadap DKICT KUSKOP;	Semua Pengguna

c) menjalani tapisan keselamatan; d) melaksanakan prinsip-prinsip DKICT dan menjaga kerahsiaan maklumat KUSKOP; e) melaksanakan langkah-langkah perlindungan seperti berikut: i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. memeriksa maklumat dan menentukan ianya tepat dan lengkap dari masa ke semasa; iii. menentukan maklumat sedia untuk digunakan, iv. menjaga kerahsiaan kata laluan; v. mematuhi standard, prosedur, langkah 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 sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera, g) menghadiri program kesedaran keselamatan ICT; dan h) menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT KUSKOP sebagaimana di Lampiran 1 dan Borang Akta Rahsia Rasmi 1972 seperti di Lampiran 2.	
2.1.7 Jawatankuasa Pemandu ICT KUSKOP	
Jawatankuasa Pemandu ICT (JPICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT KUSKOP. Keanggotaan JPICT KUSKOP adalah seperti berikut: Pengerusi : KSU Ahli :	JPICT KUSKOP

1. Setiausaha Bahagian Kanan / Setiausaha Bahagian / Ketua Unit 2. Ketua Agensi Urusetia : BPTM Bidang Kuasa : a) memperakukan/meluluskan dokumen DKICT KUSKOP; b) memantau tahap pematuhan keselamatan ICT; c) memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam KUSKOP yang mematuhi keperluan DKICT KUSKOP. d) menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; e) memastikan DKICT KUSKOP selaras dengan dasar-dasar ICT semasa Kerajaan; f) menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; g) membincang tindakan yang melibatkan pelanggaran DKICT KUSKOP. h) membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden; dan i) **(g)** dan **(h)** adalah tertakluk kepada tindakan tatatertib.	
2.1.8 Pasukan Tindak Balas Insiden Keselamatan ICT KUSKOP (CERT KUSKOP)	
Keanggotaan adalah seperti berikut: Pengarah CERT KUSKOP : CIO Pengurus CERT KUSKOP : ICTSO Ahli : 1. Ketua Penolong Setiausaha SKA, STICT dan BLESS 2. Penolong Setiausaha Kanan SKA, STICT dan BLESS 3. Penolong Setiausaha SKA, STICT dan BLESS 4. Penolong Pegawai Teknologi Maklumat BPTM dan BLESS Peranan dan tanggungjawab adalah seperti berikut:	

a) Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden;

b) Merekod dan menjalankan siasatan awal insiden yang diterima;

c) Menangani tindak balas *(response)* insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;

d) Mengambil tindakan pemulihan dan pengukuhan; dan

e) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada KUSKOP.

2.1.9 Jawatankuasa Keselamatan ICT KUSKOP

Keanggotaan adalah seperti berikut:

Pengerusi : Setiausaha Bahagian BPTM

Ahli :

1. Ketua SKA, STICT dan BLESS
2. Pentadbir-pentadbir Rangkaian dan Keselamatan, Pusat Data, Pangkalan Data, Laman Web, Sistem Aplikasi dan E-mel BPTM dan BLESS.

Urusetia : STICT, BPTM

Peranan dan tanggungjawab adalah seperti berikut:

a) Menyelenggara dokumen DKICT KUSKOP;

b) Memantau tahap pematuhan DKICT KUSKOP;

c) Merancang, melaksana, menyelaras dan memantau pengurusan keselamatan ICT KUSKOP;

d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;

e) Menjalankan penilaian ke atas tahap keselamatan ICT KUSKOP dan mengambil tindakan pengukuhan atau pemulihan; dan

f) Mengambil tindakan terhadap sebarang insiden yang dilaporkan.

2.2 PIHAK KETIGA

Objektif:

Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Kontraktor, Pembekal dan Penyedia Perkhidmatan Luaran dan lain-lain).

2.2.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga

Pihak ketiga terdiri daripada Kontraktor, Pembekal dan Penyedia Perkhidmatan Luaran. Peranan dan tanggungjawab pihak ketiga adalah bertujuan bagi memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi adalah seperti berikut: a) membaca, memahami dan mematuhi DKICT KUSKOP; b) perlu menandatangani Surat Akuan Pematuhan DKICT KUSKOP seperti di **Lampiran 1**; c) perlu juga menandatangani Perakuan Akta Rahsia Rasmi 1972 bagi perakuan untuk tidak membocorkan sebarang maklumat rasmi yang diperolehi sepanjang tempoh penyampaian perkhidmatan dengan KUSKOP seperti di **Lampiran 2**; d) menyedari implikasi keselamatan ke atas sebarang tindakan yang dilakukan; e) melaporkan dengan segera sebarang aktiviti atau keadaan yang meragukan yang mungkin memberikan ancaman kepada aset maklumat; f) memastikan kerahsiaan maklumat KUSKOP terpelihara; g) mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat seta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; h) mengenalpasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; i) akses kepada aset ICT KUSKOP perlu berlandaskan kepada perjanjian kontrak; j) memastikan semua syarat dan polisi keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai;	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga

a. DKICT KUSKOP; b. Tapisan Keselamatan; c. Perakuan Akta Rahsia Rasmi 1972; dan d. Hak Harta Intelek.	

PERKARA 3
PENGURUSAN ASET

3.1 AKAUNTABILITI ASET

Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT KUSKOP.

3.1.1 Inventori Aset ICT

Perkara ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: a) memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori serta sentiasa dikemaskini; 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 KUSKOP; d) peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumenkan dan dilaksanakan; dan e) setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Semua Pengguna

3.2 Pengelasan dan Pengendalian Maklumat

Objektif:

Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuian.

3.2.1 Kategori Maklumat

Mengenalpasti kategori maklumat merupakan satu langkah penting dalam memastikan perlindungan yang mencukupi dan bersesuaian dengan kategori maklumat berkenaan. Semua maklumat yang dijana atau dikumpul oleh kementerian dan agensi hendaklah diasingkan mengikut kategori Maklumat Rasmi dan Maklumat Rahsia Rasmi. Kedua-dua kategori boleh mengandungi Maklumat Pengenalan Peribadi *(Personal Identifiable Information - PII)*. Data Terbuka juga merupakan sebahagian daripada Maklumat Rasmi. a) Maklumat Rahsia Rasmi Maklumat Rahsia Rasmi mempunyai erti yang diberikan kepadanya di bawah Akta Rahsia Rasmi 1972 [Akta 88]. Apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 [Akta 88] dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972. b) Maklumat Rasmi Maklumat Rasmi adalah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh mana-mana agensi Kerajaan semasa menjalankan urusan rasmi. Maklumat Rasmi ini juga adalah merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara. c) Maklumat Pengenalan Peribadi Maklumat Pengenalan Peribadi PII adalah maklumat yang boleh digunakan secara tersendiri atau digunakan dengan maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu yang juga dikategorikan sebagai Maklumat Rahsia Rasmi. d) Data Terbuka Data Terbuka adalah maklumat yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi Kerajaan dan organisasi swasta untuk pelbagai tujuan. Kementerian dan agensi hendaklah mematuhi pekeliling yang sedang berkuat kuasa.	Semua Pengguna

PII dikecualikan daripada Data Terbuka.	
3.2.2 Pengelasan Maklumat	
Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a) Terbuka; b) Rahsia Besar; c) Rahsia; d) Sulit; dan e) Terhad.	Semua Pengguna
3.2.3 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a) menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) menentukan maklumat sedia untuk digunakan; d) menjaga kerahsiaan kata laluan; e) mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f) memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; g) menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum; dan h) menjaga maklumat pengenalan peribadi (PII atau Personally Identifiable Information) daripada disebar dan disalahguna oleh pihak yang tidak bertanggungjawab.	Semua Pengguna

PERKARA 4
KESELAMATAN SUMBER MANUSIA

4.1 KESELAMATAN SUMBER MANUSIA DALAM TUGAS HARIAN

Objektif:

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

4.1.1 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan KUSKOP serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b) menjalankan tapisan keselamatan untuk pegawai dan kakitangan KUSKOP serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; c) mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan; dan d) pekerja sementara juga tertakluk kepada syarat-syarat **4.1.1 (a) – (c)** dan sebarang syarat lain yang ditetapkan oleh Bahagian Pengurusan Sumber Manusia.	Semua Pengguna

4.1.2 Dalam Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:	Semua Pengguna

a) memastikan pegawai dan kakitangan KUSKOP serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh KUSKOP; b) memastikan program kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT KUSKOP secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; c) memastikan adanya proses tindakan disiplin dan/ atau undang-undang ke atas pegawai dan kakitangan KUSKOP serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh KUSKOP; d) memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, boleh dirujuk kepada Bahagian Pengurusan Sumber Manusia KUSKOP; dan e) pekerja sementara juga tertakluk kepada syarat-syarat **4.1.2 (a) – (d)** dan sebarang syarat lain yang ditetapkan oleh Bahagian Pengurusan Sumber Manusia KUSKOP.	
4.1.3 Bertukar atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) memastikan semua aset ICT dikembalikan kepada KUSKOP mengikut peraturan dan/ atau terma perkhidmatan yang ditetapkan; b) membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat merujuk kepada peraturan yang ditetapkan oleh KUSKOP dan/ atau terma perkhidmatan; dan c) pekerja sementara juga tertakluk kepada syarat-syarat **4.1.3 (a) – (b)** dan sebarang syarat lain yang ditetapkan oleh Bahagian Pengurusan Sumber Manusia.	Semua Pengguna

PERKARA 5
KESELAMATAN FIZIKAL DAN PERSEKITARAN

5.1 KESELAMATAN KAWASAN

Objektif:

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

5.1.1 Kawalan Kawasan

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan tahap keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c) Memasang alat penggera atau kamera; d) Menghadkan jalan keluar masuk; e) Mengadakan kaunter kawalan; f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; g) Mewujudkan perkhidmatan kawalan keselamatan; h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;	Pegawai Keselamatan Kementerian

j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, rusuhan dan bencana; k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
5.1.2 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) setiap warga KUSKOP termasuk pekerja sementara hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b) semua pas keselamatan hendaklah diserahkan balik kepada KUSKOP apabila warga KUSKOP termasuk pekerja sementara berhenti atau bersara; c) semua pelawat/pihak ketiga hendaklah mendapatkan Pas Keselamatan Pelawat di Kaunter Pelawat di pintu masuk Bangunan KUSKOP. Amalan ini juga perlu dipatuhi di setiap cawangan KUSKOP negeri. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan d) kehilangan pas mestilah dilaporkan dengan segera.	Warga KUSKOP/ Pelawat/ Pihak Ketiga
5.1.3 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan Pelawat/pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi oleh pegawai KUSKOP sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Warga KUSKOP/ Pelawat/ Pihak Ketiga
5.1.4 Kawalan Keselamatan Pusat Data	

Untuk memastikan semua server sentiasa selamat daripada pencerobohan atau sebarang ancaman dan membolehkan ia dicapai sepanjang masa, semua server hendaklah diletakkan di dalam pusat data yang mempunyai kemudahan keselamatan, penyaman udara khas dan kemudahan perlindungan suhu dan kebakaran. Pusat Data juga seharusnya dilengkapkan dengan ciri-ciri keselamatan lain seperti CCTV dan UPS. Berikut beberapa langkah untuk melindungi server tersebut : a) Pengawalan keluar masuk pengguna ke pusat data melalui sistem ***Security Access Door;*** b) Memasang kemera litar tertutup (**CCTV)** bagi tujuan pemantauan dan perekodan aktiviti di dalam Pusat Data***;*** c) Hanya personel yang mempunyai kebenaran sahaja yang dibenarkan memasuki Pusat Data; d) Memastikan Pusat Data sentiasa bersih dan peralatan ICT tidak terdedah kepada habuk; e) Penyaman udara mestilah berfungsi dengan baik. di mana suhunya adalah bersesuaian dengan pusat data; f) Semua peralatan keselamatan, UPS dan penyaman udara mestilah diselenggarakan secara berkala; dan g) Pusat Data juga dilengkapi dengan Sistem Pencegahan dan Penggera Kebakaran yang diselenggarakan secara berkala.	BPTM

5.2 KESELAMATAN PERALATAN
Objektif: Melindungi peralatan ICT KUSKOP dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

5.2.1 Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Warga KUSKOP termasuk pekerja sementara hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna;	Warga KUSKOP

b) Warga KUSKOP termasuk pekerja sementara bertanggungjawab sepenuhnya ke atas semua peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

c) Warga KUSKOP termasuk pekerja sementara dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;

d) Warga KUSKOP termasuk pekerja sementara dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pihak BPTM;

e) Warga KUSKOP termasuk pekerja sementara adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;

f) Warga KUSKOP termasuk pekerja sementara mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini *(updated)* di samping melakukan imbasan ke atas media storan yang digunakan;

g) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;

h) Peralatan-peralatan kritikal perlu disokong oleh UPS mengikut keperluan;

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

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

k) Peralatan ICT yang dipinjam dari stor BPTM dan hendak dibawa keluar dari premis KUSKOP, perlulah mendapat kelulusan Pengarah atau Pengurus BPTM yang berkenaan dan direkodkan bagi tujuan pemantauan;

l) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;

m) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

n) Warga KUSKOP termasuk pekerja sementara tidak dibenarkan mengubah lokasi peralatan ICT dari tempat asal ia ditempatkan tanpa kebenaran Pihak BPTM; o) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pihak BPTM untuk di baikpulih; p) Semua peralatan ICT mestilah didaftarkan di dalam Sistem Pengurusan Aset (SPA) dan ditampal dengan pelekat aset rasmi; q) Sebarang pelekat selain daripada pelekat aset rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut mudah dikenal pasti; r) Semua komputer dan komputer riba yang dibekalkan oleh KUSKOP mesti didaftarkan dengan domain KUSKOP melalui penggunaan *Active Directory* (AD); s) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; t) Warga KUSKOP termasuk pekerja sementara dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pihak BPTM; u) Warga KUSKOP termasuk pekerja sementara bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; v) Warga KUSKOP termasuk pekerja sementara hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; w) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan x) Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
5.2.2 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti *catridge tape*, *optical disk*, *flash disk*, *external harddisk*, *USB drive* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.	Pentadbir Sistem ICT dan Warga KUSKOP

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b) Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; e) Permohonan dan pergerakan media storan hendaklah direkodkan; f) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; g) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h) Semua data di dalam media storan yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan i) Penghapusan maklumat atau kandungan media storan mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
5.2.3 Media Tandatangan Digital	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Warga KUSKOP termasuk pekerja sementara hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Warga KUSKOP
5.2.4 Media Perisian dan Aplikasi	

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan KUSKOP; b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Setiausaha Bahagian BPTM; dan c) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Warga KUSKOP
5.2.5 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	BPTM/ BLESS
5.2.6 Peralatan ICT yang di bawa ke luar premis	
Perkakasan yang dibawa keluar dari premis KUSKOP adalah terdedah kepada pelbagai risiko keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Warga KUSKOP

a) Peralatan perlu dilindungi dan dikawal sepanjang masa; b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan c) Mematuhi *standard operating procedure* (SOP) yang berkuat kuasa.	
5.2.7 Pelupusan Perkakasan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau aset bernilai rendah yang dibekalkan oleh KUSKOP dan ditempatkan di KUSKOP. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KUSKOP. a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; f) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset; g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; h) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan	Unit Pengurusan Aset

menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di KUSKOP; iii. Memindah keluar dari KUSKOP mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab KUSKOP; dan v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *thumb drive* atau *external harddisk* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan. i) Maklumat lanjut pelupusan bolehlah merujuk kepada Tatacara Pengurusan Aset Alih Kerajaan AM2.6 (1PP) berkuatkuasa 3 Julai 2014.	
5.2.8 Komputer Riba	
a) Pastikan pengguna membuat satu salinan segala maklumat yang berada di dalam komputer riba ke dalam media storan yang lain seperti *USB drive* sebelum dibawa keluar daripada pejabat atau ke luar negara; b) Elakkan daripada menyimpan terlalu banyak maklumat penting di dalam komputer riba, sebaliknya simpan maklumat tersebut di dalam media storan yang lain; c) Komputer riba yang baru di bawa pulang atau dipulangkan ke KUSKOP mestilah dikuarantin sehingga proses penyahpepijat dilakukan; d) Pegawai yang meminjam/menggunakan komputer riba KUSKOP bertanggungjawab untuk menjaga keselamatan komputer riba tersebut daripada sebarang kemalangan atau kecurian; e) Berhati-hati dengan penggunaan rangkaian tanpa wayar. Matikan *Bluetooth* atau *Infra Red* sekiranya ianya tidak diperlukan; dan f) Laporkan dengan segera jika berlaku sebarang insiden yang tidak diingini kepada CERT KUSKOP.	Semua Pengguna

5.2.9 Peminjaman Peralatan ICT	
Semua peralatan ICT termasuklah komputer, komputer riba, pencetak dan aksesori yang berkaitan seperti kabel komputer dan sebagainya, adalah di bawah tanggungan BPTM KUSKOP. Oleh itu setiap peralatan yang dipinjam atau dibawa keluar atau masuk perlulah mengikut prosedur berikut: a) Hubungi pihak Unit Sokongan Teknikal untuk membuat peminjaman peralatan yang dikehendaki; b) Pengguna dikehendaki memohon melalui Sistem Pinjaman Aset dan menandatangani borang Senarai Peralatan Yang Dibawa Masuk/Keluar (luaran) yang disediakan oleh BPTM; c) Peralatan yang dipinjam perlulah dikembalikan setelah selesai menggunakannya untuk semakan dan simpanan pihak BPTM serta menandatangani borang Senarai Peralatan Yang Dibawa Masuk/Keluar; d) Peminjam adalah bertanggungjawab untuk memastikan kesemua peralatan dikembalikan dengan sempurna, lengkap dan selamat; dan e) Sebarang kerosakan dan kegagalan peralatan berfungsi dengan baik hendaklah dilaporkan kepada BPTM dengan segera.	Warga KUSKOP
5.3 KESELAMATAN PERSEKITARAN	
Objektif: Melindungi aset ICT KUSKOP dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
5.3.1 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pegawai Keselamatan KUSKOP. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi:	Pegawai Keselamatan Jabatan

a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak berhampiran peralatan ICT; g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya satu (1) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	
5.3.2 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b) Peralatan sokongan seperti UPS dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	BPTM/ BLESS
5.3.3 Kabel	

Kabel rangkaian komputer hendaklah dilindungi kerana ia boleh disalahguna. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	BPTM/ BLESS
5.3.4 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Langkah-Langkah Keselamatan Sekiranya Berlaku Kebakaran; dan b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Bahagian yang dilantik mengikut aras.	Warga KUSKOP
5.4 KESELAMATAN DOKUMEN	
Objektif: Melindungi maklumat KUSKOP dari sebarang bentuk ancaman/persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
5.4.1 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;	Semua Pengguna

b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur Keselamatan; c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	
5.4.2 Simpanan Data Atas Talian *(Cloud)*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap dokumen rasmi hanya dibenarkan disimpan di *private cloud storage.* b) Dokumen terperingkat tidak dibenarkan disimpan di *public cloud storage.* c) Setiap dokumen yang disimpan di atas talian perlu ditetapkan kata laluan untuk membuka dokumen.	Warga KUSKOP

PERKARA 6
PENGURUSAN OPERASI DAN KOMUNIKASI

6.1 PENGURUSAN PROSEDUR OPERASI

Objektif:

Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

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

6.1.1 Pengendalian Prosedur

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c) Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	Warga KUSKOP

6.1.2 Pengurusan Perubahan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan dengan aset ICT berkenaan;	Warga KUSKOP

c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
6.1.3 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Setiausa Bahagian BPTM
6.2 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PIHAK KETIGA	
Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
6.2.1 Perkhidmatan Penyampaian	
Perkara-perkara yang mesti 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;	Semua Pengguna

c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko; dan d) Melaksanakan audit terhadap prestasi perkhidmatan pihak ketiga.	

6.3 PERANCANGAN DAN PENERIMAAN SISTEM

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

6.3.1 Perancangan Kapasiti

Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. 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.	BPTM

6.3.2 Penerimaan Sistem

Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT dan CIO

6.4 PERISIAN BERBAHAYA

Objektif:

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

6.4.1 Perlindungan dari Perisian Berbahaya

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memasang sistem keselamatan untuk mengesan ancaman ICT seperti antivirus, *Intrusion Prevention System* (IPS) dan *Web Application Firewall* (WAF) serta mengikut prosedur penggunaan yang betul dan selamat;	

b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d) Mengemas kini antivirus dengan *pattern* antivirus yang terkini; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	

6.5 HOUSEKEEPING	
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
6.5.1 Backup	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Salinan *backup* hendaklah direkodkan dan disimpan di *off site.* Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terkini;	BPTM

b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan d) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	

6.6 PENGURUSAN RANGKAIAN

Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

6.6.1 Kawalan Infrastruktur Rangkaian

Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pemantauan rangkaian dan server KUSKOP bagi memastikan keselamatan dari pencerobohan dan kelancaran pengoperasian; b) Pemasangan Sistem Pemantauan Rangkaian untuk memantau dan mengesan semua aktiviti dan trafik di dalam rangkaian; c) Pemasangan Sistem Pengurusan dan Penganalisa Log bagi merekod dan menganalisa log-log untuk tujuan forensik ICT semasa berlakunya insiden. d) Capaian kepada infrastruktur rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; e) Pemasangan *firewall* untuk mengawal capaian ke atas sistem yang telah dibangunkan dan memastikan keselamatan aset ICT dalam rangkaian dari pencerobohan; f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah seliaan KUSKOP; g) Pemasangan *proxy* dan *Web Content Filter* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis	BPTM

Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; h) Menggunakan infrastruktur keselamatan ICT menyeluruh bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat KUSKOP; i) Perkhidmatan *Wireless* untuk kegunaan awam hendaklah diasingkan daripada rangkaian dalaman KUSKOP; j) Semua pengguna hanya dibenarkan menggunakan rangkaian KUSKOP sahaja. Penyambungan rangkaian melalui modem/ router/ telefon/ dll persendirian adalah dilarang sama sekali; k) Mengasingkan rangkaian mengikut segmen sistem maklumat, pengguna dalaman dan pengguna luar. l) Sebarang penyambungan rangkaian yang bukan di bawah kawalan KUSKOP hendaklah mendapat kebenaran ICTSO; m) Larangan memuat turun perisian berbahaya bagi mengelakkan prestasi rangkaian terganggu dan mengelakkan penyebaran virus; dan n) Penggunaan *Secure Socket Layer Virtual Private Network (*SSL VPN) bagi capaian aplikasi dalaman KUSKOP dari luar rangkaian PCN/MyGov*Net.	

6.7 PENGURUSAN MEDIA	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
6.7.1 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Semua Pengguna
6.7.2 Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut:	Semua Pengguna

a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e) Menyimpan semua media di tempat yang selamat; f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat; dan g) Pengendalian media hendaklah merujuk kepada KEW.PA-2 (Penyerahan Aset).	
6.7.3 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan system 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 semua aktiviti capaian dokumentasi sedia ada.	Semua Pengguna
6.8 PENGURUSAN PERTUKARAN MAKLUMAT	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara KUSKOP dan agensi luar terjamin.	
6.8.1 Pertukaran Maklumat	

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara KUSKOP dengan agensi luar; c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KUSKOP; dan d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua Pengguna
6.8.2 Pengurusan Mel Elektronik (E-mel)	
Penggunaan emel di KUSKOP hendaklah dipantau secara berterusan oleh Pentadbir Emel untuk memenuhi keperluan etika penggunaan emel 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*" (Pekeliling MAMPU) dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: a) Penggunaan emel rasmi KUSKOP (@KUSKOP.gov.my) adalah untuk kegunaan urusan rasmi sahaja. Pengguna dilarang menggunakan emel rasmi KUSKOP untuk tujuan komersil, politik, perjudian, jenayah, perniagaan dan sebagainya; b) Pengguna dilarang melaksanakan konfigurasi penerimaan emel dari emel rasmi ke emel peribadi tanpa justifikasi dan kelulusan Pentadbir emel bagi mengelak penyalahgunaan emel urusan rasmi kerja; c) Pengguna dilarang menyebarkan gambar-gambar lucah, emel berunsurkan fitnah, perkauman, gangguan seksual atau yang berkaitan dengannya; d) Pengguna dilarang membenarkan akaun emel dan kata laluan digunakan oleh orang lain untuk tujuan menghantar, membaca dan menjawab emel bagi pihaknya;	Warga KUSKOP

e) Penghantaran emel rasmi hendaklah menggunakan akaun emel rasmi dan pastikan alamat emel penerima adalah betul;

f) Pengguna dilarang menggunakan akaun emel persendirian seperti gmail, yahoo atau mana-mana *public* emel untuk menghantar sebarang emel untuk tujuan urusan rasmi;

g) Pengguna dilarang membuat pendaftaran sistem online yang tidak rasmi penggunakan emel rasmi KUSKOP kerana emel tersebut dikhuatiri akan disebar dan disalahgunakan untuk tujuan aktiviti penyebaran virus, emel *spamming*, emel *phishing* dan *junk mail* seperti iklan pemasaran produk;

h) Pengguna tidak digalakkan membuka lampiran emel dari penghantar yang tidak dikenali, berkemungkinan mengandungi virus atau program yang akan menceroboh komputer pengguna tanpa disedari. *Hackers* biasa menggunakan fail berformat *.doc, *.docx, *.xls, *.xlsx & *.pdf untuk memperdaya penerima emel

i) Pengguna dilarang menghantar dan membuka fail lampiran emel (attachment file) berformat seperti *.scr, *.com, *.exe, *.dll, *.pif, *.vbs, *.bat, *.asd, *.chm, *.ocx, *.hlp, *.hta, *.js, *.shb, *.shs, *.vb, *.vbe, *.wsf, *.wsh, *.reg, *.ini, *.diz, *.cpp, *.cpl, *.vxd, *.sys dan *.cmd. Ia dikhuatiri akan menyebarkan virus secara automatik apabila dibuka;

j) Pengguna dilarang menyebarkan fail-fail yang mengandungi kod perosak (*malicious code*) seperti virus, *worm, trojan horse* dan *back door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain;

k) Pengguna mestilah melaksanakan *encryption* atau menetapkan *password* ke atas maklumat-maklumat terperingkat terutama yang dihantar menerusi rangkaian terbuka seperti Internet. Pengguna juga dilarang menghantar *password* yang ditetapkan melalui emel bersama fail tetapi ianya perlu dihantar melalui penggunaan sms atau lain-lain saluran seperti *instant messaging* (IM) atau sebagainya;

l) Pengguna dilarang menghantar dokumen yang besar melebihi 10MB bagi memastikan sistem emel tidak terganggu dan berada dalam prestasi yang baik;

m) Penghantaran emel bergambar (grafik) bagi jemputan/hebahan mesyuarat atau seminar perlulah menggunakan saiz yang kecil tidak melebihi 150KB bagi mengawal storan/quota *mailbox* pengguna dan prestasi capaian emel;

n) Pengguna dikehendaki membuat penyelenggaraan ke atas akaun emel mereka dari semasa ke semasa untuk mengelakkan sebarang gangguan ke atas penggunaan emel;

o) Pengguna digalakkan untuk mencetak dan mendokumenkan semua emel yang penting untuk mengelakkan kehilangan maklumat penting apabila berlaku kerosakan kepada cakera keras komputer;

p) Pengguna hendaklah membuat salinan dan menyimpan fail kepilan ke dalam satu *folder* berasingan dari setiap emel yang penting bagi tujuan *backup* jika berlaku sebarang masalah kepada cakera keras komputer;

q) Nama pegawai dan kakitangan KUSKOP yang bertukar atau berhenti hendaklah dimaklumkan dengan segera kepada BPTM agar akaun emel dapat dikemaskinikan dengan segera;

r) Pengguna mesti memaklumkan kepada pentadbir sistem ICT dengan segera sekiranya mengesyaki akaun telah disalahgunakan;

s) Semua mesej-mesej elektronik yang diwujudkan atau disimpan di dalam sistem adalah dianggap tidak peribadi. Pentadbir sistem atau ICTSO KUSKOP berhak untuk membuat semakan kandungan emel pengguna. Isi kandungan emel tersebut tidak akan diakses atau didedahkan selain daripada untuk tujuan keselamatan atau diperlukan oleh undang-undang;

t) Pengguna hendaklah bertanggungjawab dan sentiasa menyelenggara *mailbox* masing-masing. Emel yang tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

u) Pentadbir emel boleh menamatkan akaun emel pengguna atas sebab-sebab berikut:

   i. Bertukar ke agensi lain
   ii. Bersara
   iii. Ditamatkan perkhidmatan
   iv. Tindakan tatatertib

v) Penutupan akaun emel kakitangan adalah selepas dua (2) minggu dari tarikh akhir perkhidmatan di KUSKOP;

w) Kuota adalah diberi mengikut gred seperti berikut:

   i. Gred 1 sehingga 53 : 2GB
   ii. Gred 54 ke atas : 4GB

x) Penambahan kuota adalah melalui emel permohonan dengan justifikasi keperluan pemohon; dan y) Akaun emel rasmi KUSKOP hanya dibekalkan kepada kakitangan KUSKOP dan kakitangan kontrak sahaja. Bagi pekerja sementara, e-mel akan diberikan tertakluk kepada justifikasi permohonan.	

6.9 PERKHIDMATAN E-DAGANG *(ELECTRONIC COMMERCE SERVICES)*

Objektif:

Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.

6.9.1 E-Dagang

Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat Kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Semua Pengguna

6.9.2 Makluman Umum

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian;	Semua Pengguna

b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	
6.10 PEMANTAUAN DAN LOG	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
6.10.1 Pengauditan dan Forensik ICT	
CERT KUSKOP mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a) Sebarang percubaan pencerobohan kepada sistem ICT KUSKOP; b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti Kerajaan; e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; g) Aktiviti penyalahgunaan akaun emel; dan h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	CERT KUSKOP
6.10.2 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi	Pentadbir Sistem ICT

membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: a) Rekod setiap aktiviti transaksi; b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan d) 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 Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
6.10.3 Sistem Log	
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: a) Pemasangan Sistem Pengurusan dan Penganalisa Log bagi merekod dan memproses segala aktiviti yang berlaku. 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 lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.	Pentadbir Sistem ICT dan ICTSO
6.10.4 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;	Pentadbir Sistem ICT

b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KUSKOP atau PERKARA keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	

PERKARA 7
KAWALAN CAPAIAN

7.1 DASAR KAWALAN CAPAIAN

Objektif:

Mengawal capaian ke atas maklumat.

7.1.1 Keperluan Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d) Kawalan ke atas kemudahan pemprosesan maklumat.	BPTM

7.2 PENGURUSAN CAPAIAN PENGGUNA

Objektif:

Mengawal capaian pengguna ke atas aset ICT KUSKOP.

7.2.1 Akaun Pengguna

Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi :	BPTM

a) Akaun yang diperuntukkan oleh kementerian sahaja boleh digunakan;

b) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan KUSKOP. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;

c) Penggunaan akaun milik orang lain adalah dilarang;

d) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;

e) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut:

i. Bertukar ke agensi lain;
ii. Bersara; atau
iii. Ditamatkan perkhidmatan.

7.2.2 Hak Capaian

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

Keperluan capaian hendaklah sentiasa dipantau dan dikemaskini bagi memastikan hak capaian ini diberikan kepada warga yang dibenarkan sahaja.

7.2.3 Pengurusan Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh KUSKOP.

Kata nama pengguna (*User* ID) merupakan satu pengenalan identiti yang unik bagi setiap pengguna yang menggunakan sesuatu sistem komputer. Setiap nama pengguna yang dibekalkan akan mempunyai kata laluan yang unik untuk membenarkan pengguna mendapat akses ke sistem-sistem tertentu.

Untuk menjamin keselamatan nama pengguna dan kata laluan, langkah-langkah berikut mesti dipatuhi oleh setiap pengguna sistem dan rangkaian KUSKOP:

a) Rahsiakan kata laluan. Pendedahan kepada yang tidak berhak adalah satu kesalahan di bawah Akta Jenayah Komputer 1997.

Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;

b) Pengguna dilarang daripada menggunakan ID pengguna atau nama sebagai kata laluan;

c) Kata laluan mestilah mempunyai ciri-ciri seperti berikut:

   i. Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara;
   ii. Kombinasi antara aksara besar dan kecil, angka dan aksara khusus. (*contoh: P@ssW0rd!@34)*

d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan 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;

g) Penguatkuasaan penukaran kata laluan semasa *login* kali pertama;

h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

i) Pengguna dilarang menggunakan sebarang maklumat peribadi seperti tarikh lahir dan sebagainya sebagai kata laluan;

j) Kata laluan hendaklah ditukar selepas minimum 90 hari atau maksimum 180 hari atau selepas tempoh masa yang telah ditetapkan yang dirasakan bersesuaian dengan persekitaran pengguna;

k) Mengelakkan penggunaan semula kata laluan yang baru digunakan;

l) Laporkan segera kepada CERT KUSKOP sekiranya kata laluan disyaki telah dicerobohi, dan kata laluan sedia ada akan diubah serta-merta;

m) Pengguna dilarang menggunakan perkataan yang boleh diperolehi daripada mana-mana kamus dalam sebarang bahasa;

n) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;

7.2.4 Clear Desk dan Clear Screen

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	Semua Pengguna
7.2.5 Perkakasan Tanpa Penyeliaan *(Unattended Equipment)*	
Perkakasan ICT yang ditinggalkan tanpa penyeliaan hendaklah diberi perlindungan yang memenuhi ciri-ciri asas keselamatan dan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti adalah terjamin.	BPTM
7.3 KAWALAN CAPAIAN RANGKAIAN	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
7.3.1 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian KUSKOP, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan	Pentadbir Sistem ICT

c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	
7.3.2 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan Internet di KUSKOP hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian KUSKOP; b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c) Penggunaan teknologi *seperti bandwidth manager* untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; e) Segala maklumat yang diperolehi daripada Internet dan emel mestilah dikira tidak sahih selagi kesahihannya belum lagi dibuktikan; f) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; g) Bahan rasmi adalah dilarang dari dimuat naik ke Internet tanpa kebenaran pihak pengurusan; h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; i) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh KUSKOP; j) Warga KUSKOP dilarang daripada memuat naik sebarang dokumen, perisian berlesen, emel dan sebagainya ke server atau ruang storan yang dipunyai oleh pihak luar tanpa sebarang kebenaran daripada pihak Pengurusan;	Warga KUSKOP

k) Warga KUSKOP yang menggunakan akaun KUSKOP (KUSKOP.gov.my) merupakan wakil KUSKOP. Oleh itu, setiap warga diingatkan supaya tidak menggunakan akaun tersebut untuk tujuan komersial, politik, perjudian, jenayah dan sebagainya;

l) Fail yang dimuat turun dari Internet mestilah diimbas dengan menggunakan perisian antivirus sebelum ia diinstal atau digunapakai. Semua langkah keselamatan perlu dilaksanakan untuk mengesan sebarang virus dan mengelakkannya daripada tersebar;

m) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;

n) Pengguna dilarang melayari laman web yang tidak beretika seperti laman web pornografi, *online games, social networking* dan sebagainya;

o) Pengguna dilarang menggunakan talian capaian Internet alternatif yang lain seperti modem persendirian dan Wireless Broadband untuk mengakses Internet sewaktu menggunakan aset ICT Kerajaan tanpa sebarang kebenaran dan tanpa sebarang perlindungan seperti firewall;

p) Pengguna dilarang daripada memuat turun dan/atau mengubah sebarang perisian yang dimuat turun daripada Internet untuk mengelakkan berlakunya pelanggaran hak cipta terpelihara;

q) Internet tidak menjamin kerahsiaan maklumat. Maklumat sensitif yang dihantar melalui Internet terdedah kepada risiko dihidu oleh pihak ketiga. Semua pekerja diminta untuk berhati-hati dan berwaspada apabila menghantar sebarang maklumat melalui Internet;

r) Setiap warga KUSKOP bertanggungjawab ke atas sebarang salah perlakuan dan tindakan yang diambil sewaktu menggunakan kemudahan Internet yang diberikan; dan

s) BPTM juga berhak untuk memeriksa setiap komputer yang digunakan oleh warga KUSKOP untuk memastikan setiap arahan di dalam dasar ini dipatuhi oleh semua warga.

7.3.3 Capaian *Public* WIFI

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Warga KUSKOP tidak dibenarkan menggunakan capaian *public* WIFI percuma untuk urusan rasmi KUSKOP contohnya WIFI di McDonalds, Starbuck dan yang seumpamanya; dan b) Dokumen yang hendak dihantar melalui *public* WIFI perlulah di *encrypt* dan mempunyai kata laluan.	Warga KUSKOP

7.4 KAWALAN CAPAIAN SISTEM PENGOPERASIAN

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

7.4.1 Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a) Mengesahkan pengguna yang dibenarkan; b) Mewujudkan jejak audit ke atas semua capaian system pengoperasian terutama pengguna bertaraf *super user;* dan c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;	Pentadbir Sistem ICT

c) Mengehadkan dan mengawal penggunaan program; dan d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
7.4.2 Token Keselamatan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan token GPKI hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; b) Permohonan GPKI untuk pengguna adalah perlu melalui *Authorised Personnel (AP)* dan *Sub Admin (SA)* yang telah dilantik diperingkat KUSKOP; c) Token hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; d) Perkongsian token untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Token yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; e) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada AP/SA yang telah dilantik diperingkat KUSKOP (Merujuk kepada pegawai di Bahagian Pengurusan Teknologi Maklumat); dan f) Pelaksanaan hendaklah merujuk kepada Panduan Pengguna Token Portal GPKI MAMPU.	Warga KUSKOP
7.5 KAWALAN CAPAIAN APLIKASI DAN MAKLUMAT	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.	
7.5.1 Capaian Aplikasi dan Maklumat	
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi:	Pentadbir Sistem ICT

a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); c) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah dibenarkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja;	
7.6 PERANTI MUDAH ALIH DAN KERJA JARAK JAUH	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peranti mudah alih dan kemudahan kerja jarak jauh.	
7.6.1 Peranti Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Merekod aktiviti keluar masuk penggunaan peranti mudah alih milik Kerajaan bagi mengesan pergerakan peranti tersebut daripada kehilangan dan kerosakan; b) Peranti mudah alih milik Kerajaan hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan bagi mengelakkan daripada kecurian atau salah guna; dan c) Memastikan keselamatan maklumat semasa menggunakan peranti mudah alih.	Warga KUSKOP
7.6.2 Bring Your Own Device (BYOD)	
Perkara yang perlu dipatuhi adalah seperti berikut:	Warga KUSKOP

a) Pengguna BYOD perlu memastikan keselamatan maklumat semasa menggunakan peralatan BYOD;

b) Pengguna BYOD adalah dilarang memasang perisian yang tidak dibenarkan oleh KUSKOP;

c) Pengguna BYOD adalah dilarang memasang perisian yang mengganggu servis rangkaian KUSKOP;

d) Mengaktifkan fungsi keselamatan katalaluan di setiap komputer riba / peranti;

e) Perkakasan BYOD hendaklah dilindungi oleh perisian Antivirus bagi mengelak penyebaran virus/malware/trogen dan lain-lain keatas pengguna KUSKOP yang lain;

f) Pengguna BYOD perlu memastikan peranti yang digunakan menggunakan teknologi penyulitan (*encryption*), tandatangan digital atau sebarang mekanisme bagi melindungi maklumat elektronik semasa ianya digunakan;

g) Pengguna KUSKOP adalah dilarang menyalin dan membawa keluar maklumat organisasi dengan menggunakan peranti mudah alih dan media storan seperti USB, *external* HD dsb;

h) Pengguna BYOD perlu memadam dokumen elektronik dengan merincih secara elektronik/*'secure deletion*' selepas dokumen tidak lagi digunapakai; dan

i) Pengguna BYOD adalah dilarang meninggalkan komputer riba / peranti di ruang pejabat yang terbuka tanpa menguncikannya dengan kabel keselamatan.

7.6.3 Kerja Jarak Jauh

Perkara yang perlu dipatuhi adalah seperti berikut:

a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan aset ICT, pendedahan maklumat, capaian tidak sah ke atas sistem maklumat ICT dan penyalahgunaan kemudahan; dan

b) Perlu mendapatkan kebenaran daripada ICTSO untuk melaksanakan kerja jarak jauh;

c) Capaian ke rangkaian dalaman KUSKOP perlu melalui SSL VPN.

PERKARA 8
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN INFRASTRUKTUR DAN SISTEM

8.1 KESELAMATAN DALAM PROSES PEROLEHAN UNTUK PEMBANGUNAN INFRASTRUKTUR DAN SISTEM

Objektif:

Memastikan mekanisme perolehan infrastruktur dan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian dan mematuhi peraturan dan pekeliling semasa yang berkuatkuasa.

8.1.1 Mekanisme Perolehan Infrastruktur Dan Sistem

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Mengenal pasti keperluan sebelum sebarang perolehan dilaksanakan sama ada perolehan daripada syarikat pembekal atau pembangunan secara dalaman; b) Spesifikasi perolehan hendaklah mengandungi klausa tertentu berhubung keperluan keselamatan, pensijilan keselamatan produk, ketersediaan kod sumber, keperluan pelupusan data, keutamaan terhadap teknologi dan kepakaran tempatan, serta keperluan kompetensi pasukan pembangunan.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

8.1.2 Keperluan Keselamatan Infrastruktur dan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b) Ujian keselamatan hendaklah dijalankan ke atas data *input* untuk menyemak pengesahan dan integriti data yang dimasukkan; c) Memastikan data output adalah tepat berdasarkan data input yang dimasukkan;	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

d) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang ralat maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan e) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan mematuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	
8.1.3 Pengesahan Data Input dan Output	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem dan Pentadbir Sistem ICT
8.2 KAWALAN KRIPTOGRAFI	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
8.2.1 Enkripsi	
Warga KUSKOP hendaklah membuat enkripsi ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa seperti penggunaan *encryption* dan kata laluan pada maklumat berkenaan.	Warga KUSKOP
8.2.2 Tandatangan Digital	
Penggunaan tandatangan digital adalah diwajibkan bagi pengurusan transaksi maklumat rahsia rasmi secara elektronik.	Warga KUSKOP
8.2.3 Pengurusan Infrastruktur Kunci Awam (PKI)	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Warga KUSKOP
8.3 KESELAMTAN FAIL SISTEM	
Objektif:	

Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
8.3.1 Kawalan Fail Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b) Kod sumber atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c) Mengawal capaian ke atas kod sumber atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian 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.	Pemilik Sistem dan Pentadbir Sistem ICT
8.4 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
8.4.1 Prosedur Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi pra-syarat pentauliahan sistem. Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan; b) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; c) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggung jawab	Pemilik Sistem dan Pentadbir Sistem ICT

memantau penambahbaikan dan pembetulan yang dilakukan oleh pihak ketiga; d) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; e) Akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan f) Menghalang sebarang peluang kebocoran maklumat.	
8.4.2 Pembangunan Perisian Secara *Outsource*	
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pentadbir/pemilik sistem. Kod sumber *(source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik Kerajaan.	BPTM dan Pentadbir Sistem ICT
8.5 KAWALAN TEKNIKAL KETERDEDAHAN *(VULNERABILITY)*	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
8.5.1 Kawalan Dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT

PERKARA 9
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

9.1 MEKANISME PELAPORAN INSIDEN KESELAMATAN ICT

Objektif:

Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

9.1.1 Mekanisme Pelaporan

Pusat Kawalan dan Koordinasi Siber Negara (NC4) menyediakan platform bagi perkongsian maklumat berkaitan insiden siber untuk seluruh Prasarana Maklumat Kritikal Negara (CNII). CNII merujuk kepada aset (fizikal dan maya), sistem dan fungsi yang penting kepada negara dan kepincangan terhadap fungsi-fungsi kritikal ini akan memberikan impak yang besar kepada pertahanan dan keselamatan negara, kekuatan ekonomi negara, imej negara, kemampuan Kerajaan untuk berfungsi, kesihatan dan keselamatan orang awam. Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar Dasar Keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan kumpulan CERT KUSKOP dengan kadar segera: a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c) Kata laluan atau mekanisme kawalan akses hilang, dicuri, disyaki hilang atau didedahkan; d) Berlaku insiden yang luar biasa seperti kehilangan fail, kegagalan sistem dan serangan luar jangka emel; dan	Warga KUSKOP

e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di KUSKOP seperti di **Lampiran 4**. Prosedur pelaporan insiden keselamatan ICT berdasarkan: a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
9.2 PENGURUSAN MAKLUMAT INSIDEN KESELAMATAN ICT	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
9.2.1 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada KUSKOP. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; d) Menyediakan tindakan pemulihan segera; dan	ICTSO

e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan dan melaporkan kepada NACSA apabila berlaku sebarang insiden keselamatan ICT.	

PERKARA 10
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

10.1 DASAR KESINAMBUNGAN PERKHIDMATAN

Objektif:

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

10.1.1 Pelan Kesinambungan Perkhidmatan (BCP)

BCP adalah di bawah tanggungjawab Bahagian Khidmat Pengurusan (BKP) dan DRP adalah di bawah tanggungjawab BPTM. BCP dan DRP hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian : a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan dalam jangka masa yang ditetapkan; c) Mendokumentasikan proses dan prosedur yang telah dipersetujui; d) Mengadakan program latihan/simulasi kepada pengguna mengenai prosedur kecemasan sekurang-kurangnya setahun sekali; dan e) Mengemaskini Pelan Pemulihan Bencana (DRP) sekurang-kurangnya dua tahun sekali. BCP dan DRP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; b) Senarai personel KUSKOP dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan emel). Senarai kedua juga	ICTSO dan BPTM

hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden; c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan. Salinan BCP dan DRP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. BCP dan DRP hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian BCP dan DRP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. KUSKOP hendaklah memastikan salinan BCP dan DRP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

PERKARA 11
PEMATUHAN

11.1 PEMATUHAN DAN KEPERLUAN PERUNDANGAN

Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada DKCIT KUSKOP.

11.1.1 Pematuhan Dasar

Warga KUSKOP hendaklah membaca, memahami dan mematuhi DKICT KUSKOP dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Sebarang pelanggaran terhadap DKICT KUSKOP akan dikenakan tindakan sewajarnya. Semua aset ICT di KUSKOP termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Setiausaha/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT KUSKOP selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber KUSKOP.	Warga KUSKOP

11.1.2 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi piawaian pelaksanaan keselamatan ICT.	ICTSO

11.1.3 Pematuhan Keperluan Audit

Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.	Warga KUSKOP

Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia supaya tidak berlaku penyalahgunaan.	
11.1.4 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh Warga KUSKOP adalah seperti di Lampiran 5.	Warga KUSKOP
11.1.5 Penguatkuasaan dan Pelanggaran Dasar	
Pelanggaran DKICT KUSKOP boleh dikenakan tindakan tatatertib.	Warga KUSKOP

GLOSARI

Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk, flash disk,* CDROM, *Thumb drive* untuk sebarang kemungkinan adanya virus
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Jalur Lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
BCP	*Business Continuity Planning* (Pelan Kesinambungan Perkhidmatan)
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
CNII	*Critical National Information Infrastructure* Infrastruktur Maklumat Kritikal Negara
Denial of Service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
DRP	*Disaster Recovery Planning* (Pelan Pemulihan Bencana)
Encryption	Enkripsi ialah satu proses penyulitan data oleh penirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk unutk 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 penhantaran mesej melalui e-mel termasuk penyalahgunaan dan

	pecurian identiti, pencurian maklumat (information thef / espionage), penupiuan (hoaxes).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Hard Disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (hub) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan / atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.

LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya.
Modem	*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.
NC4	*National Cyber Coordination and Command Centre* Pusat Kawalan dan Penyelarasan Siber Negara
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pekerja Sementara	Pegawai Khidmat Sambilan (PKS)/Pegawai Sambilan Harian (PSH)
Perisian Aplikasi	Ia merujuk pada perisian arau pakej yang selalu digunakan seperti spreadsheet dan word processing ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Pihak Ketiga	Pembekal perkhidmatan/Vendor/Agensi luar.
Public Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet
Router	Penghala yang digunkan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya pencapaian internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunkan dalam jangka masa tertentu

Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki pretasi rangkaian Carrier Sense Multiple Access / Collision Detection (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan pelanggaran yang berlaku.
Threat	Gangguan dan anc aman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang disambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi
Wireless	Jaringan komputer yang berhubung tanpa melalui kabel.

Lampiran 1

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN PEMBANGUNAN USAHAWAN DAN KOPERASI (KUSKOP)

Nama (HURUF BESAR) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian (Kerajaan) : .....

*** Pihak Ketiga**
Syarikat & Alamat : .....

.....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

1. Saya telah membaca dan memahami Dasar Keselamatan ICT;
2. Saya juga akan akur dengan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT; dan
3. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....
(Tandatangan Pegawai)

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....

Nama : .....

Tarikh : .....

Lampiran 2

PERAKUAN UNTUK DITANDATANGANI OLEH KONTRAKTOR/PERUNDING/PIHAK KETIGA BERKENAAN DENGAN KEMENTERIAN PEMBANGUNAN USAHAWAN DAN KOPERASI (KUSKOP)

AKTA RAHSIA RASMI 1972

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 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, 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 segala maklumat rasmi yang saya perolehi dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau mana-mana kerajaan dalam Malaysia, adalah milik kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan sama ada secara lisan atau dengan menulis, 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 mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani suatu akuan selanjutnya bagi maksud ini apabila meninggalkan Perkhidmatan Perunding Kerajaan.

Tandatangan : ……

Nama dengan Huruf Besar : .....

No. Kad Pengenalan : .....

Jawatan : .....

Syarikat : .....

Tarikh : .....

Cop/ Meterai Syarikat :

Disaksikan oleh : ……
(Tandatangan)

Nama dengan Huruf Besar : .....

No Kad Pengenalan : .....

Jawatan : .....

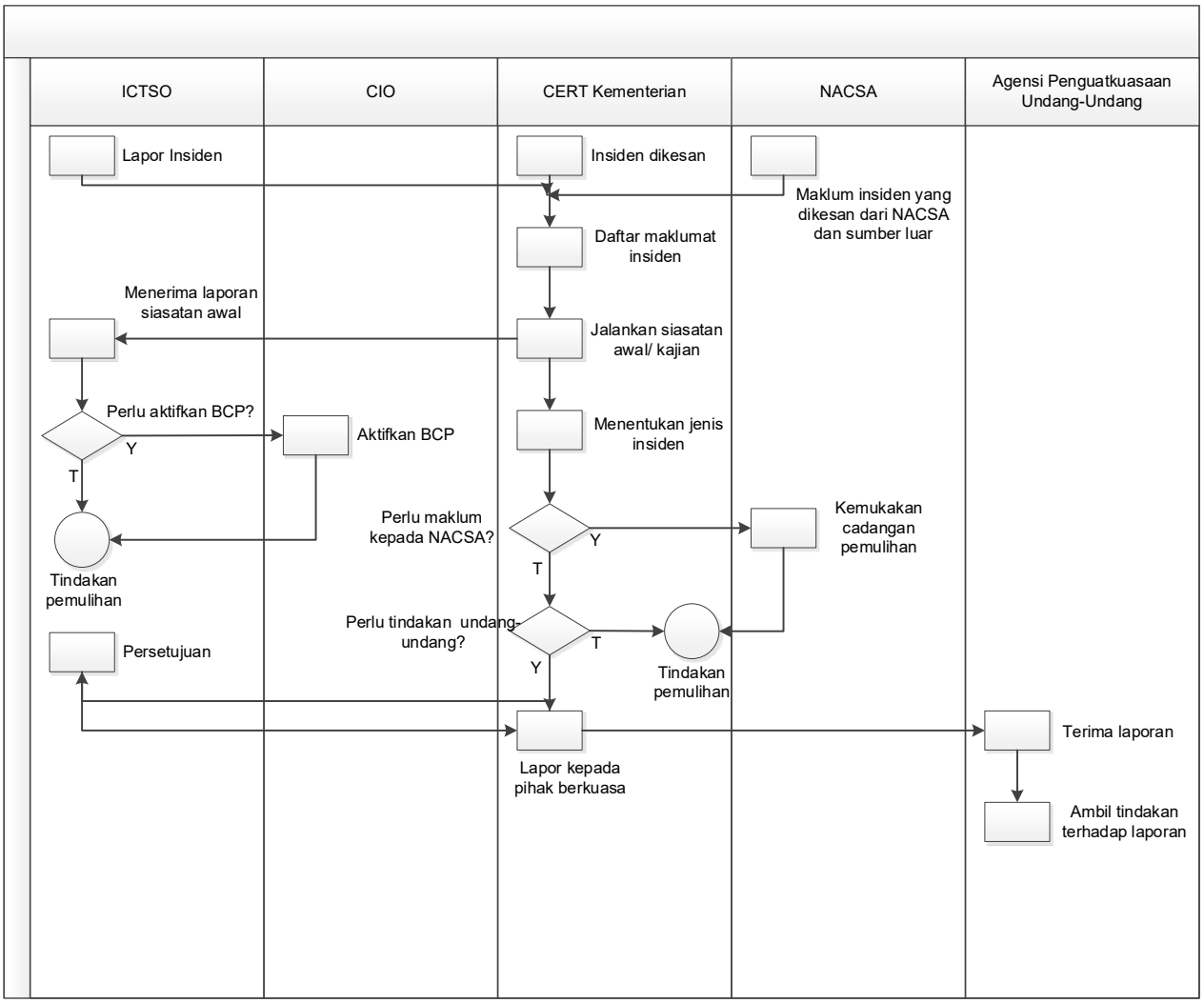
Jabatan : .....

Tarikh : .....

Cop Jabatan :

Lampiran 3

PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT KEMENTERIAN PEMBANGUNAN USAHAWAN DAN KOPERASI (KUSKOP)



Lampiran 4

SENARAI PERUNDANGAN DAN PERATURAN

1) Arahan Keselamatan (Semakan dan Pindaan 2015).
2) Arahan 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara.
3) Akta 709 – Akta Perlindungan Data Peribadi 2010.
4) Arahan 24 - Dasar Dan Mekanisme Pengurusan Krisis Siber Negara.
5) Pekeliling Am Bil. 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam.
6) Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam.
7) Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital Document Management System (DDMS) Sektor Awam 25 Januari 2015.
8) Dasar Kriptografi Negara 12 Julai 2013.
9) Surat Pekeliling Perbendaharaan – Garis Panduan Mengenai Pengurusan Perolehan Information Telecommunication Technology ICT Kerajaan SPP 3/2013.
10) 1Pekeliling Perbendaharaan Malaysia (1PP).
11) Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013.
12) Arahan Ketua Pegawai Keselamatan Kerajaan 5 jun 2012 – Langkah-Langkah Keselamatan Perlindungan Bagi Mencegah Kehilangan Komputer Riba Dan Peranti Mudah Alih Di Sektor Awam.
13) PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2011 (Pindaan Kedua).
14) Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat 24 Nov 2010.
15) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam, 22 Jan 2010.
16) Akta 709 – Akta Perlindungan Data Peribadi 2010.
17) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam.
18) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan, 23 Nov 2007.
19) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan, 1 Jun 2007.
20) Arahan Teknologi Maklumat, MAMPU, 2007.
21) Akta 680 – Aktiviti Kerajaan Elektronik 2007.
22) Arahan Ketua Setiausaha Negara Bil. 1 Tahun 2007 – Langkah-Langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lain-Lain Peralatan Komunikasi ICT Tanpa Kebenaran Atau Kuasa Yang Sah Di Agensi-Agensi Kerajaan.
23) Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) Di Agensi-Agensi Kerajaan, 20 Oktober 2006.
24) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam.
25) Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam 04/2006.
26) Akta 658 – Akta Perdagangan Elektronik 2006.
27) Surat Pekeliling Am Bil. 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.
28) Akta 629 – Akta Arkib Negara 2003.

29) Akta 606 – Akta Cakera Optik 2000.
30) Akta 588 – Akta Komunikasi dan Multimedia 1998.
31) Akta 562 - AktaTandatangan Digital 1997.
32) Akta 563 – Akta Jenayah Komputer 1997.
33) Akta 564 - Telemedicine Act 1997.
34) Akta 88 – Akta Rahsia Rasmi 1972.
35) Akta 332 – Akta Hak Cipta 1987.
36) Surat Pekeliling Am Bilangan 2/1987 – Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987).
37) Akta 298 – Kawasan Larangan Tempat Larangan 1959
38) Akta 56 – Akta Keterangan 1950.
39) National Cyber Security Policy (NCSP)
40) Guideline to Determine Information Security Professionals Requirement for the CNII Agencies /Organisations.
41) Arahan Tetap Sasaran Penting.
42) Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara.
43) Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi.
44) Pekeliling Transformasi Pentadbiran Awam Bil. 1 Tahun 2017 – Pelaksanaan Analitis Data Raya Sektor Awam (aDRSA).
45) Perintah Am Bab D.

BAHAGIAN PENGURUSAN TEKNOLOGI MAKLUMAT
KEMENTERIAN PEMBANGUNAN USAHAWAN DAN KOPERASI (KUSKOP)
Aras 4, Blok E4/5, Kompleks E, Pusat Pentadbiran Kerajaan Persekutuan 62668 Putrajaya, Malaysia
Tel: 603-8000 8000 Fax: 603-8889 3703 E-mel: bpmhelpdesk@medac.gov.my