# KPKK

## Dasar Keselamatan
## Teknologi Maklumat dan Komunikasi (ICT)
## Kementerian Penerangan Komunikasi dan Kebudayaan
## (Ministry of Information Communication and Culture)

**Versi 1.0**

**16 JULAI 2009**

## KANDUNGAN


PENGENALAN 6
OBJEKTIF 6
PERNYATAAN DASAR 7
SKOP 8
PRINSIP-PRINSIP 9

**PERKARA 01 DASAR KESELAMATAN ICT**

**Dasar Keselamatan ICT**

DM-010101 Pelaksanaan Dasar 11
DM-010102 Penyebaran Dasar 11
DM-010103 Penyelenggaraan Dasar 11
DM-010104 Pemakaian Dasar 11

**PERKARA 02 ORGANISASI KESELAMATAN**

**Infrastruktur Keselamatan Organisasi**

DM-020101 Ketua Setiausaha 12
DM-020102 Ketua Pegawai Maklumat (CIO) 12
DM-020103 Pengurus ICT 13
DM-020104 Pegawai Keselamatan ICT (ICTSO) 13
DM-020105 Pentadbir Sistem ICT 14
DM-020106 Pengguna 15
DM-020107 Pasukan Pengendali Insiden Keselamatan ICT (CERT, KPKK) 16

**Pihak Ketiga**

DM-020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga 17

**PERKARA 03 PENGURUSAN ASET**

DM-030101 Inventori Aset 18

**Pengelasan dan Pengendalian Maklumat**

DM-030201 Pengelasan Maklumat 18
DM-030202 Pengendalian Maklumat 18

**PERKARA 04 KESELAMATAN SUMBER MANUSIA**

**Keselamatan ICT Dalam Tugas Harian**

DM-040101 Tanggungjawab Keselamatan 20
DM-040102 Terma dan Syarat Perkhidmatan 20
DM-040103 Perakuan Akta Rahsia Rasmi 20
DM-040104 Sebelum Berkhidmat 20
DM-040105 Dalam Perkhidmatan 21
DM-040106 Tamat Perkhidmatan Atau Bertukar 21

## PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN


**Keselamatan Kawasan**

DM-050101 Perimeter Keselamatan Fizikal 22
DM-050102 Kawalan Masuk Fizikal 22
DM-050103 Kawasan Larangan 23

**Keselamatan Peralatan**

DM-050201 Peralatan ICT 23
DM-050202 Media Storan 25
DM-050203 Media Perisian dan Aplikasi 25
DM-050204 Penyelenggaraan 26
DM-050205 Peminjaman Perkakasan Untuk Kegunaan di Luar Pejabat 26
DM-050206 Pengendalian Peralatan Luar Yang Dibawa Masuk/Keluar 26
DM-050207 Pelupusan 27
DM-050208 *Clear Desk* dan *Clear Screen* 28

**Keselamatan Persekitaran**

DM-050301 Kawalan Persekitaran 28
DM-050302 Kabel 29
DM-050303 Bekalan Kuasa 29
DM-050304 Prosedur Kecemasan 30

**Keselamatan Dokumen dan Sistem Dokumentasi**

DM-050401 Dokumen 30


## PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI


**Pengurusan Prosedur Operasi**

DM-060101 Pengendalian Prosedur 31
DM-060102 Kawalan Perubahan 31
DM-060103 Pengasingan Tugas dan Tanggungjawab 32

**Perancangan dan Penerimaan Sistem**

DM-060201 Perancangan Kapasiti 32
DM-060202 Penerimaan Sistem 32

**Perisian Berbahaya**

DM-060301 Perlindungan dari Perisian Berbahaya 32

***Housekeeping***

DM-060401 *Backup* 33
DM-060402 Sistem Log 34

**Pengurusan Rangkaian**

DM-060501 Kawalan Infrastruktur Rangkaian 34

**Pengurusan Media**

DM-060601 Penghantaran dan Pemindahan 35
DM-060602 Prosedur Pengendalian Media 35
DM-060603 Pengurusan Pertukaran Maklumat 36

**Keselamatan Komunikasi**

DM-060701 Mel Elektronik 36
DM-060702 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga 38
DM-060703 Pemantauan 38

**PERKARA 07 KAWALAN CAPAIAN**

**Dasar Kawalan Capaian**

DM-070101 Keperluan Dasar 39

**Pengurusan Capaian Pengguna**

DM-070201 Akaun Pengguna 39
DM-070202 Hak Capaian 39
DM-070203 Pengurusan Kata laluan 40
DM-070204 Kad Pintar 40

**Kawalan Capaian**

DM-070301 Kawalan Capaian Rangkaian 41
DM-070302 Capaian Jarak Jauh 41
DM-070303 Capaian Internet 41

**Kawalan Capaian Sistem dan Aplikasi**

DM-070401 Capaian Sistem Pengoperasian 42
DM-070402 Sistem Maklumat dan Aplikasi 43

**Audit**

DM-070501 Pengauditan dan Forensik ICT 44
DM-070502 Jejak Audit 45

**PERKARA 08 PEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM**

**Keselamatan Dalam Membangunkan Sistem dan Aplikasi**

DM-080101 Keperluan Keselamatan 46
DM-080102 Pengesahan Data Input 46
DM-080103 Kawalan Prosesan 46
DM-080104 Pengesahan Data Output 46

**Kriptografi**

DM-080201 Penyulitan 46
DM-080202 Pengurusan Infrastruktur Kunci Awam (PKI) 47

**Fail Sistem**

DM-080301 Kawalan Fail Sistem 47

**Pembangunan dan Proses Sokongan Sistem**

DM-080401 Kawalan Perubahan 47
DM-080402 Pembangunan Secara *Outsource* 47
DM-080403 Kawalan dari Ancaman Teknikal 47

**PERKARA 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT**

**Pengurusan Insiden Keselamatan ICT**

DM-090101 Mekanisme Pelaporan Insiden Keselamatan ICT 48
DM-090102 Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT 49
DM-090103 Pengurusan Maklumat Insiden Keselamatan ICT 49

**PERKARA 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN**

**Dasar Kesinambungan Perkhidmatan**

DM-100101 Pelan Kesinambungan Perkhidmatan 51
DM-100102 Pengurusan Kesinambungan Perkhidmatan 51

**PERKARA 11 PEMATUHAN**

**Pematuhan dan Keperluan Perundangan**

DM-110101 Pematuhan Dasar 52
DM-110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal 52
DM-110103 Pematuhan Keperluan Audit 52
DM-110104 Keperluan Perundangan 52

**Tindakan Tatatertib**

DM-110201 Pelanggaran Dasar/Perundangan 54

GLOSARI 55

LAMPIRAN

Lampiran A – Surat Akuan Pematuhan Dasar Keselamatan ICT 57
Lampiran B – Proses Kerja Pelaporan Insiden Keselamatan ICT 58
Lampiran C – Borang Pengisytiharan Barang Keluar/Masuk 60

## PENGENALAN

Dasar Keselamatan ICT KPKK (DKICT KPKK) merangkumi Dasar Keselamatan ICT Kementerian Penerangan Komunikasi dan Kebudayaan dan semua Jabatan/Agensi di bawahnya. Dasar ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) Kementerian Penerangan Komunikasi dan Kebudayaan (KPKK). Dasar ini juga menerangkan kepada semua pengguna di KPKK mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT KPKK.

## OBJEKTIF

DKICT KPKK diwujudkan untuk menjamin kesinambungan urusan pengoperasian dan pengurusan ICT KPKK dengan meminimumkan kesan insiden keselamatan ICT KPKK.

Objektif utama DKICT KPKK ialah seperti berikut :-

a. Memastikan kelancaran pengoperasian dan pengurusan ICT KPKK dengan meminimumkan kerosakan atau kemusnahan;

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

c. Mencegah salah guna atau kecurian aset ICT Kerajaan.

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

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

Selain dari itu, langkah-langkah ke arah menjamin keselamatan 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

Sistem ICT KPKK terdiri daripada manusia, perkakasan, perisian, telekomunikasi, kemudahan ICT dan data. DKICT KPKK 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 Sistem ICT KPKK terjamin keselamatannya sepanjang masa, DKICT KPKK merangkumi perlindungan semua bentuk maklumat Kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran, dan yang dibuat salinan keselamatan ke dalam semua aset ICT KPKK. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut :-

**a. Perkakasan**
Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan agensi. 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 agensi;

**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.
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 agensi. Contoh : Sistem dokumentasi, prosedur operasi, rekod-rekod agensi, 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 agensi bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

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 KPKK dan perlu dipatuhi adalah seperti berikut :-

**a. Akses atas dasar perlu mengetahui**

Akses terhadap penggunaan aset ICT KPKK hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

**b. Hak akses minimum**

Hak akses pengguna hanya diberi pada tahap 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 KPKK. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah :-

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;
v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

**d. Pengasingan**

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

**e. Pengauditan**

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

**f. Pematuhan**

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

**g. Pemulihan**

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan; dan

**h. Saling Bergantungan**

Setiap prinsip di atas adalah saling 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.

## PERKARA 01 DASAR KESELAMATAN ICT

| Objektif | | |
|---|---|---|
| DKICT KPKK diwujudkan untuk melindungi aset ICT KPKK bagi memastikan kelancaran operasi organisasi secara berterusan, meminimumkan kerosakan atau kemusnahan aset-aset ICT melalui usaha pencegahan atau mengurangkan kesan kejadian yang tidak diingini berdasarkan kepada ciri-ciri keselamatan iaitu kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan. | | |
| | **KENYATAAN** | **TINDAKAN** |
| **DM-010101** | **Pelaksanaan Dasar** | |
| | Pelaksanaan dasar ini akan dijalankan oleh Ketua Setiausaha (KSU) dibantu oleh Jawatankuasa CIO dan ICTSO yang dipengerusikan oleh Ketua Pegawai Maklumat (CIO) dengan keahlian terdiri daripada Pengurus ICT, Pegawai Keselamatan ICT (ICTSO) serta semua CIO, Pengurus ICT dan ICTSO Jabatan/Agensi di bawahnya. | KSU |
| **DM-010102** | **Penyebaran Dasar** | |
| | Dasar ini perlu disebarkan kepada semua pengguna KPKK merangkumi semua warga KPKK, pembekal, pakar runding dan lain-lain yang bertugas dan/atau berurusan dengan KPKK dan semua Jabatan/Agensi di bawahnya. | Semua ICTSO |
| **DM-010103** | **Penyelenggaraan Dasar** | |
| | DKICT KPKK 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 KPKK :-<br><br>a. Kenal pasti dan tentukan perubahan yang diperlukan;<br><br>b. Kemukakan cadangan pindaan secara bertulis kepada Jawatankuasa CIO dan ICTSO KPKK untuk pembentangan dan persetujuan Jawatan Kuasa Pemandu ICT (JPICT) yang di pengerusikan oleh KSU;<br><br>c. Perubahan yang telah dipersetujui oleh JPICT mestilah dimaklumkan kepada semua pengguna; dan<br><br>d. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun. | Semua ICTSO |
| **DM-010104** | **Pemakaian Dasar** | |
| | DKICT KPKK adalah terpakai kepada semua pengguna ICT KPKK dan tiada pengecualian diberikan. | Semua Pengguna |

## PERKARA 02 ORGANISASI KESELAMATAN

| Objektif | | |
|---|---|---|
| Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT KPKK. | | |
| **Infrastruktur Organisasi Keselamatan** | | |
| **DM-020101** | **Ketua Setiausaha** | |
| | Peranan dan tanggungjawab KSU adalah seperti berikut :-<br><br>a. Membaca, memahami dan mematuhi DKICT KPKK;<br><br>b. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah DKICT KPKK;<br><br>c. Memastikan semua pengguna mematuhi DKICT KPKK;<br><br>d. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi;<br><br>e. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT KPKK; dan<br><br>f. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN PENERANGAN KOMUNIKASI DAN KEBUDAYAAN. (Lampiran A) | KSU |
| **DM-020102** | **Ketua Pegawai Maklumat (CIO)** | |
| | Ketua Pegawai Maklumat (CIO) adalah Setiausaha Bahagian Kanan Pengurusan KPKK dan semua Ketua Pengarah/Pengurus Besar Jabatan/Agensi. Peranan dan tanggung jawab CIO adalah seperti berikut :-<br><br>a. Membaca, memahami dan mematuhi DKICT KPKK;<br><br>b. Membantu KSU dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT KPKK;<br><br>c. Menentukan keperluan keselamatan ICT KPKK; dan<br><br>d. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN PENERANGAN KOMUNIKASI DAN KEBUDAYAAN. (Lampiran A) | Semua CIO |

| | | |
|---|---|---|
| **DM-020103** | **Pengurus ICT** | |
| | Pengurus ICT ialah Setiausaha Bahagian Pengurusan (BPM) KPKK dan semua Pengarah Bahagian/Ketua Cawangan ICT Bahagian/Agensi. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut :-<br><br>a. Membaca, memahami dan mematuhi DKICT KPKK;<br><br>b. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan KPKK;<br><br>c. Menentukan kawalan akses semua pengguna terhadap aset ICT KPKK;<br><br>d. Memaklumkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO;<br><br>e. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KPKK; dan<br><br>f. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN PENERANGAN KOMUNIKASI DAN KEBUDAYAAN. (Lampiran A) | Semua Pengurus ICT |
| **DM-020104** | **Pegawai Keselamatan ICT (ICTSO)** | |
| | ICTSO KPKK adalah Ketua Penolong Setiausaha Bahagian Pengurusan Maklumat (BPM) KPKK dan semua Pengarah Bahagian/Ketua Cawangan ICT Bahagian/Agensi. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut :-<br><br>a. Membaca, memahami dan mematuhi DKICT KPKK;<br><br>b. Mengurus keseluruhan program-program keselamatan ICT KPKK;<br><br>c. Menguatkuasakan DKICT KPKK;<br><br>d. Memberi penerangan, taklimat dan pendedahan berkenaan DKICT KPKK kepada semua pengguna KPKK;<br><br>e. Mewujudkan dan melaksanakan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT KPKK;<br><br>f. Menjalankan pengurusan risiko;<br><br>g. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan Bahagian dan Jabatan/Agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya;<br><br>h. Memberi dan menyebarkan amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang | Semua ICTSO |

| | | |
|---|---|---|
| | bersesuaian;<br><br>i. Melaporkan insiden keselamatan ICT kepada Pasukan Pengendali Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumkannya kepada CIO;<br><br>j. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;<br><br>k. Melaporkan sebarang salah laku pengguna yang melanggar DKICT KPKK kepada CIO;<br><br>l. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar DKICT KPKK;<br><br>m. Menyedia, melaksanakan dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT;<br><br>n. Menyedia, melaksanakan dan menyelaras penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT KPKK; dan<br><br>o. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN PENERANGAN KOMUNIKASI DAN KEBUDAYAAN. (Lampiran A) | |
| **DM-020105** | **Pentadbir Sistem ICT** | |
| | Pentadbir Sistem ICT ialah Penolong Setiausaha (PSU) (BPM) KPKK dan semua Pegawai Teknologi Maklumat/Jurutera Jabatan/Agensi merupakan Pentadbir Sistem ICT di Jabatan/Agensi masing-masing.<br><br>Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut :-<br><br>a. Membaca, memahami dan mematuhi DKICT KPKK;<br><br>b. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas;<br><br>c. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT KPKK;<br><br>d. Memantau aktiviti capaian sistem aplikasi harian pengguna;<br><br>e. Bertanggungjawab memantau setiap perkakasan ICT KPKK yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang | Semua PTM KPKK, Pegawai yang diturunkan kuasa |

| | | |
|---|---|---|
| | baik;<br><br>f. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;<br><br>g. Melaporkan sebarang insiden keselamatan ICT kepada ICTSO masing-masing;<br><br>h. Menyimpan dan menganalisis rekod jejak audit;<br><br>i. Menyediakan laporan penggunaan bandwidth rangkaian dan sistem secara berkala 4 kali setahun; dan<br><br>j. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN PENERANGAN KOMUNIKASI DAN KEBUDAYAAN. (Lampiran A) | |
| **DM-020106** | **Pengguna** | |
| | Pengguna adalah semua warga KPKK, pembekal, pakar runding dan lain-lain yang bertugas dan/atau berurusan dengan KPKK dan Jabatan/Agensi di bawahnya.<br>Peranan dan tanggungjawab pengguna adalah seperti berikut :-<br><br>a. Membaca, memahami dan mematuhi DKICT KPKK;<br><br>b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;<br><br>c. Lulus tapisan keselamatan (jika berkaitan);<br><br>d. Melaksanakan prinsip-prinsip DKICT KPKK dan menjaga kerahsiaan maklumat KPKK;<br><br>e. Melaksanakan langkah-langkah perlindungan seperti berikut :-<br><br>1. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;<br>2. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;<br>3. Menentukan maklumat sedia untuk digunakan;<br>4. Menjaga kerahsiaan kata laluan;<br>5. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;<br>6. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan<br>7. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.<br><br>f. Melaporkan segera sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO | Pengguna |

| | | |
|---|---|---|
| | masing-masing;<br><br>g. Menghadiri program-program kesedaran mengenai keselamatan ICT KPKK; dan<br><br>h. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN PENERANGAN KOMUNIKASI DAN KEBUDAYAAN. (Lampiran A) | |
| **DM-020107** | **Pasukan Pengendali Insiden Keselamatan ICT KPKK (CERT KPKK)** | |
| | Keanggotaan CERT KPKK adalah seperti berikut :-<br><br>**Pengarah CERT:** Pengurus ICT (Setiausaha BPM, KPKK)<br><br>**Pengurus CERT:** Pegawai Keselamatan ICT (ICTSO, KPKK)<br><br>**Ahli :**<br>• Pengurus ICT Jabatan/Agensi<br>• ICTSO Jabatan/Agensi<br>• Wakil Pegawai Teknologi Maklumat Kementerian/Jabatan/Agensi<br>• Wakil Penolong Pegawai Teknologi Maklumat Kementerian/Jabatan/Agensi<br><br>Peranan dan tanggungjawab CERT KPKK adalah seperti berikut:<br><br>a. Menerima dan mengesan aduan keselamatan ICT KPKK dan menilai tahap dan jenis insiden;<br><br>b. Merekodkan dan menjalankan siasatan awal insiden yang diterima;<br><br>c. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;<br><br>d. Menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai *input* atau untuk tindakan seterusnya;<br><br>e. Memberi khidmat nasihat kepada semua CIO mengenai tindakan pemulihan dan pengukuhan;<br><br>f. Menyebarkan makluman berkaitan pemulihan dan pengukuhan kepada semua pengguna KPKK; dan<br><br>g. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan. | CERT KPKK |

| Pihak Ketiga | | |
|---|---|---|
| Objektif : Menjamin keselamatan semua aset ICT KPKK yang digunakan oleh pihak ketiga. | | |
| **DM-020201** | **Keperluan Keselamatan Kontrak dengan Pihak Ketiga** | |
| | Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak luar/asing dikawal.<br><br>Perkara yang perlu dipatuhi termasuk yang berikut :-<br><br>a. Membaca, memahami dan mematuhi DKICT KPKK;<br><br>b. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;<br><br>c. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pengguna;<br><br>d. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga dan akses kepada aset ICT KPKK perlu berlandaskan kepada perjanjian kontrak. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai :-<br><br>i. DKICT KPKK;<br>ii. Tapisan Keselamatan;<br>iii. Perakuan Akta Rahsia Rasmi 1972;<br>iv. Hak Harta Intelek; dan<br>v. Arahan Teknologi Maklumat.<br><br>e. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN PENERANGAN KOMUNIKASI DAN KEBUDAYAAN. (Lampiran A) | Semua CIO, Pengurus ICT, ICTSO, Pentadbir Sistem ICT dan Pihak Ketiga |

## PERKARA 03 PENGURUSAN ASET

| Objektif | | |
|---|---|---|
| Memberi dan menyokong perlindungan keselamatan yang bersesuaian ke atas semua aset ICT KPKK. | | |
| **DM-030101** | **Inventori Aset** | |
| | Semua aset ICT KPKK hendaklah direkodkan. Mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. | Pentadbir Sistem ICT dan Pegawai Aset |
| | Setiap pengguna adalah bertanggung jawab ke atas semua aset ICT di bawah jagaan dan kawalannya. | Semua Pengguna |
| **Pengelasan dan Pengendalian Maklumat** | | |
| Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian. | | |
| **DM-030201** | **Pengelasan Maklumat** | |
| | Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut :-<br><br>a. Rahsia Besar;<br>b. Rahsia;<br>c. Sulit; atau<br>d. Terhad. | Pegawai yang diberi kuasa |
| | Setiap pengguna adalah bertanggung jawab mengurus maklumat bersesuaian dengan peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan. | Semua Pengguna |
| **DM-030202** | **Pengendalian Maklumat** | |
| | Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut :-<br><br>a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;<br>b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;<br>c. Menentukan maklumat sedia untuk digunakan;<br>d. Menjaga kerahsiaan kata laluan;<br>e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; | Semua Pengguna |

| | | |
|---|---|---|
| | f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan<br>g. Menjaga kerahsiaan langkah-langkah keselamatan ICT KPKK dari diketahui umum. | |

## PERKARA 04 KESELAMATAN SUMBER MANUSIA

| Objektif | | |
|---|---|---|
| Memastikan semua sumber manusia yang terlibat termasuk warga KPKK, kontraktor, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT KPKK. | | |
| **Keselamatan ICT Dalam Tugas Harian** | | |
| **DM-040101** | **Tanggungjawab Keselamatan** | |
| | Peranan dan tanggungjawab pengguna terhadap keselamatan ICT KPKK mestilah lengkap, jelas, direkodkan, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak.<br><br>Keselamatan ICT KPKK merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT KPKK yang digunakan di dalam melaksanakan tugas harian. | Semua Pengguna |
| **DM-040102** | **Terma dan Syarat Perkhidmatan** | |
| | Semua pengguna KPKK yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa. | Semua Pengguna KPKK yang dilantik |
| **DM-040103** | **Perakuan Akta Rahsia Rasmi** | |
| | Semua pengguna yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972. | Semua Pengguna |
| **DM-040104** | **Sebelum Berkhidmat** | |
| | Semua pengguna mestilah memahami tanggungjawab masing-masing ke atas keselamatan aset ICT KPKK bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT.<br><br>Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Peranan dan tanggungjawab penjawat awam, kontraktor, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dengan aset ICT Kerajaan perlu dinyatakan dengan jelas dan terperinci sebelum, semasa dan selepas perkhidmatan; dan<br><br>b. Penyaringan dan pengesahan latar belakang calon untuk penjawat awam, kontraktor, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan hendaklah dilakukan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan. | Semua Pengguna |

| | | |
|---|---|---|
| **DM-040105** | **Dalam Perkhidmatan** | |
| | Semua Pengguna hendaklah faham dan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong DKICT KPKK dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT.<br><br>Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Memastikan semua pengguna KPKK menguruskan keselamatan berdasarkan perundangan dan peraturan yang ditetapkan oleh KPKK;<br><br>b. Memastikan latihan kesedaran yang berkaitan mengenai pengurusan keselamatan ICT KPKK diberi kepada semua pengguna KPKK dan sekiranya perlu diberikan kepada kontraktor, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa;<br><br>c. Memastikan adanya proses tindakan disiplin ke atas semua pengguna KPKK, sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan dalam DKICT KPKK; dan<br><br>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 KPKK. Sebarang kursus dan latihan teknikal yang diperlukan, pihak pengguna boleh merujuk kepada pihak ICT masing-masing. | Semua Pengguna<br><br><br><br><br><br><br><br><br><br><br>Semua ICTSO<br><br><br><br>Semua Pengguna |
| **DM-040106** | **Tamat Perkhidmatan Atau Bertukar** | |
| | Memastikan semua pengguna KPKK diuruskan dengan teratur apabila tamat perkhidmatan atau bertukar dari KPKK.<br><br>Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Memastikan semua aset ICT Kerajaan dikembalikan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan<br><br>b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan dan/atau terma perkhidmatan . | Semua Pengguna KPKK yang dilantik |

## PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

| Objektif | | |
|---|---|---|
| Melindungi pejabat dan maklumat daripada sebarang bentuk pencerobohan dan ancaman. | | |
| **DM-050101** | **Perimeter Keselamatan Fizikal** | |
| | Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut :-<br><br>a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;<br><br>b. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan;<br><br>c. Memperkukuhkan dinding dan siling;<br><br>d. Memasang alat penggera atau kamera;<br><br>e. Mengehadkan jalan keluar masuk;<br><br>f. Mengadakan kaunter kawalan;<br><br>g. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan<br><br>h. Mewujudkan perkhidmatan kawalan keselamatan. | Semua ICTSO, Ketua Pegawai Keselamatan yang dilantik (jika berkaitan) |
| **DM-050102** | **Kawalan Masuk Fizikal** | |
| | Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Setiap pengguna KPKK hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;<br><br>b. Setiap pelawat boleh mendapat Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan;<br><br>c. Semua pas keselamatan hendaklah diserahkan balik kepada bahagian berkenaan apabila pengguna berhenti atau bersara;<br><br>d. Setiap pelawat hendaklah mendaftar di pintu utama terlebih dahulu;<br><br>e. Kehilangan pas mestilah dilaporkan dengan segera; dan | Semua Pengguna dan Pelawat |

| | | |
|---|---|---|
| | f. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT KPKK. | |
| **DM-050103** | **Kawasan Larangan** | |
| | Semua pengguna dilarang berada di Pusat Data (*Data Centre*) KPKK/Jabatan/Agensi kecuali dengan kebenaran dan/atau ditemani oleh pegawai yang diberi kuasa. Pusat Data merupakan kawasan larangan yang dihadkan kemasukannya bagi melindungi aset ICT KPKK yang terdapat di dalam kawasan tersebut.<br><br>Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya. | Semua Pengguna |
| | **Keselamatan Peralatan** | |
| Objektif : Melindungi peralatan dan maklumat daripada kehilangan, kerosakan, kecurian atau salah guna yang mendatangkan gangguan. | | |
| **DM-050201** | **Peralatan ICT** | |
| | Semua pengguna perlu mematuhi langkah-langkah keselamatan seperti berikut :-<br><br>a. Menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna;<br><br>b. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;<br><br>c. Bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;<br><br>d. Dilarang sama sekali menambah, menanggalkan atau mengganti sebarang perkakasan ICT yang telah ditetapkan;<br><br>e. Dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem;<br><br>f. Memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan seperti *hard disk*, disket, *thumbdrive* dan *external hard disk*;<br><br>g. Melindungi semua peralatan sokongan ICT daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna;<br><br>h. Bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah jagaan dan/atau kawalannya; | Semua Pengguna |

i. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS);

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

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

l. Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden;

m. Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

n. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ianya ditempatkan tanpa kebenaran Pegawai Aset/ Pentadbir Sistem ICT KPKK;

o. Sebarang kerosakan perkakasan ICT KPKK hendaklah dilaporkan kepada Pentadbir Sistem ICT KPKK untuk di baik pulih;

p. Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT KPKK tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

q. Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal;

r. Dilarang sama sekali mengubah *password administrator* yang telah ditetapkan oleh pihak ICT;

s. Bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;

t. Memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan “OFF” apabila meninggalkan pejabat; dan

u. Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO KPKK/Jabatan/Agensi.

| | | |
|---|---|---|
| **DM-050202** | **Media Storan** | |
| | Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, *external hard disk* dan media storan lain.<br><br>Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.<br><br>Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :-<br><br>a. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;<br><br>b. Bagi media storan yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu;<br><br>c. Semua media storan data yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat;<br><br>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;<br><br>e. Media storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang dikategorikan selamat. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja;<br><br>f. Akses dan pergerakan kepada media storan perlu direkodkan;<br><br>g. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; dan<br><br>h. Mengadakan salinan atau penduaan (data *backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data. | Semua Pengguna |
| **DM-050203** | **Media Perisian dan Aplikasi** | |
| | Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :-<br><br>a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan di Kementerian/Jabatan/Agensi;<br><br>b. Sistem aplikasi dalaman tidak dibenarkan diagih/didemontrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT;<br><br>c. Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada media storan | Semua Pengguna |

| | | |
|---|---|---|
| | berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan<br><br>d. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan. | |
| **DM-050204** | **Penyelenggaraan** | |
| | Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.<br><br>Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :-<br><br>a. Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;<br><br>b. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan;<br><br>c. Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja;<br><br>d. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; dan<br><br>e. Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan. | Semua Pegawai Aset, Pentadbir Sistem ICT Kementerian/ Jabatan/Agensi |
| **DM-050205** | **Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat** | |
| | Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko.<br><br>Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :-<br><br>a. Mendapatkan kelulusan Pegawai Aset/ Pentadbir Sistem ICT Kementerian/Jabatan/Agensi bagi membawa keluar peralatan atau maklumat tertakluk kepada tujuan yang dibenarkan; dan<br><br>b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan bagi tujuan pemantauan. | Semua Pengguna |
| **DM-050206** | **Pengendalian Peralatan Luar Yang Dibawa Masuk/Keluar** | |
| | Bagi peralatan yang dibawa masuk/keluar pejabat, langkah-langkah keselamatan yang perlu diambil adalah seperti berikut :- | Semua Pengguna |

| | | |
|---|---|---|
| | a. Memastikan peralatan yang dibawa masuk tidak mengancam keselamatan ICT KPKK;<br><br>b. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh KPKK/Jabatan/Agensinya bagi membawa masuk/keluar peralatan (Lampiran C - Borang Pengisytiharan Barang Keluar/Masuk); dan<br><br>c. Memastikan peralatan yang dibawa keluar tidak mengandungi maklumat Kerajaan. | |
| **DM-050207** | **Pelupusan** | |
| | Pelupusan melibatkan semua peralatan ICT KPKK yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori.<br><br>Peralatan ICT yang hendak dilupuskan perlu melalui proses pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KPKK.<br><br>Langkah-langkah seperti berikut hendaklah diambil :-<br><br>a. Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;<br><br>b. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;<br><br>c. Media storan (*internal/external hard disk*) hendaklah dikeluarkan dan disimpan di tempat yang telah dikhaskan dengan ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;<br><br>d. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset dan Stor (MyAsset);<br><br>e. Pelupusan peralatan ICT KPKK hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; | Semua Pegawai Aset, Pentadbir Sistem ICT |
| | f. Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut :-<br><br>i. Menyimpan mana-mana peralatan ICT KPKK yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggalkan dan menyimpan komponen dalaman CPU seperti RAM, *Hard disk*, *Motherboard* dan sebagainya;<br><br>ii. Menyimpan dan memindahkan perkakasan tambahan komputer seperti UPS, speaker atau mana-mana peralatan yang berkaitan ke mana-mana bahagian di Kementerian/Jabatan/Agensi; | Semua Pengguna |

| | | |
|---|---|---|
| | iii. Membawa keluar dari pejabat mana-mana peralatan ICT KPKK yang hendak dilupuskan;dan<br><br>iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab KPKK.<br><br>g. Semua Pengguna ICT KPKK bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin kepada media storan kedua seperti disket atau *thumbdrive* sebelum maklumat tersebut dihapuskan daripada peralatan komputer yang hendak dilupuskan. | |
| **DM-050208** | ***Clear Desk* dan *Clear Screen*** | |
| | Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.<br><br>*Clear Desk* bermaksud tidak meninggalkan sebarang maklumat penting di atas meja apabila pengguna tidak berada di tempatnya.<br><br>*Clear Screen* bermaksud tidak memaparkan sebarang maklumat penting di paparan skrin apabila pengguna tidak berada di tempatnya.<br><br>Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :-<br><br>a. Menggunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer;<br><br>b. Maklumat-maklumat penting hendaklah disimpan di dalam laci atau kabinet fail yang berkunci; dan<br><br>c. Semua dokumen hendaklah diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat atau media output yang lain. | Semua Pengguna |
| | **Keselamatan Persekitaran** | |
| Objektif : Melindungi aset ICT KPKK dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan. | | |
| **DM-050301** | **Kawalan Persekitaran** | |
| | Bagi mengelakkan kerosakan terhadap pejabat dan aset ICT KPKK, semua cadangan berkaitan pejabat sama ada urusan perolehan, penyewaan atau pengubahsuaian hendaklah dirujuk terlebih dahulu kepada pegawai yang berkenaan.<br><br>Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil :- | Semua Pengguna |

| | | |
|---|---|---|
| | a. Merancang dan menyediakan pelan keseluruhan susun atur ruang pejabat yang menempatkan pusat data, bilik percetakan, peralatan komputer dan sebagainya dengan teliti;<br><br>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;<br><br>c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dilihat dan dikendalikan;<br><br>d. Bahan mudah terbakar hendaklah disimpan di luar kawasan penyimpanan aset ICT;<br><br>e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT;<br><br>f. Pengguna dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan<br><br>g. Semua peralatan perlindungan hendaklah diperiksa dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu. | |
| **DM-050302** | **Kabel** | |
| | Kabel komputer hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut :-<br><br>a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;<br><br>b. Melindungi kabel daripada sebarang kerosakan;<br><br>c. Memastikan laluan pemasangan kabel yang sesuai; dan<br><br>d. Membuat pelabelan kabel. | Semua ICTSO |
| **DM-050303** | **Bekalan Kuasa** | |
| | Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.<br><br>Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa :-<br><br>a. Semua peralatan ICT KPKK hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang | Semua ICTSO |

| | | |
|---|---|---|
| | sesuai hendaklah disalurkan kepada peralatan ICT;<br><br>b. Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan<br><br>c. Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual. | |
| **DM-050304** | **Prosedur Kecemasan** | |
| | Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :-<br><br>a. Hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada 'Garis Panduan Keselamatan KPKK 2007'; dan<br><br>b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada pegawai yang berkenaan. | Semua Pengguna |
| | **Keselamatan Dokumen dan Sistem Dokumentasi** | |
| **DM-050401** | **Dokumen** | |
| | Bagi memastikan integriti maklumat, semua pengguna perlu mengambil langkah-langkah berikut :-<br><br>a. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin;<br><br>b. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada;<br><br>c. Setiap dokumen hendaklah di fail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;<br><br>d. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur Arahan Keselamatan;<br><br>e. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan;<br><br>f. Pelupusan dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan<br><br>g. Menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik. | Semua Pengguna |

## PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

| Objektif | | |
|---|---|---|
| Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan. | | |
| **Pengurusan Prosedur Operasi** | | |
| **DM-060101 Pengendalian Prosedur** | | |
| | Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Semua prosedur keselamatan ICT KPKK yang di wujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal;<br><br>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<br><br>c. Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan. | Semua ICTSO |
| **DM-060102 Kawalan Perubahan** | | |
| | Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai yang berkenaan atau pemilik aset ICT terlebih dahulu;<br><br>b. Aktiviti-aktiviti seperti memasang, menyenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pegawai yang berkenaan dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;<br><br>c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan<br><br>d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak. | Semua Pengguna |

| | | |
|---|---|---|
| **DM-060103** | **Pengasingan Tugas dan Tanggungjawab** | |
| | Skop tugas dan tanggung jawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahan yang tidak dibenarkan ke atas aset ICT.<br><br>Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. | Semua Pengurus ICT, ICTSO |
| | **Perancangan dan Penerimaan Sistem** | |
| Objektif : Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem. | | |
| **DM-060201** | **Perancangan Kapasiti** | |
| | Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan<br><br>b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. | Semua ICTSO dan Pentadbir Sistem ICT |
| **DM-060202** | **Penerimaan Sistem** | |
| | Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. | Semua ICTSO dan Pentadbir Sistem ICT |
| | **Perisian Berbahaya** | |
| Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan trojan. | | |
| **DM-060301** | **Perlindungan dari Perisian Berbahaya** | |
| | Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan *Intrusion Prevention System* (IPS) dan mengikut prosedur penggunaan yang betul dan selamat; | Semua ICTSO dan Pentadbir Sistem ICT |

| | | |
|---|---|---|
| | b. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;<br><br>c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;<br><br>d. Mengemas kini *pattern* anti virus dari semasa ke semasa;<br><br>e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;<br><br>f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;<br><br>g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;<br><br>h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian/aplikasi yang dibangunkan; dan<br><br>i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus. | |
| ***Housekeeping*** | | |
| Objektif : Melindungi integriti maklumat dan perkhidmatan komunikasi agar sentiasa boleh diakses. | | |
| **DM-060401** | ***Backup*** | |
| | Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan di simpan.<br><br>Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;<br><br>b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi;<br><br>c. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; | Semua Pentadbir Sistem ICT |

| | | |
|---|---|---|
| | d. *Backup* hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat; dan<br><br>e. Menyimpan sekurang-kurangnya tiga (3) generasi *backup*. | |
| **DM-060402** | **Sistem Log** | |
| | Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;<br><br>b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan<br><br>c. Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO Kementerian/ Jabatan/Agensi. | Semua Pentadbir Sistem ICT |
| | **Pengurusan Rangkaian** | |
| Objektif : Melindungi maklumat dalam rangkaian dan infrastruktur sokongan. | | |
| **DM-060501** | **Kawalan Infrastruktur Rangkaian** | |
| | Infrastruktur rangkaian mestilah di kawal dan diuruskan sebaik mungkin bagi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan :-<br><br>a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;<br><br>b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;<br><br>c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;<br><br>d. Semua peralatan mestilah melalui proses *User Acceptance Test* (UAT) semasa pemasangan dan konfigurasi;<br><br>e. *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta di konfigurasi;<br><br>f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan KPKK; | Semua Pentadbir Sistem ICT |

| | | |
|---|---|---|
| | g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO Kementerian/ Jabatan/Agensi;<br><br>h. Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat KPKK;<br><br>i. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;<br><br>j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan KPKK hendaklah mendapat kebenaran ICTSO;<br><br>k. Semua pengguna hanya dibenarkan menggunakan rangkaian KPKK sahaja. Penggunaan modem dan rangkaian KPKK secara serentak adalah dilarang sama sekali;<br><br>l. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan; dan<br><br>m. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum. | |
| **Pengurusan Media** | | |
| Objektif : Melindungi aset ICT KPKK dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal. | | |
| **DM-060601** | **Penghantaran dan Pemindahan** | |
| | Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pentadbir Sistem Kementerian/Jabatan/Agensi terlebih dahulu. | Semua Pengguna |
| **DM-060602** | **Prosedur Pengendalian Media** | |
| | Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;<br><br>b. Mengehadkan dan menentukan capaian media kepada pengguna yang sah sahaja;<br><br>c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan;<br><br>d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; | Semua Pentadbir Sistem ICT |

| | | |
|---|---|---|
| | e. Menyimpan semua media di tempat yang selamat; dan<br><br>f. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat. | |
| **DM-060603** | **Pengurusan Pertukaran Maklumat** | |
| | Pengurusan Pertukaran Maklumat bertujuan untuk memastikan keselamatan pertukaran maklumat dan perisian dalam agensi dan mana-mana entiti luar terjamin.<br><br>Langkah-langkah bagi Pengurusan Pertukaran Maklumat adalah seperti berikut :-<br><br>a. Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;<br><br>b. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara KPKK dengan pihak luar;<br><br>c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KPKK;<br><br>d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan<br><br>e. Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat KPKK. | Semua Pengguna |
| | **Keselamatan Komunikasi** | |
| Objektif : Melindungi aset ICT KPKK melalui sistem komunikasi yang selamat. | | |
| **DM-060701** | **Mel Elektronik (E-mel)** | |
| | Penggunaan e-mel KPKK hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan” dan mana-mana undang-undang bertulis yang berkuat kuasa.<br><br>Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh KPKK sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; | Semua Pengguna |

b. Penggunaan e-mel rasmi bagi tujuan peribadi adalah tidak dibenarkan;

c. Setiap e-mel yang disediakan perlu mematuhi format yang telah ditetapkan oleh KPKK;

d. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;

e. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;

f. Penggunaan fail kepilan (*attachment*) dibuat sekiranya perlu, tidak melebihi empat puluh (40) megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

g. Penghantaran lampiran dalam format/*extension " *.exe, *.bat, *.hta, *.cmd* dan *.com"* tidak dibenarkan;

h. Mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;

i. Mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

j. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;

k. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

l. Tentukan tarikh dan masa sistem komputer adalah tepat;

m. Hanya warga KPKK/Jabatan/Agensi sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi KPKK/Jabatan/Agensi;

n. Fungsi *Auto-Reply* adalah tidak dibenarkan kecuali pengguna yang bercuti atau bertugas di luar pejabat iaitu dengan menggunakan mesej *Out-of-Office*;

o. Bahagian Pentadbiran dan Pengurusan Sumber Manusia KPKK/Jabatan/Agensi perlu memaklumkan sebarang status pengguna (bertukar Jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke KPKK/Jabatan/Agensi bagi tujuan pengemaskinian e-mel yang terlibat; dan

p. Pengguna adalah mewakili diri sendiri dan bertanggungjawab ke atas maklumat yang dikeluarkan

| | | |
|---|---|---|
| | dalam setiap perhubungan yang dibuat secara elektronik. | |
| **DM-060702** | **Pengurusan Penyampaian Perkhidmatan Pihak Ketiga** | |
| | Memastikan pelaksanaan dan penyenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.<br><br>Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dilaksanakan dan diselenggarakan oleh pihak ketiga;<br><br>b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak dan diaudit dari semasa ke semasa; dan<br><br>c. Pengurusan kepada perubahan penyediaan perkhidmatan termasuk menyelenggarakan dan menambahbaikkan polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko. | Semua ICTSO dan Pihak Ketiga |
| **DM-060703** | **Pemantauan** | |
| | Bertujuan memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, di antaranya seperti berikut :-<br><br>a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;<br><br>b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu di wujud dan hasilnya perlu dipantau secara berkala;<br><br>c. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;<br><br>d. Aktiviti pentadbiran dan operator sistem perlu direkodkan;<br><br>e. Kesalahan, kesilapan dan / atau penyalahgunaan perlu di log, dianalisis dan diambil tindakan sewajarnya; dan<br><br>f. Masa yang berkaitan dengan sistem pemprosesan maklumat dalam KPKK atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui. | Semua Pentadbir Sistem ICT |

## PERKARA 07 KAWALAN CAPAIAN

| Objektif | | |
|---|---|---|
| Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT KPKK. | | |
| **Dasar Kawalan Capaian** | | |
| **DM-070101 Keperluan Dasar** | | |
| | Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. | Semua Pentadbir Sistem ICT |
| **Pengurusan Capaian Pengguna** | | |
| Objektif : Mengawal capaian pengguna ke atas aset ICT KPKK. | | |
| **DM-070201 Akaun Pengguna** | | |
| | Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan langkah-langkah berikut hendaklah dipatuhi :-<br><br>a. Akaun yang diperuntukkan sahaja boleh digunakan;<br><br>b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;<br><br>c. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan yang ditetapkan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;<br><br>d. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan<br><br>e. Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut :-<br><br>i) Pengguna bercuti panjang;<br>ii) Bertukar bidang tugas kerja;<br>iii) Bertukar ke agensi lain;<br>iv) Bersara; atau<br>v) Ditamatkan perkhidmatan. | Semua Pengguna |
| **DM-070202 Hak Capaian** | | |
| | Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas. | Semua Pentadbir Sistem ICT |

| | | |
|---|---|---|
| **DM-070203** | **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 seperti berikut :-<br><br>a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;<br><br>b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau di kompromi;<br><br>c. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf dan nombor (alphanumerik) manakala kata laluan bagi pembangunan aplikasi sistem yang baru mestilah sekurang-kurangnya dua belas (12) aksara dengan kombinasi aksara, angka dan aksara khas berkuat kuasa Januari 2008;<br><br>d. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;<br><br>e. Kata laluan w*indows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;<br><br>f. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;<br><br>g. Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula;<br><br>h. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; dan<br><br>i. Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan. | Semua Pengguna |
| **DM-070204** | **Kad Pintar** | |
| | a. Penggunaan kad pintar Kerajaan elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan elektronik yang dikhususkan.<br><br>b. Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain;<br><br>c. Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan | Semua Pengguna KPKK yang terlibat |

| | | |
|---|---|---|
| | d. Sebarang kehilangan, kerosakan dan kata laluan disekat terhadap kad pintar perlu dimaklumkan kepada pihak ICT masing-masing. | |
| **Kawalan Capaian** | | |
| Objektif : Menghalang capaian yang tidak sah dan tanpa kebenaran serta boleh menyebabkan kerosakan. | | |
| **DM-070301** | **Kawalan Capaian Rangkaian** | |
| | Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Memastikan pengguna membuat capaian pada sistem yang dibenarkan sahaja;<br><br>b. Mewujudkan mekanisme pengesahan yang sesuai untuk mengawal capaian oleh pengguna jarak jauh;<br><br>c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; dan<br><br>d. Mewujud dan melaksanakan kawalan pengalihan laluan (*routing control*) untuk memastikan rangkaian boleh diakses oleh pengguna. | Semua Pentadbir Sistem ICT |
| **DM-070302** | **Capaian Jarak Jauh** | |
| | a. Penghantaran maklumat yang menggunakan capaian jarak jauh menggunakan kaedah ***Remote Access*** mestilah menggunakan kaedah penyulitan (*encryption*);<br><br>b. Lokasi bagi akses ke sistem ICT KPKK hendaklah dipastikan selamat ; dan<br><br>c. Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada CIO. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini. | Semua Pengguna |
| **DM-070303** | **Capaian Internet** | |
| | a. Penggunaan Internet hendaklah dipantau secara berterusan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code,* virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian KPKK/Jabatan/ Agensinya; | Semua Pentadbir Sistem ICT |
| | b. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; | Semua Pengurus ICT |
| | c. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; | Semua Pentadbir Sistem ICT |

| | | |
|---|---|---|
| | d. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing*, *video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan;<br><br>e. Penggunaan modem telefon untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali;<br><br>f. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut :-<br>i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video/audio, lagu yang boleh menjejaskan tahap capaian Internet; dan<br><br>ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.<br><br>g. Pengguna hendaklah berhenti dan memutuskan talian dengan serta merta sekiranya menerima dan disambungkan ke laman Internet yang mengandungi unsur-unsur tidak menyenangkan. | Semua Pentadbir Sistem ICT<br><br>Semua Pengguna |
| **Kawalan Capaian Sistem dan Aplikasi** | | |
| Objektif : Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. | | |
| **DM-070401** | **Capaian Sistem Pengoperasian** | |
| | Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan.<br><br>Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi :-<br><br>a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan;<br><br>b. Merekodkan capaian yang berjaya dan gagal; dan<br><br>c. Membekalkan kemudahan untuk pengesahan; bagi sistem kata kunci digunakan, kualiti kata kunci perlu mendapat pengesahan.<br><br>Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut :-<br><br>a. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Jabatan;<br><br>b. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* | Semua Pentadbir Sistem ICT, ICTSO |

| | | |
|---|---|---|
| | c. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; dan<br><br>d. Menyediakan tempoh penggunaan mengikut kesesuaian.<br><br>Perkara-perkara yang perlu dipatuhi termasuk berikut :-<br><br>a. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin;<br><br>b. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna;<br><br>c. Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti;<br><br>d. Mengehadkan dan mengawal penggunaan program utiliti yang berkemampuan bagi satu tempoh yang ditetapkan; dan<br><br>e. Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi. | |
| **DM-070402** | **Sistem Maklumat dan Aplikasi** | |
| | Capaian sistem dan aplikasi di KPKK adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi :-<br><br>a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan;<br><br>b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini;<br><br>c. Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan;<br><br>d. Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;<br><br>e. Memastikan kawalan sistem adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan | Semua Pentadbir Sistem ICT, ICTSO |

| | | |
|---|---|---|
| | f. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimana pun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja. | |
| | **Audit** | |
| **DM-070501** | **Pengauditan dan Forensik ICT** | |
| | ICTSO mestilah bertanggungjawab merekod dan menganalisa :-<br><br>a. Sebarang percubaan pencerobohan kepada sistem ICT KPKK;<br><br>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*);<br><br>c. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;<br><br>d. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti Kerajaan;<br><br>e. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;<br><br>f. Aktiviti instalasi dan penggunaan perisian yang membebankan *bandwidth* rangkaian;<br><br>g. Aktiviti penyalahgunaan akaun e-mel; dan<br><br>h. Aktiviti penukaran *IP address* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem.<br><br>Langkah-langkah yang perlu diambil adalah seperti berikut :-<br><br>a. ICTSO akan menentukan prosedur pengumpulan bahan bukti (*hard disk*/media storan) yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan;<br><br>b. Proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat; dan<br><br>c. Sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, laporan khas perlu disediakan.<br><br>Semua proses dan hasil siasatan adalah SULIT. | Semua ICTSO |

| DM-070502 | Jejak Audit | |
|---|---|---|
| | Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem.<br><br>Aktiviti jejak audit mengandungi :-<br><br>a. Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan;<br><br>b. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya;<br><br>c. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan;<br><br>d. Catatan jejak audit dari semasa ke semasa untuk membantu mengesan aktiviti yang tidak normal dengan lebih awal;<br><br>e. Menyediakan laporan jika perlu; dan<br><br>f. Aktiviti perlindungan dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubah suaian yang tidak dibenarkan. | Semua Pentadbir Sistem ICT |

## PERKARA 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

| Objektif | | |
|---|---|---|
| Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian. | | |
| **Keselamatan Dalam Membangunkan Sistem dan Aplikasi** | | |
| **DM-080101** | **Keperluan Keselamatan** | |
| | Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>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;<br><br>b. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; dan<br><br>c. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan. | Semua Pentadbir Sistem ICT, ICTSO |
| **DM-080102** | **Pengesahan Data Input** | |
| | Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian. | Semua Pentadbir Sistem ICT |
| **DM-080103** | **Kawalan Prosesan** | |
| | Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan. | Semua Pentadbir Sistem ICT |
| **DM-080104** | **Pengesahan Data Output** | |
| | Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat. | Semua Pentadbir Sistem ICT |
| **Kriptografi** | | |
| Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat. | | |
| **DM-080201** | **Penyulitan** | |
| | Pengguna hendaklah membuat penyulitan (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa. | Semua Pengguna |

| | | |
|---|---|---|
| **DM-080202** | **Pengurusan Infrastruktur Kunci Awam (PKI)** | |
| | Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, di musnah dan didedahkan sepanjang tempoh sah kunci tersebut. | Semua Pengguna |
| | **Fail Sistem** | |
| Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat. | | |
| **DM-080301** | **Kawalan Fail Sistem** | |
| | Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Proses pengemas kini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;<br><br>b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji;<br><br>c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubah suaian tanpa kebenaran, penghapusan dan kecurian; dan<br><br>d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan. | Semua Pentadbir Sistem ICT |
| | **Pembangunan dan Sokongan Sistem** | |
| Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi. | | |
| **DM-080401** | **Kawalan Perubahan** | |
| | Perubahan atau pengubah suaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai. | Semua Pentadbir Sistem ICT |
| **DM-080402** | **Pembangunan Secara *Outsource*** | |
| | Pembangunan perisian aplikasi secara *outsource* perlu dipantau oleh BPM KPKK.<br><br>*Source code* adalah menjadi hak milik KPKK. | Semua Pentadbir Sistem ICT |
| **DM-080403** | **Kawalan dari Ancaman Teknikal** | |
| | Maklumat mengenai ancaman teknikal sistem maklumat yang digunakan perlu diperolehi. Pendedahan organisasi kepada ancaman teknikal perlu dinilai bagi mengenal pasti tahap risiko yang bakal dihadapi. | Semua Pentadbir Sistem ICT |

## PERKARA 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

| Objektif | | |
|---|---|---|
| Untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan dan memastikan sistem ICT KPKK dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej KPKK/Jabatan/Agensinya dan sistem penyampaian perkhidmatan. | | |
| **Pengurusan Insiden Keselamatan ICT** | | |
| **DM-090101** | **Mekanisme Pelaporan Insiden Keselamatan ICT** | |
| | Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada CERT KPKK dengan kadar segera :-<br><br>a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;<br><br>b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;<br><br>c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;<br><br>d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan<br><br>e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.<br><br>Sekiranya berlaku insiden keselamatan ICT, maka mekanisme pelaporan adalah seperti berikut :- | Semua Pengguna |
| | **i. Pelaporan**<br>Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO dan kepada CERT KPKK untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. | Semua Pengguna |
| | **ii. CERT KPKK**<br>Pasukan CERT KPKK akan bertindak menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai *input* atau untuk tindakan seterusnya. | CERT KPKK |
| | **iii. Tanggungjawab Pengguna**<br>Semua pengguna yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden keselamatan ICT kepada ICTSO, kerentanan (*vulnerabality*) yang diperhatikan atau disyaki terdapat dalam sistem maklumat menerusi mekanisme pelaporan ini. Ini adalah bagi | Semua Pengguna |

| | | |
|---|---|---|
| | mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan menceroboh.<br><br>**iv. Tindakan Dalam Keadaan Berisiko Tinggi**<br>Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak. | Semua CIO, ICTSO |
| **DM-090102** | **Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT** | |
| | Semua pegawai pasukan pengendali insiden keselamatan ICT atau CERT KPKK perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur operasi standard keselamatan CERT KPKK dan GCERT.<br><br>CERT KPKK menerima aduan atau laporan daripada pengguna, laporan yang dikesan dari PRISMA atau laporan dari sumber luar. Seterusnya, maklumat tentang insiden akan didaftarkan. Siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden tersebut. Laporan insiden kemudiannya dimaklumkan kepada GCERT MAMPU. Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan dipanjangkan kepada agensi penguat kuasa undang-undang.<br><br>CERT KPKK yang diketuai oleh Pengurus ICT akan menjalankan tindakan pengendalian secara capaian jarak jauh (*remote*) atau *on-site.* Sekiranya laporan tersebut memerlukan bantuan GCERT MAMPU, permohonan perlu dihantar bagi mendapatkan maklum balas GCERT MAMPU.<br><br>Bagi laporan yang memerlukan bantuan daripada CERT agensi yang lain, permohonan perlu dihantar melalui GCERT MAMPU dan khidmat nasihat akan disalurkan. CERT KPKK seterusnya akan menyediakan laporan dan ICTSO mengesahkan sekiranya Pelan Kesinambungan Perkhidmatan / *Business Resumption Plan* (*BRP*) perlu diaktifkan atau sebaliknya. Pengesahan perlu dihantar kepada CIO bagi mengaktifkan *BRP*.<br><br>Laporan insiden yang tidak memerlukan *BRP* akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan.<br><br>Carta lengkap mengenai perjalanan laporan insiden seperti di Lampiran B. | CERT KPKK |
| **DM-090103** | **Pengurusan Maklumat Insiden Keselamatan ICT** | |
| | Perkara yang perlu dipatuhi adalah seperti berikut :-<br><br>a. Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan dan tindakan untuk melaksanakan peningkatan dan kawalan tambahan bagi mengawal | Semua ICTSO |

| | | |
|---|---|---|
| | kekerapan, kerosakan dan kos kejadian insiden akan datang, dan untuk tujuan mengkaji semula dasar-dasar keselamatan aset ICT sedia ada. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada KPKK/Jabatan/Agensinya;<br><br>b. Memastikan bahan-bahan bukti berkaitan insiden keselamatan ICT dapat disediakan, disimpan, disenggarakan dan mempunyai perlindungan keselamatan. Penyediaan bahan-bahan bukti seperti jejak audit, *backup* secara berkala dan media *backup offline* hendaklah mengikut amalan terbaik yang disarankan oleh Kerajaan dari semasa ke semasa;<br><br>c. Memastikan semua bahan bukti adalah selaras dengan peraturan pengumpulan maklumat dari segi kualiti, kelengkapan dan kebolehpercayaan bahan bukti yang termaktub dalam bidang kuasa perundangan berkenaan; dan<br><br>d. Perkara-perkara yang mesti dipatuhi termasuk yang berikut :-<br><br>i. Melindungi Integriti semua bahan bukti;<br>ii. Menyalin bahan bukti oleh personel yang dipertanggungjawabkan;<br>iii. Merekodkan semua maklumat aktiviti penyalinan termasuk pegawai terlibat, media, perisian, perkakasan dan *tools* yang digunakan;<br>iv. Memaklumkan pihak berkuasa perundangan, seperti pegawai undang-undang dan polis (jika perlu); dan<br>v. Mendapatkan nasihat dari pihak berkuasa perundangan ke atas bahan bukti yang perlukan. | |

## PERKARA 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

| Objektif | | |
|---|---|---|
| Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan. | | |
| **Dasar Kesinambungan Perkhidmatan** | | |
| **DM-100101** | **Pelan Kesinambungan Perkhidmatan** | |
| | Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian :-<br><br>a. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;<br><br>b. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;<br><br>c. Mendokumentasikan proses dan prosedur yang telah dipersetujui;<br><br>d. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;<br><br>e. Membuat penduaan; dan<br><br>f. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. | Semua ICTSO |
| **DM-100102** | **Pengurusan Kesinambungan Perkhidmatan** | |
| | Pengurusan Kesinambungan Perkhidmatan adalah mekanisme bagi mengurus dan memastikan kepentingan *stakeholder* sistem penyampaian perkhidmatan dilindungi dan imej KPKK terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan KPKK di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan.<br><br>Pengurus ICT adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT KPKK. | Semua ICTSO |

## PERKARA 11 PEMATUHAN

| Objektif | | |
|---|---|---|
| Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada DKICT KPKK. | | |
| **Pematuhan dan Keperluan Perundangan** | | |
| **DM-110101** | **Pematuhan Dasar** | |
| | DKICT KPKK dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa hendaklah dibaca, difahami dan dipatuhi.<br><br>Semua aset ICT KPKK termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. | Semua Pengguna |
| **DM-110102** | **Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal** | |
| | ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.<br><br>Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi standard pelaksanaan keselamatan. | Semua ICTSO |
| **DM-110103** | **Pematuhan Keperluan Audit** | |
| | Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat.<br><br>Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.<br><br>Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan. | Semua Pengguna |
| **DM-110104** | **Keperluan Perundangan** | |
| | Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi :-<br><br>a. Arahan Keselamatan;<br><br>b. *"Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS)";<br><br>c. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"; | Semua Pengguna |

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

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

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

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

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

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

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

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

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

m. Akta Rahsia Rasmi 1972;

n. Akta Tandatangan Digital 1997;

o. Akta Jenayah Komputer 1997;

p. Akta Hak cipta (Pindaan) Tahun 1997;

q. Akta Komunikasi dan Multimedia 1998;

r. Arahan Teknologi Maklumat 2007;

s. Perintah-Perintah Am; dan

t. Arahan Perbendaharaan.

| Tindakan Tatatertib | | |
|---|---|---|
| Objektif : Meningkatkan kesedaran dan pematuhan ke atas DKICT KPKK. | | |
| **DM-110201** | **Pelanggaran Dasar / Perundangan** | |
| | Pelanggaran DKICT KPKK dan semua perbuatan kecuaian, kelalaian dan pelanggaran keselamatan yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 akan dikenakan tindakan tatatertib. | Semua Pengguna |

| GLOSARI | |
|---|---|
| *Antivirus* | Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM 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* | Lebar Jalur<br>Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan. |
| CERT KPKK | Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya. |
| CIO | *Chief Information Officer*<br>Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi. |
| *Denial of service* | Halangan pemberian perkhidmatan. |
| *DKICT KPKK* | Dasar Keselamatan ICT KPKK dan semua Jabatan/Agensi di bawahnya. |
| *Downloading* | Aktiviti muat-turun sesuatu perisian. |
| *Encryption* | Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah. |
| *Firewall* | Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya. |
| *Forgery* | Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft / espionage*), penipuan(*hoaxes*). |
| GCERT | *Government Computer Emergency Response Team* atau Pasukan Pengendali Insiden Keselamatan ICT Kerajaan. |
| *Hard disk* | Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas. |
| *Hub* | Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain. |
| ICT | *Information and Communication Technology*.(Teknologi Maklumat dan Komunikasi). |
| ICTSO | *ICT Security Officer*<br>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 Prevention System (IPS)* | Sistem Pencegah Pencerobohan<br>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. |
| KPKK | Kementerian Penerangan Komunikasi dan Kebudayaan |
| LAN | *Local Area Network*<br>Rangkaian Kawasan Setempat yang menghubungkan 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<br>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. |
| *Outsource* | Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui. |
| Perisian Aplikasi | Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau Jabatan. |
| Pihak Ketiga | Kontraktor, Pembekal, Pakar Runding dan pihak-pihak lain yang berkepentingan |
| *Public-Key Infrastructure (PKI)* | Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet. |
| *Router* | Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet. |
| *Screen saver* | Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu. |
| *Server* | Pelayan komputer |
| *Switches* | Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku. |
| *Threats* | Gangguan dan ancaman 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 bersambung. |
| *Video Conferencing* | 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* LAN | Jaringan komputer yang terhubung tanpa melalui kabel. |

**Lampiran A**

**SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT**
**KEMENTERIAN PENERANGAN KOMUNIKASI DAN KEBUDAYAAN**

Nama : …….....

No. Kad Pengenalan : …….

Jawatan : ……..

Kementerian / Jabatan : ……..

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

☐ Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT: dan

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

.....
( Tanda Tangan Pegawai )

Tarikh : .....

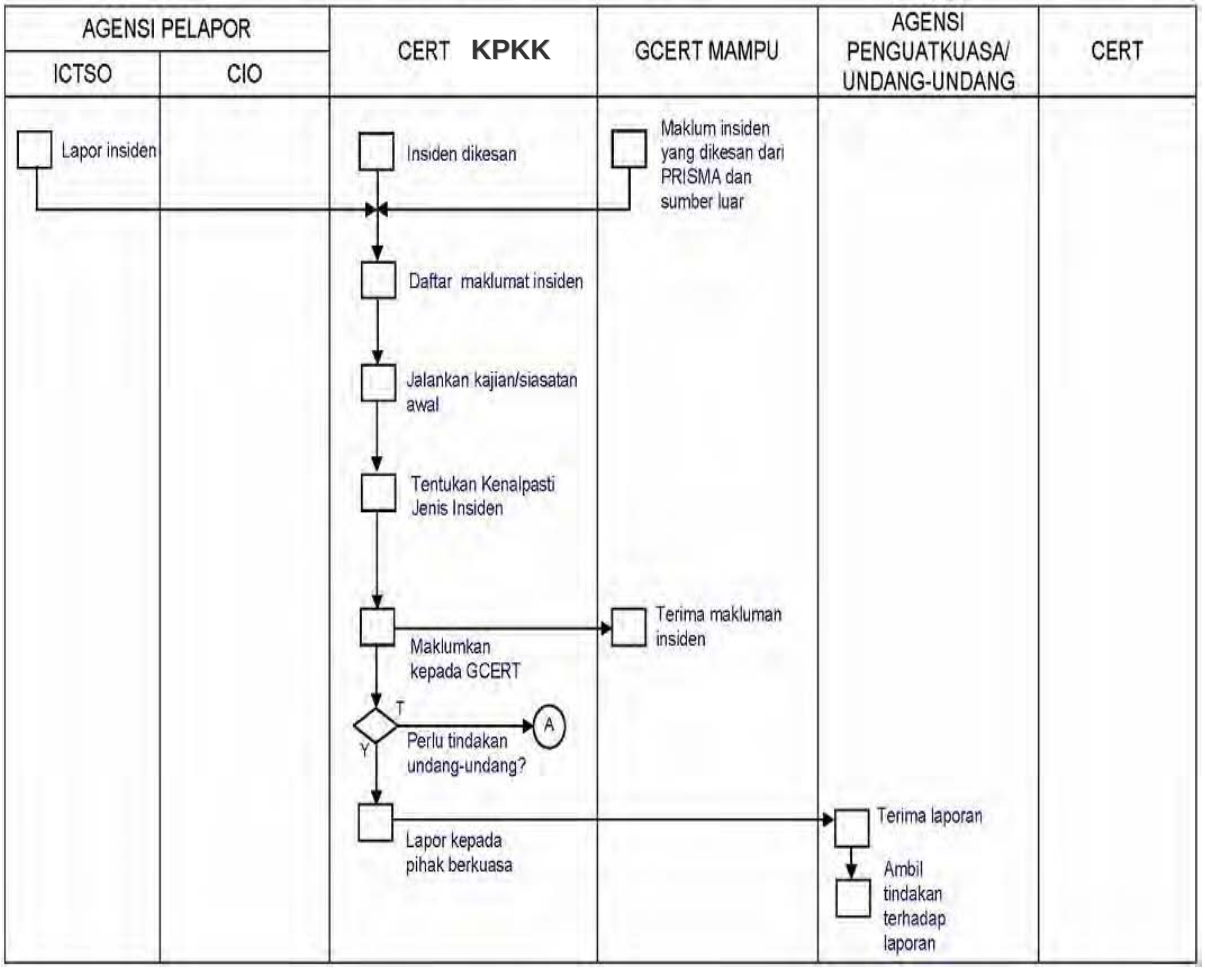
Pengesahan Pegawai Keselamatan ICT

.....
( Nama Pegawai Keselamatan ICT )
b.p Ketua Setiausaha
Kementerian Penerangan Komunikasi dan Kebudayaan

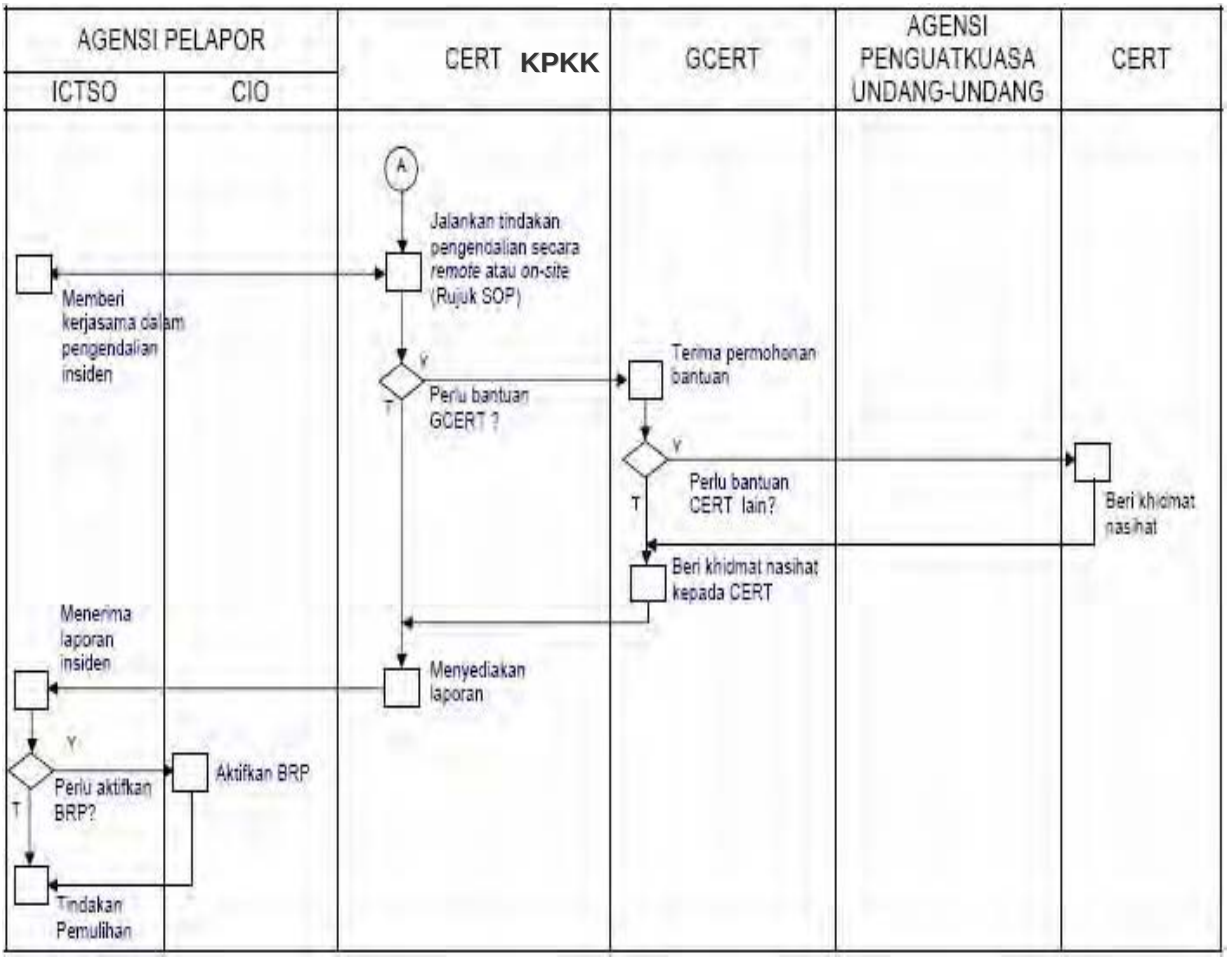
Tarikh : ..... .....

**Lampiran B**

## PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT KPKK



**PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT KPKK**
(Sambungan)



**Lampiran C**

**BORANG PENGISYTIHARAN BARANG KELUAR/MASUK**
**BAHAGIAN KESELAMATAN**
**KEMENTERIAN PENERANGAN KOMUNIKASI DAN KEBUDAYAAN**

Nama : ..... Syarikat : .....

No. Kenderaan : .....

Urusan dengan Bahagian/Unit/Cawangan : .....

**BHG. A : SENARAI BARANG YANG DI BAWA MASUK**

1.
2.
3.
4.
5.

…….. ……..
Tandatangan Pemilik Kenderaan Tandatangan Pengawal Keselamatan

**BHG. : SENARAI BARANG YANG DIBAWA KELUAR**

1.
2.
3.
4.
5.

Disahkan oleh : …….
Tandatangan

Nama :

Jab./Caw./Bhg./Unit :

Tarikh :

***Nota :**

Pihak Tuan hendaklah menentukan dan memastikan barangan yang dikeluarkan mempunyai Surat Kebenaran. Sekiranya tiada, ia boleh dianggap barangan curi dan boleh dirampas oleh Bahagian Keselamatan.