# DASAR KESELAMATAN ICT

## PERBADANAN KEMAJUAN NEGERI MELAKA

## TARIKH KUATKUASA:

## 1 APRIL 2019

## VERSI 1.0

| RUJUKAN | VERSI | TARIKH |
|---|---|---|
| DKICT PKNM | 1.0 | 1 / 4 / 2019 |

# KANDUNGAN

## 1. Pengenalan

Dasar keselamatan ICT (DKICT) PKNM mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT PKNM

## 2. Objektif

Dasar Keselamatan ICT PKNM diwujudkan untuk menjamin kesinambungan urusan PKNM dengan meminimumkan kesan insiden keselamatan ICT.

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

Manakala, objektif utama Keselamatan ICT PKNM ialah seperti berikut:

a) Memastikan kelancaran operasi PKNM dan meminimumkan kerosakan atau kemusnahan.
b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi.
c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

## 3. Skop

Dasar ini meliputi semua sumber atau aset ICT yang terdiri daripada :

i. **Maklumat atau Data** (contoh: fail, dokumen, data elektronik yang mengandungi maklumat-maklumat yang boleh digunakan untuk mencapai misi dan objektif PKNM).

ii. **Manusia** iaitu individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian PKNM bagi mencapai misi dan objektif PKNM.

iii. **Perisian** iaitu program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. (contoh: aplikasi dan sistem perisian),

iv. **Perkakasan** iaitu semua aset yang menyokong keperluan pemprosesan dan penstoran maklumat. Contoh: komputer, peralatan

komunikasi dan media magnet, peralatan komunikasi dan sebagainya).

v. **Perkhidmatan** atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya seperti rangkaian.

vi. Premis komputer dan komunikasi iaitu semua yang menempatkan perkara yang mengandungi perkara (i) – (v)

Dasar ini adalah terpakai oleh semua pengguna di PKNM termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT PKNM.

## 4. Prinsip-prinsip

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT PKNM dan perlu dipatuhi adalah seperti berikut:

### 4.1 Akses atas dasar perlu mengetahui

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

### 4.2 Had akses minimum

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

### 4.3 Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT PKNM;

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.

### 4.4 Pengasingan

Tugas mewujud, memadam, kemaskini, 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;

### 4.5 Pengauditan

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

### 4.6 Pematuhan

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

### 4.7 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

## 5. Dasar Keselamatan ICT

Objektif**:** DKICT PKNM diwujudkan untuk melindungi aset ICT PKNM 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.

### 5.1 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Ketua Pegawai Eksekutif dibantu oleh Unit Teknologi Maklumat, PKNM.

### 5.2 Penyebaran Dasar

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

### 5.3 Penyelenggaraan Dasar

Dasar Keselamatan ICT PKNM 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 Dasar Keselamatan ICT PKNM;

- Kenalpasti dan tentukan perubahan yang diperlukan;
- Kemuka cadangan pindaan secara bertulis kepada Ketua Pegawai Eksekutif untuk pembentangan dan persetujuan Mesyuarat Pengurusan PKNM
- Perubahan yang telah dipersetujui oleh Mesyuarat Pengurusan dimaklumkan kepada semua pengguna; dan
- Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.

### 5.4 Pengecualian Dasar

Dasar keselamatan ICT PKNM adalah terpakai kepada semua pengguna ICT PKNM dan tiada pengecualian diberikan.

## 6. Keselamatan Sumber Manusia

### 6.1 Keselamatan ICT dalam tugas harian

Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT PKNM.

**Tanggungjawab Keselamatan**

- Peranan dan tanggungjawab **pengguna** terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta

dinyatakan di dalam fail meja atau kontrak.

- Keselamatan ICT merangkumi tanggungjawab **pengguna** dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.

**Terma dan Syarat Perkhidmatan**

Semua **kakitangan PKNM** yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa berkuatkuasa.

**Perakuan Akta Rahsia Rasmi**

**Kakitangan PKNM** yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.

### 8.1 Menangani Insiden Keselamatan ICT

Meminimumkan kesan insiden keselamatan ICT.

### 8.2 Pelapor Insiden

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada Pasukan *Computer Emergency Response Team* (CERT) Negeri Melaka dengan kadar segera:

- Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;
- Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;
- Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan;
- Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerapkali gagal dan komunikasi tersalah hantar;
- Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.
- Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan ICT” mengenainya bolehlah dirujuk.

### 8.3 Program Kesedaran Keselamatan ICT

- **Unit Teknologi Maklumat, PKNM** perlu memastikan setiap pengguna di PKNM perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka.
- Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT PKNM.

### 8.4 Pelanggaran Dasar

Pelanggaran dasar ICT PKNM akan dikenakan tindakan tatatertib.

## 9. Keselamatan Fizikal

### 9.1 Keselamatan Kawasan

Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.

#### 9.1.1 Perimeter Keselamatan Fizikal

Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. **Pegawai Keselamatan PKNM** perlu memastikan langkah-langkah keselamatan fizikal tidak terhad kepada langkah- langkah berikut:

- Kawasan keselamatan fizikal hendaklah di kenalpasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;
- Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan;
- Memperkukuhkan dinding dan siling;
- Memasang alat penggera atau kamera;
- Menghadkan jalan keluar masuk;
- Mengadakan kaunter kawalan;
- Mewujudkan perkhidmatan kawalan keselamatan.

### 9.1.2 Keselamatan Masuk Fizikal

- Setiap pengguna perlu mengimbas kad akses apabila masuk premis pejabat PKNM dan di minta mendaftar di Kaunter Pertanyaan..
- Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT PKNM.

### 9.1.3 Kawasan Larangan

Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di PKNM adalah bilik Ketua Pegawai Eksekutif, Bilik Timbalan Pengerusi, Bilik Komunikasi (Server), Bilik Fail dan Bilik Kebal, Bahagian Kewangan, Unit Ukur Bahan, Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja;

Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai;

## 9.2 Keselamatan Peralatan

Melindungi peralatan dan maklumat;

### 9.2.1 Perkakasan

Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu:

- Setiap **pengguna** hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna;
- Semua perkakasan hendaklah disimpan atau diletakkan ditempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan;
- Setiap **pengguna** adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan
- Sebarang bentuk penyelewengan atau salahguna perkakasan hendaklah dilaporkan.

### 9.2.2 Kabel

**Unit Teknologi Maklumat PKNM** perlu memastikan;

Kabel komputer hendaklah dilindungi kerana punca maklumat boleh menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:

- Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
- Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; dan
- Melindungi laluan pemasangan kabel sepenuhnya.

### 9.2.3 Penyelenggaraan

Perkakasan hendaklah diselanggarakan dengan betul bagi memastikan kebolehsediaan dan integriti.

- Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan;
- perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja;
- Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; dan
- Semua penyelenggaraan mestilah mendapat kebenaran daripada Ketua Bahagian berkenaan.

### 9.2.4 Peminjaman Perkakasan untuk kegunaan di luar pejabat

Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan:

- Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; dan
- Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.

### 9.2.5 Peralatan di Luar Premis

Bagi perkakasan yang dibawa keluar dari premis PKNM, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud diluar kawalan PKNM:

- Peralatan perlu dilindungi dan dikawal sepanjang masa; dan
- Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.

### 9.2.6 Pelupusan

Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan PKNM;

- Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding*, *grinding*, *degauzing* atau pembakaran;
- Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; dan
- Maklumat lanjut pelupusan bolehlah merujuk kepada surat pekeliling perbendaharaan bilangan 1 tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan".
- Tindakan yang diambil perlu mengambil kira Arahan Keselamatan, Garis Panduan Pengurusan Rekod Elektronik dan Akta Arkib Negara 2003.

### *9.2.7 Clear Desk* dan *Clear Screen*

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. ***Clear desk*** bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja atau dipaparan skrin apabila pengguna tidak berada ditempatnya:

- Gunakan kemudahan ***password screen saver*** atau log keluar apabila meninggalkan komputer;
- Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci;
- Tidak menulis password komputer di kertas atau mana-mana medium yang boleh dicapai oleh mana-mana individu; dan
- Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.

## 9.3 Keselamatan Persekitaran

Melindungi aset ICT PKNM dari sebarang bentuk ancaman persekitaran disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

### 9.3.1 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk perolehan, penyewaan, pengubahsuaian, pembelian hendaklah dirujuk terlebih dahulu kepada Bahagian Pembangunan dan Pelaburan PKNM. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil:

- Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;
- 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;
- Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
- Bahan mudah terbakar hendaklah disimpan diluar kawasan kemudahan penyimpanan aset ICT;
- Semua bahan cecair hendaklah diletakkan ditempat yang bersesuaian dan berjauhan dari aset ICT;
- Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan
- Semua peralatan perlindungan hendaklah **disemak dan diuji sekurang- kurangnya dua (2) kali dalam setahun.** Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.

### 9.3.2 Bekalan Kuasa

**Unit Teknologi Maklumat, PKNM** bertanggungjawab dan memastikan;

- Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;
- Peralatan sokongan seperti UPS (Uninteruptable Power Supply) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan
- Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.

### 9.3.3 Prosedur Kecemasan

Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik.

## 9.4 Keselamatan Dokumen dan Maklumat

Objektif**:** Bagi memastikan integriti terhadap maklumat dan melindungi maklumat PKNM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.

- memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin;
- menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen;
- menggunakan penyulitan (encryption) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik. Penyulitan (encryption) bermaksud proses untuk mengubah data ke dalam bentuk yang tidak dapat dibaca tanpa melakukan proses deskripsi (decrypting), iaitu mengubah kembali ke bentuk aslinya terlebih dahulu; dan
- pada dasarnya, enkripsi (encryption) adalah proses untuk mengubah pesanan atau data ke dalam bentuk yang tidak dapat dibaca tanpa melakukan proses dekripsi (decrypting), iaitu mengubah kembali ke bentuk aslinya terlebih dahulu.

- memastikan dokumen yang mengandungi bahan atau maklumat sulit diambil segera dari pencetak

## 10. Pengurusan Operasi dan Komunikasi

### 10.1 Pengurusan Operasi

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

#### 10.1.1 Pengendalian Prosedur

- Semua prosedur keselamatan ICT yang diwujudkan, dikenalpasti dan masih digunapakai hendaklah didokumenkan, disimpan dan dikawal;
- 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
- Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.

#### 10.1.2 Kawalan Perubahan

- Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada Pegawai atasan atau pemilik aset ICT terlebih dahulu;
- Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;
- Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
- Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

### 10.1.3 Prosedur Pengurusan Insiden

Unit Teknologi Maklumat bersama Pasukan ***Computer Emergency renponse Team*** **(CERT)** Negeri Melaka bertanggungjawab bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan; prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut;

- Mengenalpasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran;
- Menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;
- Menyimpan jejak audit dan memelihara bahan bukti; dan
- Menyediakan tindakan pemulihan segera.

## 10.2 Perancangan dan Penerimaan Sistem

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

### 10.2.1 Perancangan Kapasiti

- Unit Teknologi Maklumat, PKNM perlu memastikan 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
- 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.

### 10.2.2 Penerimaan Sistem

Unit Teknologi Maklumat, PKNM perlu memastikan semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.

## 10.3 Perisian Berbahaya

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

### 10.3.1 Perlindungan dari perisian berbahaya

- Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, Intrusion Prevention System dan mengikut prosedur penggunaan yang betul dan selamat;
- Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997;
- Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya;
- Mengemaskini antivirus setiap minggu;
- Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;
- Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;
- Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan
- Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

## 10.4 Housekeeping

Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.

### 10.4.1 Penduaan

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 disimpan di *off site*.

- Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;
- Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; dan
- Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.

### 10.4.2 Sistem Log

- Mewujudkan sistem log bagi merekodkan semua aktiviti harian penggunaan;
- Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaikpulih dengan segera; dan
- Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada Pasukan *Komputer Emergency Response Team* (CERT) Negeri Melaka.

## 10.5 Pengurusan Rangkaian

Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

### 10.5.1 Kawalan Infrastruktur Rangkaian

Memastikan Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan:-

- Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;
- Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;
- Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;
- ***Firewall*** hendaklah dipasang di antara rangkaian dalaman dan sistem yang melebarkan maklumat rahsia rasmi kerajaan serta dikonfigurasi oleh

pentadbir sistem;

- Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan PKNM;
- Memasang ***Web Content Filter*** pada internet *gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan";
- Sebarang penyambungan rangkaian yang bukan di bawah kawalan PKNM hendaklah mendapat kebenaran Unit Teknologi Maklumat;
- Semua pengguna hanya dibenarkan menggunakan rangkaian PKNM sahaja. Penggunaan modem dan modem tanpa wayar jalur lebar mestilah mendapat kebenaran Unit Teknologi Maklumat, PKNM dan
- Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.

## 10.6 Pengurusan Media

Objektif: Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.

### 10.6.1 Penghantaran dan Pemindahan

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.

### 10.6.2 Prosedur Pengendalian media

- Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;
- Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja;
- Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan;
- Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;
- Menyimpan semua media di tempat yang selamat; dan
- Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus

atau dimusnahkan mengikut prosedur yang betul dan selamat.

### 10.7 Keselamatan komunikasi

Melindungi aset ICT melalui sistem komunikasi yang selamat.

#### 10.7.1 Internet

- Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan;
- Bahan yang diperoleh dari internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber internet hendaklah dinyatakan;
- Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke internet;
- Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;
- Sebarang bahan yang dimuat turun dari internet hendaklah digunakan untuk tujuan yang dibenarkan oleh PKNM.
- Maklumat lanjut mengenai keselamatan internet bolehlah merujuk kepada pekeliling kemajuan pentadbiran awam bilangan 1 tahun 2003 bertajuk “ Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di agensi-agensi kerajaan”.

## 11. Kawalan Capaian

Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT PKNM.

### 11.1 Keperluan Dasar

**Unit Teknologi Maklumat, PKNM** perlu memastikan capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada.

## 11.2 Pengurusan Capaian Pengguna

Mengawal capaian pengguna ke atas aset ICT PKNM.

### 11.2.1 Akaun Pengguna

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

- Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan.
- Akaun pengguna mestilah unik.
- Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;
- Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan Jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;
- Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan
- Unit Terknologi Maklumat, PKNM boleh **membeku dan menamatkan** akaun pengguna atas sebab-sebab berikut;

  - Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) minggu
  - Bertukar bidang tugas kerja
  - Bertukar ke agensi lain
  - Bersara; atau
  - Ditamatkan perkhidmatan

### 11.2.2 Jejak Audit

**Unit Teknologi Maklumat, PKNM** perlu memastikan jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau

penyalahgunaan sistem. Aktiviti jejak audit mengandungi;

- Maklumat identiti pengguna, sumber yang digunakan perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan;
- Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan
- Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

Unit Teknologi Maklumat hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.

### 11.3 Kawalan Capaian Sistem dan Aplikasi

Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.

### 11.4 Sistem Maklumat dan Aplikasi

Unit Teknologi Maklumat, PKNM perlu memastikan capaian sistem dan aplikasi di PKNM adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi:

- Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti;
- Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini;
- Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan;
- Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;

- Kata laluan perlu sentiasa dikemaskini atau ditukar oleh pengguna bagi meningkatkan tahap keselamatan;
- Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan
- Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walaubagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.

### 11.5 Peralatan Komputer Mudah Alih

Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.

#### 11.5.1 Penggunaan Peralatan Komputer Mudah Alih

- Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; dan
- Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.

## 12. Pembangunan dan Penyelenggaraan Sistem

### 12.1 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

#### 12.1.1 Keperluan Keselamatan

- **Unit Teknologi Maklumat, PKNM** perlu memastikan pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;
- 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
- Sebaik-baiknya, 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.

## 12.2 Kriptografi

Melindungi kerahsiaan, integriti dan kesahihan maklumat

### 12.2.1 Penyulitan

- **Pengguna** hendaklah membuat penyulitan ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.
- Penyulitan perlulah menggunakan teknologi algoritma yang standard dan terbukti keberkesanannya seperti DES, Blowfish, RSA, RC5 dan IDEA.
- Kunci penyulitan simetrik perlulah melebihi 56 bits. Sistem penyulitan Asimetrik mestilah menggunakan kunci yang melebihi atau sama.
- Penggunaan algoritma penyulitan yang tersendiri dan tertutup (proprietary) adalah dilarang sama sekali. Walaubagaimanapun ianya boleh diberi pertimbangan jika mendapat kelulusan dari Cyber Security Malaysia.

### 12.2.2 Tandatangan Digital

Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.

### 12.2.3 Pengurusan Kunci

Pengurusan kunci hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

## 12.3 Fail Sistem

Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.

### 12.3.1 Kawalan Fail Sistem

- Proses pengemaskini fail sistem hanya boleh dilakukan oleh Unit

Teknologi Maklumat, PKNM atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;

- Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji;
- Mengawal capaian ke atas kod atau aturcara program bagi mengelak kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan
- Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.

### 12.4 Pembangunan dan Proses Sokongan

Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

#### 12.4.1 Kawalan Perubahan

Audit Teknologi Maklumat, PKNM perlu memastikan perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.

## 13. Pengurusan Kesinambungan Perkhidmatan

### 13.1 Dasar Kesinambungan Perkhidmatan

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

#### 13.1.1 Kesinambungan Perkhidmatan

Pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi.

## 14. Pematuhan

### 14.1 Pematuhan dan Keperluan Perundangan

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar ICT PKNM.

#### 14.1.1 Pematuhan Dasar

- Setiap pengguna di PKNM hendaklah membaca, memahami dan

mematuhi Dasar Keselamatan ICT PKNM dan undang-undang atau peraturan-peraturan lain yang berkaitan dan berkuat kuasa.

- Semua aset ICT di PKNM termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna dan mengesan penggunaan selain dari tujuan yang telah ditetapkan.

### 14.1.2 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

- Unit Teknologi Maklumat, PKNM perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.
- Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi standard pelaksanaan keselamatan.

### 14.1.3 Pematuhan Keperluan Audit

- Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat.
- Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.
- Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.

### 14.1.4 Keperluan Perundangan

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di PKNM:

- Akta Aktiviti Kerajaan Elektronik 2007;
- Akta Rahsia Rasmi 1972;
- Akta Tandatangan Digital 1997;
- Akta Jenayah Komputer 1997;
- Akta Hak cipta (Pindaan) Tahun 1997;
- Akta Komunikasi dan Multimedia 1998;
- Akta Arkib Negara 2003.
- Arahan Teknologi Maklumat 2007;
- Arahan Keselamatan;

- Arahan Perbendaharaan.
- Tatacara Pengurusan Aset Alih Kerajaan 2007.
- Garis Panduan Pengurusan Rekod Elektronik: Pengurusan Rekod Elektronik Dalam Persekitaran Berstruktur
- Perintah-Perintah Am;
- "Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)";
- Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";
- Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)";
- Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan";
- Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam";
- Surat Pekeliling Am Bilangan 4 Tahun 2006 bertajuk "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi
- (ICT) Sektor Awam";
- Surat Pekeliling Perbendaharaan Bilangan 8 Tahun 2006 bertajuk "Peraturan Perolehan Perkhidmatan Perunding";
- Pekeliling Am Bilangan 1 Tahun 2006 bertajuk "Pengurusan laman Web/Portal Sektor Awam";
- Surat Arahan MAMPU bertajuk "Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi- Agensi Kerajaan" bertarikh 1 Jun 2007;
- Surat Arahan MAMPU bertajuk "Langkah-langkah Pemantapan Pelaksanaan Mel Elektronik di Agensi- Agensi Kerajaan" bertarikh 23 November 2007;
- 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;
- Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan

Penilaian Risiko Keselamatan Maklumat Sektor Awam;

## 14.2 Pelanggaran Dasar

Objektif: Meningkatkan kesedaran dan pematuhan ke atas DKICT PKNM.

### 14.2.1 Tindakan Tatatertib

Pelanggaran DKICT PKNM dan semua perbuatan kecuaian, kelalaian dan pelanggaran keselamatan boleh dikenakan tindakan tatatertib.