

POLISI PENGURUSAN ASET DAN MEDIA

1.0 TUJUAN POLISI

Mengenal pasti aset ICT bagi memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT.

2.0 SKOP POLISI

- i. Polisi pengurusan aset dan media meliputi tatacara berikut :
 - a. Pengurusan Aset ICT
 - b. Pengelasan Maklumat
 - c. Pengurusan Media Mudah Alih

3.0 PENGURUSAN ASET ICT

3.1 Tanggungjawab pemilik aset ICT adalah seperti berikut;

- a) Memastikan aset telah didaftarkan dan dilabel dengan label "Hakmilik Kerajaan";
- b) Mengesahkan penempatan aset ICT di bawah kawalannya melalui Borang Kew PA-7 (Senarai Aset Di Lokasi);
- c) Menyemak dan memastikan semua aset ICT di bawah kawalannya berfungsi dengan sempurna;
- d) Bertanggung jawab sepenuhnya ke atas aset ICT di bawah kawalannya dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan tanpa kebenaran pihak pengurusan atau Unit IT;
- e) Bertanggungjawab ke atas kerosakan atau kehilangan aset ICT di bawah kawalannya;
- f) Melindungi aset ICT daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;
- g) Pemilik aset bertanggungjawab untuk membenarkan perisian keselamatan seperti perisian antivirus atau *windows security* dikemaskini secara berkala untuk melindungi peralatan ICT dari ancaman *virus, worm* dan seumpamanya;
- h) Melaporkan sebarang kerosakan aset ICT kepada Pegawai Aset atau Unit ICT untuk dibaik pulih dengan melengkapkan **Borang Aduan Kerosakan Aset Alih ICT** seperti di **Lampiran A**;
- i) Memastikan semua aset ICT dalam keadaan 'OFF' apabila meninggalkan pejabat;
- j) Memastikan semua peranti storan yang disambung kepada komputer atau komputer riba jabatan dibuat imbasan (*scan*) terlebih dahulu sebelum fail atau folder di dalam media berkaitan dibuka bagi mengelak ancaman *virus, worm* dan seumpamanya;
- k) Melaporkan salah guna aset ICT kepada Pegawai Aset atau atau Ketua Jabatan;
- l) Memastikan peminjaman dan bawa keluar aset dari premis jabatan telah mendapat kebenaran dengan melengkapkan **Borang Permohonan Pergerakan/ Pinjaman Aset Alih** seperti **Lampiran B**.

- m) Memastikan aset yang dipinjam diserahkan semula kepada jabatan dengan menandatangani kembali Borang Permohonan Pergerakan/ Pinjaman Aset Alih di ruang Pengesahan Pemulang.
- n) Peminjam bertanggungjawab untuk memastikan aset dan aksesori yang dipulangkan adalah dalam keadaan baik, berfungsi dan sama seperti yang dipinjam. Peralatan termasuk aksesori perlu sama kuantiti dan kualiti yang dipinjam. Data/ fail di dalam aset yang dipinjam adalah tanggungjawab peminjam dan hendaklah dipadam sebelum pemulangan. Data/ fail sulit (*confidential*) mestilah dihapuskan untuk mengelakkan dari disalahguna oleh pihak yang tidak bertanggungjawab; dan
- o) Peminjam adalah bertanggungjawab sepenuhnya terhadap keselamatan perkakasan ICT tersebut. Sekiranya berlaku kehilangan dalam tempoh peminjaman, peminjam perlu melaporkan kepada Ketua Jabatan dan membuat laporan polis dalam tempoh 24 jam. Pengurusan kehilangan aset ICT perlu merujuk kepada tatacara kehilangan aset alih yang berkuatkuasa.

3.2 Semua aset ICT yang dibekalkan hendaklah:

- a) Dipulangkan kepada jabatan apabila pengguna meninggalkan jawatan yang disandang atau meninggalkan jabatan (bertukar, bersara atau tamat perkhidmatan);
- b) Sebarang pindah milik aset kepada pihak ketiga/ fasiliti KKM yang lain di bawah JKNP perlu mendapat kelulusan sebelum pindah milik dibuat; dan
- c) Maklumat yang disimpan dalam aset ICT yang akan dipindah milik kepada pihak ketiga/ fasiliti KKM yang lain di bawah JKNP perlu disalin dan dihapuskan sebelum dipindah milik.

4.0 PENGELASAN MAKLUMAT

4.1 Pengelasan Maklumat

- a) Semua maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh Pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan seperti berikut :
 - i. Rahsia Besar;
 - ii. Rahsia
 - iii. Sulit; atau
 - iv. Terhad

4.2 Pengendalian Aset dan Maklumat

- a) Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut :
 - i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
 - ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
 - iii. Menentukan maklumat sedia untuk digunakan;
 - iv. Menjaga kerahsiaan kata laluan;
 - v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang berkuatkuasa;
 - 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.
 - viii. Memastikan keselamatan maklumat dan data terpelihara di pelayan dan storan dengan memastikan komputer pengguna tidak mempunyai maklumat sulit;
 - ix. Maklumat persendirian yang disimpan di dalam komputer adalah di bawah tanggungjawab pengguna sendiri; dan
 - x. Pengguna digalakkan menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer.

5.0 PENGURUSAN MEDIA MUDAH ALIH

5.1 Takrifan Media Mudah Alih

Media mudah alih adalah peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat dan media storan yang boleh alih (*pen drive/ external hard disk*).

5.2 Pengurusan Media Mudah Alih

- a) Peraturan yang perlu dipatuhi dalam pengurusan media mudah alih adalah berdasarkan Arahan Keselamatan seperti berikut:
 - i. Semua media mudah alih perlu disimpan di ruang penyimpanan yang baik/ selamat;
 - ii. Akses untuk memasuki kawasan penyimpanan media mudah alih hendaklah dihadkan;
 - iii. Media mudah alih perlu dikawal dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;
 - iv. Melabel semua media mengikut tahap sensitiviti maklumat;

- v. Media mudah alih yang mengandungi data terperingkat hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan berikut;
 - Akses dan pergerakan media mudah alih yang mengandungi data terperingkat perlu direkodkan;
 - Peralatan *backup* bagi media mudah alih diletakkan di tempat yang terkawal;
 - Mewujudkan salinan atau pendua media mudah alih bagi tujuan keselamatan;
 - Maklumat rasmi sahaja boleh disimpan dalam media mudah alih yang dibekalkan oleh kerajaan;
 - Menghadkan pengedaran media untuk tujuan yang dibenarkan sahaja; dan
 - Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan.

5.3 Pelupusan Media

- a) Pelupusan media perlu mendapat kelulusan dari Jawatankuasa Pengurusan Aset Kerajaan (JPAK) dan mengikut tatacara pengurusan aset yang berkuatkuasa.
- b) Peraturan yang perlu dipatuhi seperti berikut:
 - i. Media yang mengandungi maklumat terperingkat mestilah dilupuskan mengikut prosedur yang betul serta selamat;
 - ii. Memastikan data terperingkat/ sensitif dihapuskan (*wipe data*) dengan teratur dan selamat dengan merujuk garis panduan yang berkuatkuasa;
 - iii. Tatacara pelupusan media dilaksanakan mengikut Pekeliling Pengurusan Aset Alih Kerajaan yang berkuat kuasa;
 - iv. Sebarang pelupusan data dalam media telah mendapat kelulusan pemilik maklumat terlebih dahulu.

5.4 Penghantaran dan Pemindahan

- a) Media yang mengandungi maklumat rasmi hendaklah dilindungi dari capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pengangkutan/ penghantaran.
- b) Penghantaran dan pemindahan media mudah alih perlu merujuk kepada Arahan Keselamatan berikut:
 - i. Mendapat kebenaran pemilik bagi penghantaran atau pemindahan media ke luar;
 - ii. Mempunyai rekod penghantaran dan pemindahan media ke luar;
 - iii. Maklumat terperingkat dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan. Pemindahan media yang mengandungi maklumat terperingkat perlu dilindungi dengan kata laluan dan penyulitan. Maklumat kata laluan berkaitan perlu dihantar kepada penerima melalui emel atau medium lain yang selamat. Sekiranya maklumat sulit pada media tidak dapat dibuat penyulitan, perlindungan fizikal tambahan pada media wajar dipertimbangkan;

iv. Sebarang penyalahgunaan atau pendedahan maklumat ketika pengurusan media perlu dilapor segera kepada Ketua Jabatan.

5.5 Media Mudah Alih Persendirian (*Bring Your Own Device*)

Pengguna BYOD perlu mematuhi tatacara penggunaan BYOD seperti berikut:

- a) Maklumat rasmi kerajaan adalah hak milik kerajaan;
- b) Bahan rasmi yang dimuatnaik, diedar dan dikongsi perlu mendapat kebenaran Ketua Jabatan;
- c) Menandatangani Surat Akuan Pematuhan DKICT & Akta Rahsia Rasmi 1972 [Akta 88];
- d) Peranti yang digunakan mempunyai kawalan keselamatan seperti perisian anti virus atau melaksanakan penyulitan ke atas *file/ folder* yang mengandungi maklumat sulit dan terperingkat.
- e) Pengguna **DILARANG** :
 - i. Menyimpan maklumat rasmi ke dalam peranti BYOD tanpa kebenaran Ketua Jabatan;
 - ii. Mengakses maklumat rasmi dan terperingkat menggunakan peranti BYOD;
 - iii. Membuat *backup* maklumat rasmi ke dalam peranti BYOD;
 - iv. Merakam maklumat rasmi bagi tujuan peribadi;
 - v. Menjadikan BYOD sebagai *access point* kepada aset ICT jabatan untuk capaian ke internet tanpa kebenaran Pentadbir ICT atau ICTSO.

6.0 PENGUATKUASAAN

Polisi ini hendaklah dipatuhi dalam memastikan kelancaran pelaksanaan perkhidmatan ICT di Jabatan Kesihatan Negeri, Negeri Sembilan.

7.0 RUJUKAN

- i. Dasar Keselamatan ICT Kementerian Kesihatan Malaysia (KKM);
- ii. Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam;
- iii. Garis Panduan Dasar Pengurusan Rekod dan Arkib Elektronik (Garis Panduan Pengurusan Rekod Elektronik)



BORANG ADUAN KEROSAKAN
JABATAN KESIHATAN NEGERI SEMBILAN

1. MAKLUMAT PENGADU

NAMA	
UNIT / BAHAGIAN	
NO. TEL	
TARIKH ADUAN	

2. KATEGORI

BIL	PERKARA KEROSAKAN	LOKASI KEROSAKAN

3. TINDAKAN PENTADBIRAN

TARIKH SIASATAN	PENENTUAN KEROSAKAN (MUDAH/SEDERHANA/KOMPLEKS)	TINDAKAN PENTADBIRAN (TARIKH)	PENGESAHAN PENGADU (NAMA / T/T)

4. ULASAN PENTADBIRAN :

TANDATANGAN :

NAMA :

JAWATAN :

TARIKH :

* PEGAWAI BERTANGGUNG JAWAB : SHAMSUDIN BIN MOHD YUSOFF (EXT : 5729 / 0183883610)
MOHD NORFADLEEV BIN HAMZAH (EXT:5715 / 0172777267)

LAMPIRAN B

Pekeliling Perbendaharaan Malaysia

AM 2.4 Lampiran A

KEW.PA-9

No. Permohonan :

BORANG PERMOHONAN PERGERAKAN/ PINJAMAN ASET ALIH

Nama Pemohon :		Tujuan :	
Jawatan :		Tempat Digunakan:	
Bahagian :		Nama Pengeluar:	

Bil.	No. Siri Pendaftaran	Keterangan Aset	Tarikh		(Lulus/ Tidak Lulus)	Tarikh		Catatan
			Dipinjam	Dijangka Pulang		Dipulangkan	Diterima	
..... (Tandatangan Peminjam) Nama : Jawatan : Tarikh :				 (Tandatangan Pelulus) Nama : Jawatan : Tarikh :			
..... (Tandatangan Pemulang) Nama : Jawatan : Tarikh :				 (Tandatangan Penerima) Nama : Jawatan : Tarikh :			