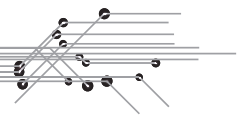




# **DASAR KESELAMATAN**

## **TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (DKICT)**

**Jabatan Pengairan dan Saliran Malaysia**  
**VERSI 2.0**



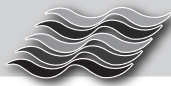
Diterbitkan oleh:

Bahagian Pengurusan Maklumat  
Jabatan Pengairan dan Saliran Malaysia  
Jalan Sultan Salahuddin  
50626 Kuala Lumpur

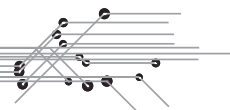
Telefon : 03 - 2616 1400 / 1500 (*General Line*)  
Faks : 03 - 2697 2600  
Laman Web : <http://www.water.gov.my>  
Versi : 2.0  
Tahun Terbitan : Mac 2013

© Hak cipta terpelihara:

Tiada mana-mana bahagian daripada Dasar ini boleh diterbitkan semula atau diproses, disalin, diedarkan melalui capaian sistem di dalam sebarang bentuk (cetakan, fotokopi atau seumpamanya) tanpa mendapat kebenaran bertulis dari Jabatan Pengairan dan Saliran Malaysia (JPS).



*When you know that you're capable of dealing with whatever comes,  
you have the only security the world has to offer. — Harry Browne*

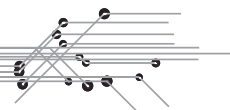


## MAKLUMAT

Tajuk	: Dasar Keselamatan Teknologi Maklumat dan Komunikasi (DKICT)
Versi	: 2.0
Tarikh Kuat Kuasa	: 15 Mac 2013
Pemilik	: Bahagian Pengurusan Maklumat, Jabatan Pengairan dan Saliran Malaysia
Nombor Rujukan	: ( 28 ) PPS.IT 29 Jld.2

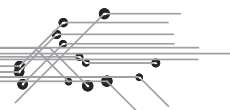
## SEJARAH SEMAKAN DAN PINDAAN

Versi	Tarikh	Ringkasan Semakan / Pindaan	Kelulusan	Tarikh Kuat Kuasa
1.0	25 Oktober 2010	Terbitan Pertama	(50) KP.JPS.2009 Kelulusan Ketua Pengarah JPS Malaysia	26 Oktober 2010
1.0	11 Oktober 2010	Kajian semula Perkara 10: Kawalan Capaian	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) JPS Bil.4 Tahun 2011	11 Oktober 2011
2.0	23 September 2012	Terbitan DKICT 2.0 Kajian semula keseluruhan DKICT JPS Malaysia	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) JPS Bil.3 Tahun 2012	15 Mac 2013



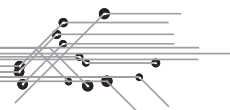
## KANDUNGAN

PERUTUSAN	iv
1. DASAR KESELAMATAN	1
1.1 Pendahuluan	1
1.2 Tujuan	1
1.3 Skop	1
1.4 Prinsip	2
1.5 Pemakaian	5
1.6 Semakan dan Pindaan	5
2. PENGURUSAN KESELAMATAN ICT	6
2.1 Tanggungjawab Pengurusan Keselamatan ICT JPS	6
2.2 Struktur Pengurusan Keselamatan ICT	6
2.3 Jawatankuasa Keselamatan ICT	7
2.4 Juruaudit	9
2.5 Penasihat Undang-undang	9
2.6 Pengurus Sumber Manusia	10
2.7 Pengguna Luaran/Asing	10
3. PENGURUSAN ASET	12
3.1 Pengurusan Aset	12
3.2 Tanggungjawab Pengurusan Aset	12
3.3 Pengelasan, Pelabelan dan Pengendalian Maklumat	13
3.4 Akauntabiliti Terhadap Aset ICT	14
4. PENGURUSAN SUMBER MANUSIA	15
4.1 Sebelum Berkhidmat	15
4.2 Dalam Perkhidmatan	15
4.3 Latihan	16
4.4 Bertukar atau Tamat Perkhidmatan	16
5. KESELAMATAN FIZIKAL DAN PERSEKITARAN	17
5.1 Tanggungjawab Keselamatan Fizikal dan Persekitaran	17
5.2 Kawalan Kawasan Terperingkat	17
5.3 Keselamatan Peralatan	18



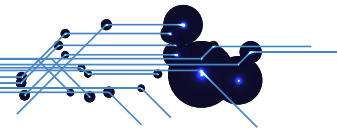
## KANDUNGAN

5.4	Prasarana Sokongan	19
5.5	Penyelenggaraan Peralatan	22
5.6	Peminjaman Peralatan	22
5.7	Pengendalian Peralatan Luar yang Dibawa Masuk / Keluar	23
5.8	Pelupusan Peralatan	23
5.9	Clear Desk dan Clear Screen	23
5.10	Melaporkan Kehilangan atau Kecurian Pas Keselamatan, Kad Pengenalan Jabatan, Kad Kuasa dan Kad Pelantikan	24
6.	PENGURUSAN OPERASI DAN KOMUNIKASI	25
6.1	Pengendalian Prosedur	25
6.2	Pengurusan Penyampaian Perkhidmatan	25
6.3	Perancangan dan Penerimaan Sistem	26
6.4	Pengurusan dan Kawalan Perubahan	26
6.5	Perlindungan Dari <i>Malicious</i> dan <i>Mobile Code</i>	27
6.6	<i>Backup</i> dan <i>Restore</i>	28
6.7	Pengurusan Keselamatan Rangkaian	29
6.8	Pengendalian Peralatan Penyimpanan Maklumat	29
6.9	Pertukaran Maklumat	30
6.10	Perkhidmatan e-Dagang ( <i>e-Commerce</i> )	30
6.11	Pemantauan	31
6.12	Pengasingan Bidang Tugas	31
6.13	Pengasingan Infrastruktur Operasi dan Pembangunan	32
6.14	Pelarasan Masa untuk Semua Sistem Di Dalam Pusat Data	32
7.	KAWALAN CAPAIAN	33
7.1	Keperluan Kawalan Capaian	33
7.2	Kawalan Capaian Pengguna	33
7.3	Pengurusan Kata Laluan	34
7.4	Kawalan Capaian Rangkaian	37
7.5	Kawalan Capaian Sistem Pengoperasian	38
7.6	Kawalan Capaian Aplikasi dan Maklumat	38
7.7	Peralatan Mudah Alih dan Kerja Jarak Jauh	39
7.8	Penggunaan Capaian Tanpa Wayar	40
7.9	Tanggungjawab Pengguna	40



## KANDUNGAN

8.	PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT	41
8.1	Keperluan Keselamatan Sistem Maklumat	41
8.2	Kawalan Kriptografi ( <i>Cryptography</i> )	41
8.3	Kawalan Fail Sistem	42
8.4	Keselamatan Dalam Proses Pembangunan dan Sokongan	42
8.5	Kawalan Teknikal Keterdedahan ( <i>Vulnerability</i> )	43
9.	PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN	44
9.1	Pengurusan Pengendalian Insiden Keselamatan	44
9.2	Insiden Keselamatan	44
9.3	Melaporkan Insiden	45
9.4	Menentukan Keutamaan Tindakan Ke Atas Insiden	45
9.5	Pengendalian Insiden	46
10.	PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	48
10.1	Kesinambungan Perkhidmatan	48
10.2	Pelan Kesinambungan Perkhidmatan	48
10.3	Perubahan atau Pengecualian <i>Business Continuity Plan</i> (BCP)	48
10.4	Program Latihan dan Kesedaran Terhadap BCP	49
10.5	Pengujian BCP	49
11.	PEMATUHAN	50
11.1	Pematuhan Dasar	50
11.2	Keperluan Perundangan	50
11.3	Perlindungan dan Privasi Data Peribadi	50
11.4	Semakan Keselamatan Maklumat	51
11.5	Pelanggaran Perundangan	51
11.6	Surat Akuan Pematuhan Dasar Keselamatan ICT	51
	PENGHARGAAN	52
	LAMPIRAN A	53
	LAMPIRAN B	54



## PERUTUSAN

### KETUA PENGARAH JABATAN PENGAIRAN DAN SALIRAN MALAYSIA



Assalamualaikum warahmatullahi wabarakatuh dan salam sejahtera,

Aset dan kemudahan ICT JPS semakin bertambah sejajar dengan peningkatan penggunaan ICT dikalangan warga JPS. Bagi memastikan kemudahan dan aset ICT digunakan dengan optimum, cekap dan selamat, DKICT JPS telah dikaji semula.

Dasar ini meliputi semua sumber dan kemudahan ICT JPS dan adalah terpakai bagi semua pengguna ICT di JPS termasuk pembekal perkakasan dan perisian ICT dan pihak-pihak lain yang menggunakan kemudahan ICT JPS. DKICT JPS akan dikemaskini daripada masa ke semasa selaras dengan perkembangan terkini.

Harapan saya, semoga semua warga JPS akan mematuhi peraturan-peraturan yang telah digariskan dalam DKICT JPS 2.0. Adalah menjadi tanggungjawab kita untuk bersama-sama menjaga dan melindungi aset ICT JPS bagi memastikan penyampaian perkhidmatan kita kepada pelanggan sentiasa cekap, berkualiti dan efektif.

Akhir kata, saya mengambil kesempatan ini untuk mengucapkan tahniah kepada Bahagian Pengurusan Maklumat (BPM) di atas kejayaan menghasilkan terbitan kajian semula Dasar Keselamatan Teknologi Maklumat dan Komunikasi (DKICT) untuk dijadikan rujukan khasnya oleh warga Jabatan ini.

Sekian, terima kasih. Wassalamualaikum warahmatullahi wabarakatuh.

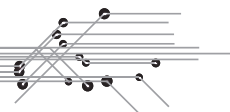
*"Keselamatan ICT Tanggungjawab Bersama"*

**DATUK IR HJ AHMAD HUSAINI BIN SULAIMAN**

Ketua Pengarah

Jabatan Pengairan dan Saliran Malaysia





## 1. DASAR KESELAMATAN

Dasar Keselamatan Teknologi Maklumat dan Komunikasi (DKICT) Jabatan Pengairan dan Saliran Malaysia JPS adalah hak milik Jabatan ini yang bertujuan memastikan hala tuju pengurusan perlindungan aset teknologi maklumat dan komunikasi (*Information and Communication Technology* - (ICT)) selaras dengan peruntukan undang-undang. Pelaksanaan dasar perlindungan ke atas kerahsiaan, integriti dan kebolehsediaan data/maklumat adalah untuk menjamin kesinambungan urusan serta perkhidmatan dengan meminimumkan kesan insiden keselamatan.

### 1.1 Pendahuluan

Jabatan Pengairan dan Saliran (JPS) bertanggungjawab memastikan keselamatan aset ICT termasuk data/maklumat, perkakasan, perisian dan rangkaian yang dimiliki atau yang dikawal selia adalah bebas daripada ancaman dan risiko yang tidak boleh diterima.

### 1.2 Tujuan

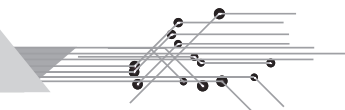
Dasar Keselamatan ICT JPS bertujuan menjamin kesinambungan operasi berasaskan prinsip kerahsiaan, integriti dan kebolehsediaan seperti berikut:

- (a) Kerahsiaan bermaksud melindungi kepentingan semua pihak berkaitan keselamatan aset ICT;
- (b) Integriti bermaksud memastikan sebarang perubahan ke atas aset ICT dilakukan oleh pihak yang dibenarkan sahaja; dan
- (c) Kebolehsediaan bermaksud aset ICT hendaklah boleh diguna bila diperlukan melalui kelancaran operasi JPS dan meminimumkan gangguan, kerosakan atau kemusnahan ke atas aset ICT.

### 1.3 Skop

Semua pihak yang menggunakan aset ICT JPS adalah bertanggungjawab ke atas perkara berikut:

- (a) Data/maklumat hendaklah boleh dicapai secara berterusan dengan cepat, tepat, mudah dan dengan cara yang diyakini selamat bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan



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

Demi memastikan keselamatan berterusan, adalah penting jaminan perlindungan merangkumi perkara-perkara berikut:

- (a) Data/Maklumat – dokumentasi dan rekod berkaitan organisasi, sistem, prosedur, pelanggan dan lain-lain;
- (b) Perkakasan – aset ICT yang digunakan untuk merekodkan, memproses dan menyimpan data/maklumat;
- (c) Perisian – semua perisian termasuk perisian aplikasi, perisian utiliti, perisian sistem, sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian dan perisian automasi pejabat;
- (d) Rangkaian – perkhidmatan yang menghubungkan capaian data / maklumat;
- (e) Premis – penempatan kemudahan ICT; dan
- (f) Manusia – individu atau kumpulan yang mempunyai pengetahuan dan kemahiran untuk mengendalikan ICT bagi mencapai objektif organisasi.

#### 1.4 Prinsip

Prinsip Dasar Keselamatan ICT JPS adalah seperti berikut:

- (a) Capaian Atas Dasar Perlu Tahu

Capaian dibenarkan dan dihadkan kepada pengguna tertentu atas dasar “perlu tahu” berdasarkan klasifikasi maklumat dan tahap tapisan keselamatan pengguna.

- (b) Hak Capaian Minimum

Hak capaian kepada pengguna dimulai pada tahap yang paling minimum. Kelulusan adalah perlu bagi membolehkan capaian pada tahap yang lebih tinggi.



(c) Akauntabiliti

Setiap pengguna adalah bertanggungjawab ke atas semua tindakan terhadap kemudahan ICT JPS yang disediakan. Tanggungjawab pengguna termasuk perkara berikut:

- (i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- (ii) Memeriksa maklumat dan menentukan ianya sentiasa tepat dan lengkap;
- (iii) Menentukan maklumat sedia untuk digunakan;
- (iv) Menjaga kerahsiaan maklumat; dan
- (v) Mematuhi langkah dan garis panduan keselamatan yang ditetapkan.

(d) Pengasingan

Setiap tugas, proses dan persekitaran pelaksanaan ICT hendaklah dipisahkan dan diasingkan sebaik mungkin untuk mengekalkan integriti dan perlindungan keselamatan daripada kesilapan dan penyalahgunaan. Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:

- (i) Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan;
- (ii) Persekitaran penerimaan iaitu peringkat di mana sesuatu aplikasi diuji; dan
- (iii) Persekitaran sebenar di mana aplikasi sedia untuk beroperasi.

(e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden atau keadaan yang mengancam keselamatan. Pengauditan adalah penting dalam menjamin akauntabiliti seperti berikut:



- (i) Mengesan pematuhan atau pelanggaran keselamatan;
  - (ii) Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya pelanggaran keselamatan; dan
  - (iii) Menyediakan bahan bukti bagi menentukan sama ada berlakunya pelanggaran keselamatan.
- (f) Pematuhan

Prinsip ini penting untuk mengelak pelanggaran Dasar melalui tindakan berikut:

- (i) Mewujudkan proses yang sistematik khususnya dalam menjamin keselamatan ICT untuk memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan;
  - (ii) Merumuskan pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenal pasti;
  - (iii) Melaksanakan program pemantauan keselamatan secara berterusan untuk memastikan standard, prosedur dan garis panduan keselamatan dipatuhi; dan
  - (iv) Menguatkuasakan amalan melaporkan sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.
- (g) Pemulihan

Pemulihan adalah untuk memastikan kebolehsediaan dan kebolehcapaian dengan meminimumkan gangguan atau kerugian akibat daripadanya adalah seperti berikut:

- (i) Merancang dan menguji Pelan Pemulihan Bencana – (*Disaster Recovery Plan*); dan
- (ii) Melaksanakan amalan terbaik dalam pelaksanaan ICT.



(h) Saling Bergantung

Prinsip keselamatan adalah saling lengkap-melengkapi dan hendaklah dipatuhi bagi jaminan keselamatan yang berkesan. Tindakan mempelbagaikan pendekatan dalam menyusun strategi mekanisme keselamatan mampu meningkatkan tahap keselamatan.

## 1.5 Pemakaian

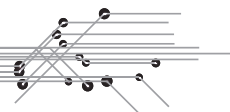
Dasar Keselamatan ICT JPS adalah terpakai kepada semua pengguna aset ICT termasuk pembekal dan pakar runding yang berurusan dengan JPS.

## 1.6 Semakan dan Pindaan

Dasar Keselamatan ICT JPS adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Setiap perubahan hendaklah mendapat pengesahan Pegawai Keselamatan ICT (*ICT Security Officer* (ICTSO)). Perubahan yang melibatkan penambahan atau pemansuhan yang memberi impak ke atas keselamatan adalah dianggap perubahan utama dan hendaklah mendapat pengesahan Jawatankuasa Pemandu ICT (JPIC) JPS.

Prosedur penyelenggaraan Dasar Keselamatan ICT JPS adalah seperti berikut:

- (a) Menyemak dasar ini sekurang-kurangnya sekali setahun bagi mengenal pasti dan menentukan perubahan yang diperlukan;
- (b) Mengemukakan cadangan pindaan atau perubahan secara bertulis; dan
- (c) Memaklumkan pindaan atau perubahan dasar yang telah dipersetujui kepada semua pengguna.



## 2. PENGURUSAN KESELAMATAN ICT

### Objektif:

Memastikan rangka kerja diwujudkan bagi menjamin pelaksanaan pengurusan keselamatan ICT yang sistematik dan berkesan.

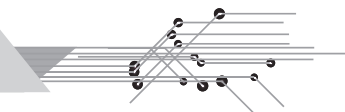
### 2.1 Tanggungjawab Pengurusan Keselamatan ICT JPS

- a) Ketua Pengarah JPS bertanggungjawab untuk:
  - (i) Mewujud dan mengetuai jawatan kuasa keselamatan ICT JPS;
  - (ii) Memastikan semua pengguna memahami dan mematuhi Dasar Keselamatan ICT JPS;
  - (iii) Memastikan keperluan sumber bagi keselamatan ICT JPS adalah mencukupi; dan
  - (iv) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT JPS.

### 2.2 Struktur Pengurusan Keselamatan ICT

Struktur organisasi formal diwujudkan untuk mengurus keselamatan ICT JPS dan mematuhi termasuk yang berikut:

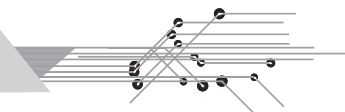
- (a) Komitmen pengurusan atasan ke atas keselamatan ICT dilaksanakan dengan aktif dan telus;
- (b) Tanggungjawab yang jelas dan jalinan perhubungan/komunikasi dengan semua pengguna dalam pengurusan keselamatan ICT;
- (c) Keperluan untuk pengurusan kerahsiaan maklumat dikenal pasti, di laksana dan dikaji secara berkala; dan
- (d) Memastikan kajian semula ke atas keselamatan maklumat dijalankan mengikut peraturan yang ditetapkan.



## 2.3 Jawatankuasa Keselamatan ICT

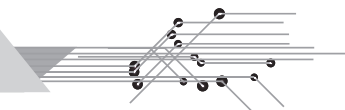
Peranan dan tanggungjawab ahli Jawatankuasa Keselamatan ICT JPS adalah seperti berikut:

- a) Ketua Pegawai Maklumat (*Chief Information Officer (CIO)*):
  - (i) Membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;
  - (ii) Menentukan keperluan dan bertanggungjawab ke atas perkara-perkara berkaitan dengan keselamatan ICT JPS; dan
  - (iii) Membangun dan menyelaraskan pelaksanaan program kesedaran dan latihan keselamatan ICT.
- (b) Pegawai Keselamatan ICT (*ICT Security Officer (ICTSO)*)
  - (i) Merancang, melaksana, mengurus dan memantau program keselamatan ICT JPS;
  - (ii) Menguatkuasakan Dasar Keselamatan ICT JPS;
  - (iii) Memberikan penerangan dan pendedahan berkenaan Dasar Keselamatan ICT JPS kepada pengguna;
  - (iv) Mewujudkan garis panduan dan prosedur selaras dengan keperluan Dasar Keselamatan ICT JPS;
  - (v) Melaksanakan pengurusan risiko keselamatan ICT;
  - (vi) Melaksanakan pengauditan, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
  - (vii) Memberikan amaran terhadap kemungkinan berlakunya ancaman keselamatan ICT seperti virus dan penggadam serta memberi khidmat nasihat dan bantuan teknikal bagi menyediakan langkah perlindungan yang bersesuaian;
  - (viii) Melaporkan insiden keselamatan ICT kepada pengurusan JPS;



- (ix) Bekerjasama dengan semua pihak yang berkaitan dalam menangani ancaman atau insiden keselamatan ICT dan memperakukan langkah penyelesaian atau pencegahan; dan
  - (x) Memberi perakuan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT JPS.
- (c) Pengurus ICT
- (i) Memastikan kajian semula dan pelaksanaan kawalan keselamatan ICT selaras dengan keperluan JPS;
  - (ii) Melaporkan ancaman atau insiden keselamatan ICT kepada ICTSO;
  - (iii) Menentukan kawalan capaian pengguna terhadap aset ICT; dan
  - (iv) Memastikan penyimpanan rekod, bahan bukti dan laporan ancaman atau insiden keselamatan ICT JPS dilaksanakan dengan berkesan.
- (d) Pentadbir Sistem ICT
- (i) Menjaga kerahsiaan maklumat keselamatan ICT;
  - (ii) Mengambil tindakan segera apabila dimaklumkan mengenai sebarang perubahan pengguna dalaman / luaran / asing berkaitan pengurusan ICT;
  - (iii) Menentukan pelaksanaan tahap capaian kemudahan ICT adalah bertepatan dengan arahan pemilik maklumat;
  - (iv) Memantau dan menyediakan laporan aktiviti penggunaan dan capaian pengguna;
  - (v) Mengenal pasti dan melaporkan aktiviti tidak normal berkaitan ICT kepada Pengurus ICT; dan
  - (vi) Menyimpan dan menganalisis rekod jejak audit.





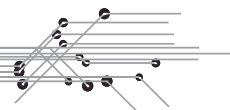
- (e) Pengguna Dalam  
  - (i) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JPS;
  - (ii) Menjaga kerahsiaan maklumat berkaitan penggunaan ICT;
  - (iii) Mengikuti dan menghayati program kesedaran keselamatan ICT;
  - (iv) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT JPS seperti di **LAMPIRAN A** atau yang setara dengannya; dan
  - (v) Melaporkan aktiviti yang tidak normal berkaitan ICT kepada Bahagian Pengurusan Maklumat (BPM) JPS.

## 2.4 Juruaudit

- (a) Mengkaji dan menilai kawalan ke atas pematuhan dan pemantauan keselamatan ICT berdasarkan dasar, *standard* dan prosedur keselamatan maklumat; dan
- (b) Menilai kawalan pengurusan keselamatan aset ICT.

## 2.5 Penasihat Undang-undang

- (a) Menyediakan khidmat nasihat perundangan bagi memastikan aktiviti ICT JPS dapat dijalankan sepenuhnya berdasarkan undang-undang dan peraturan yang berkuat kuasa;
- (b) Menyediakan khidmat nasihat perundangan bagi melindungi aset, sumber dan pegawai JPS terhadap pelbagai risiko perundangan;
- (c) Menyediakan khidmat nasihat perundangan bagi memastikan aktiviti JPS dapat dijalankan sepenuhnya berdasarkan undang-undang dan peraturan yang berkuat kuasa;
- (d) Memberi khidmat nasihat dan bantuan perundangan dalam pengurusan kontrak termasuk urusan penyediaan, kajian semula, penyelesaian pertikaian, melaksanakan tindakan perundangan ke atas pihak yang berkenaan dan menyelaras urusan tindakan perundangan ke atas JPS (sekiranya ada);



- (e) Menyediakan khidmat nasihat perundangan bagi melindungi aset, sumber dan pegawai JPS terhadap pelbagai risiko perundangan;
- (f) Menyedia dan menyemak kontrak dengan menyediakan terma dan syarat yang bersesuaian bagi memastikan aktiviti JPS yang dilaksanakan mengikut undang-undang dan peraturan; dan
- (g) Menyediakan khidmat nasihat tindakan perundangan yang sah ke atas individu, firma, syarikat, pertubuhan atau perundingan yang melanggar pelaksanaan sesuatu kontrak.

## **2.6 Pengurus Sumber Manusia**

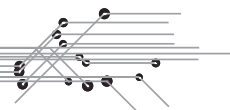
- (a) Memaklumkan dasar, polisi, pekeliling dan garis panduan pengurusan sumber manusia berkaitan dengan ICT;
- (b) Menyediakan khidmat sokongan pentadbiran bagi urusan menyimpan dan menyelenggara maklumat pengurusan sumber manusia berkaitan dengan ICT dengan mematuhi peraturan, undang-undang dan polisi yang berkuat kuasa;
- (c) Memaklumkan sebarang pertukaran, perpindahan, persaraan dan/atau penamatan perkhidmatan Pegawai kepada pentadbir sistem ICT;
- (d) Menyelaraskan urusan tata tertib dan perkhidmatan sumber manusia; dan
- (e) Menghebahkan dasar, polisi, pekeliling dan garis panduan yang berkaitan dengan perjawatan, penilaian prestasi, kemajuan kerjaya, skim gaji dan perkara-perkara lain yang berkaitan dengan perjawatan.

## **2.7 Pengguna Luaran/Asing atau Pihak Ketiga**

- (a) Menjaga kerahsiaan maklumat berkaitan penggunaan ICT;
- (b) Menandatangani Borang Soalan Keselamatan (Borang KPKK 11) atau borang yang setara/berkaitan yang berkuat kuasa;



- (c) Melaporkan aktiviti yang tidak normal berkaitan ICT kepada Bahagian Pengurusan Maklumat (BPM) JPS; dan
- (d) Mendapatkan kelulusan untuk menggunakan kemudahan ICT JPS.



### 3. PENGURUSAN ASET

#### Objektif:

Memastikan setiap aset hendaklah dikenal pasti, di kelas, di rekod dan diselenggara untuk memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT.

#### 3.1 Pengurusan Aset

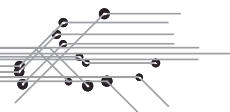
Semua aset ICT di JPS mestilah diuruskan mengikut peraturan dan tatacara yang berkuatkuasa. Setiap aset ICT hendaklah didaftarkan dalam Sistem Pemantauan Pengurusan Aset (SPA). Ketua Jabatan atau Ketua Bahagian adalah bertanggung jawab mengenal pasti pemilik aset ICT tersebut. Setiap pegawai adalah bertanggungjawab terhadap apa-apa kekurangan, kerosakan atau kehilangan aset ICT di bawah tanggungannya.

Aset ICT didefinisikan sebagai semua yang mempunyai nilai kepada agensi merangkumi perkakasan, perisian, perkhidmatan, data atau maklumat dan juga sumber manusia.

#### 3.2 Tanggungjawab Pengurusan Aset

Semua aset ICT yang dimiliki atau digunakan hendaklah diberikan kawalan dan tahap perlindungan yang sesuai oleh Ketua Pejabat mengikut peraturan yang berkuat kuasa seperti berikut:

- (a) Pemilik aset hendaklah menentukan tahap sensitiviti (terperingkat) yang bersesuaian bagi setiap maklumat aset di JPS. Pemilik aset juga hendaklah membuat keputusan dalam menentukan individu yang dibenarkan untuk capaian dan penggunaan maklumat tersebut. Pemilik aset hendaklah mematuhi Garis Panduan Pengkelasan dan Pengendalian Maklumat (*Information Classification and Handling Guideline*) dengan sewajarnya;
- (b) Pentadbir aset ICT adalah bertanggungjawab untuk menentukan prosedur kawalan khas (contohnya: kawalan capaian), kaedah pelaksanaan dan penyelenggaraan serta menyediakan langkah pemulihan yang konsisten dengan arahan pemilik aset;



- (c) Semua pengguna aset ICT di JPS mestilah mematuhi keperluan kawalan yang telah ditetapkan oleh pemilik aset atau pentadbir sistem. Pengguna adalah terdiri daripada Pegawai JPS (lantikan tetap, pinjaman, kontrak dan sambilan), konsultan, kontraktor atau pihak ketiga yang terlibat secara langsung; dan
- (d) Kehilangan/kecurian aset ICT mestilah dilaporkan serta merta mengikut prosedur pengurusan kehilangan/kecurian yang telah ditetapkan.

### 3.3 Pengelasan, Pelabelan dan Pengendalian Maklumat

#### (a) Pengelasan Maklumat

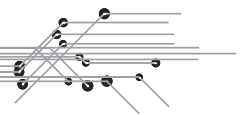
Pengelasan maklumat bertujuan memastikan setiap maklumat diberi perlindungan oleh pemilik aset untuk menentukan keperluan, keutamaan dan tahap keselamatan berdasarkan peraturan yang berkuat kuasa seperti berikut:

- (i) Rahsia Besar;
- (ii) Rahsia;
- (iii) Sulit; dan
- (iv) Terhad.

#### (b) Pelabelan dan Pengendalian Maklumat

Semua maklumat mestilah dilabelkan mengikut klasifikasi maklumat seperti yang dinyatakan pada para 3.3 (a). Sila rujuk Garis Panduan Pengelasan dan Pengendalian Maklumat (*Information Classification and Handling Guideline*) untuk keterangan lanjut.

Aktiviti yang melibatkan pemprosesan maklumat seperti penyalinan, penyimpanan, penghantaran (sama ada dari segi lisan, pos, faksimile dan mel elektronik) dan pemusnahan maklumat mestilah mengikut standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan dalam Garis Panduan Pengelasan dan Pengendalian Maklumat (*Information Classification and Handling Guideline*).



Maklumat yang diklasifikasikan sebagai Rahsia Besar, Rahsia, Sulit dan Terhad perlu dilindungi daripada didedahkan kepada pihak ketiga atau awam. Pihak ketiga jika perlu boleh diberi kebenaran capaian maklumat JPS atas dasar perlu tahu sahaja dan mestilah mendapat kebenaran pemilik aset atau pentadbir sistem.

### 3.4 Akauntabiliti Terhadap Aset ICT

Senarai maklumat aset di JPS hendaklah diwujudkan. Setiap aset perlu ditentukan dengan jelas dan pemilikan aset mestilah dipersetujui dan didokumenkan berserta lokasi semasa aset tersebut. Senarai aset hendaklah disimpan oleh Ketua Jabatan atau Ketua Bahagian.

Rekod aset di JPS adalah terdiri daripada kategori yang berikut:

- (a) Data atau maklumat – dokumentasi sistem, panduan pengguna, maklumat yang telah diarkibkan, pangkalan data, fail-fail data, bahan pembelajaran/latihan, prosedur operasi dan sokongan;
- (b) Sumber manusia – semua Pegawai JPS;
- (c) Perisian – semua perisian yang digunakan untuk mengendali, memproses, menyimpan, menjana dan mengirim maklumat. Ini meliputi perisian sistem, perisian utiliti, perisian rangkaian, program aplikasi, pangkalan data; dan
- (d) Perkakasan ICT – semua perkakasan komputer seperti komputer peribadi, stesen kerja, media magnetik dan alat prasarana seperti *Uninterruptable Power Supply* (UPS).



## 4. PENGURUSAN SUMBER MANUSIA

### Objektif:

Memastikan semua pihak yang terlibat dalam pengurusan dan penggunaan ICT hendaklah bertanggungjawab dan memahami peranan masing-masing mengikut peraturan berkaitan keselamatan ICT yang berkuat kuasa.

### 4.1 Sebelum Berkhidmat

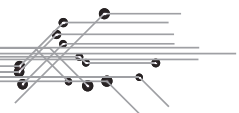
Semua pihak terlibat di dalam pengurusan dan/atau penggunaan aset ICT hendaklah bertanggungjawab dan mematuhi perkara berikut:

- (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;
- (b) Menjalankan tapisan keselamatan selaras dengan keperluan perkhidmatan mengikut peraturan sedia ada; dan
- (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

### 4.2 Dalam Perkhidmatan

Semua pihak yang terlibat dalam pengurusan dan/atau penggunaan aset ICT hendaklah bertanggungjawab dan mematuhi perkara berikut:

- (a) Mengurus keselamatan aset ICT yang dibenarkan mengikut peraturan yang ditetapkan;
- (b) Memastikan tindakan disiplin dan/atau undang-undang dilaksanakan sekiranya berlaku pelanggaran peraturan yang ditetapkan;
- (c) Memastikan tanggung jawab dan peranan dalam pengurusan keselamatan ICT dinyatakan dalam senarai tugas;
- (d) Mengikuti latihan pengurusan keselamatan ICT berdasarkan keperluan; dan
- (e) Mengikuti program kesedaran keselamatan ICT yang disediakan.



### **4.3 Latihan**

Semua Pegawai JPS haruslah diberi latihan yang bersesuaian dan berterusan dalam semua aspek kritikal yang berkaitan dengan tugas mereka seperti keselamatan, pentadbiran sistem, teknik pengaturcaraan dan sebagainya. Setiap Pegawai JPS bertanggungjawab mengenal pasti latihan yang diperlukan. Ketua Jabatan atau Ketua Bahagian bertanggungjawab mengkaji semula keperluan latihan untuk setiap Pegawai di bawahnya.

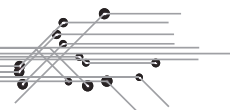
Program kesedaran keselamatan ICT juga perlu dilaksanakan secara berterusan sebagai langkah peringatan kepada Pegawai JPS akan kepentingan keselamatan aset ICT.

### **4.4 Bertukar atau Tamat Perkhidmatan**

Semua pihak yang telah terlibat dalam pengurusan dan/atau penggunaan aset ICT hendaklah bertanggungjawab dan mematuhi perkara berikut:

- (a) Memastikan semua aset ICT dikembalikan kepada JPS mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan
- (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.





## 5. KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif:

Memastikan premis dan kemudahan ICT ditempatkan di kawasan yang selamat dan dilindungi daripada sebarang ancaman fizikal dan persekitaran.

### 5.1 Tanggungjawab Keselamatan Fizikal dan Persekitaran

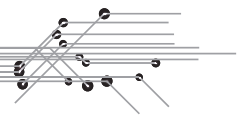
Ketua Pengarah adalah bertanggungjawab untuk melaksanakan langkah-langkah keselamatan yang perlu bagi mengesan, mencegah dan menghalang pencerobohan ke atas premis dan kawasan yang menempatkan kemudahan ICT berdasarkan peraturan yang berkuat kuasa.

### 5.2 Kawalan Kawasan Terperingkat

Kawasan terperingkat adalah premis yang dilengkapi dengan sistem keluar masuk.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
- (b) Melindungi kawasan terhad melalui kawalan keluar masuk yang bersesuaian bagi memastikan Pegawai yang diberi kebenaran sahaja boleh melalui pintu masuk ini;
- (c) Melaksana perlindungan fizikal dan menyediakan garis panduan untuk semua yang bekerja di dalam kawasan terhad;
- (d) Memastikan kawasan-kawasan penghantaran dan pemunggahan serta tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya;
- (e) Pusat data yang tiada pengawal (*unmanned*) mestilah dikunci. Pegawai sokongan teknikal daripada pihak ketiga hanya dibenarkan memasuki pusat data sekiranya perlu dan kehadiran mereka mestilah direkodkan, disahkan, diiringi dan diawasi oleh pentadbir sistem;



- (f) Aktiviti mengambil gambar, merakam video, merekodkan suara atau penggunaan peralatan yang seumpamanya tidak dibenarkan di dalam pusat data kecuali dengan kebenaran ICTSO;
- (g) Peralatan rakaman/penyimpanan seperti kamera, video, perakam suara dan storan mudah alih adalah tidak dibenarkan dibawa masuk ke dalam pusat data dan perlu disimpan di dalam kabinet yang disediakan; dan
- (h) Individu yang tidak mempunyai pengenalan diri, pengenalan diri terlindung atau gagal mengemukakan pengenalan diri yang sah perlu diiringi ke Pondok Pengawal Keselamatan dengan segera.

### 5.3 Keselamatan Peralatan

Melindungi peralatan ICT daripada kehilangan, kerosakan, kecurian atau kompromi ke atas aset ICT dan gangguan ke atas sistem penyampaian agensi.

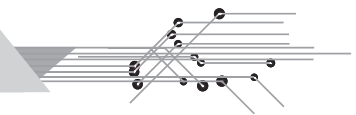
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Perkakasan
  - (i) Menempatkan dan mengawal peralatan ICT supaya risiko ancaman dan bencana dari persekitaran serta percubaan mencaroboh oleh pihak yang tidak diberi kebenaran dapat dikurangkan; dan
  - (ii) Semua cadangan pengubahsuaian, pembelian, penempatan dan pemindahan peralatan-peralatan ICT hendaklah dirujuk terlebih dahulu kepada ICTSO.

- (b) Dokumen

Bagi memastikan integriti, kerahsiaan dan kebolehsediaan maklumat serta pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi:

- (i) Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin;
- (ii) Menggunakan tanda atau label keselamatan seperti rahsia besar, rahsia, sulit atau terhad pada dokumen;



- (iii) Satu sistem pengurusan dokumen terperingkat hendaklah diwujudkan bagi menerima, memproses, menyimpan dan menghantar dokumen-dokumen tersebut supaya ianya diuruskan berasingan daripada dokumen-dokumen tidak terperingkat; dan
  - (iv) Menggunakan enkripsi ke atas dokumen terperingkat yang disediakan dan dihantar secara elektronik.
- (c) Media Storan (disket, pita magnetik, cakera keras, CD-ROM, DVD-ROM, *thumb drive* dan media storan lain).

Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

Langkah-langkah pencegahan yang perlu diambil adalah seperti berikut:

- (i) Menyediakan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
- (ii) Mengehadkan capaian kepada pengguna yang dibenarkan sahaja;
- (iii) Sebarang pelupusan hendaklah merujuk kepada tatacara pelupusan; dan
- (iv) Mengadakan sistem pengurusan media termasuk inventori, pergerakan, pelabelan dan *backup/restore*.

## 5.4 Prasarana Sokongan

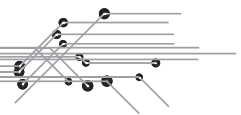
- (a) Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan perolehan dan pengubahsuaian hendaklah dirujuk terlebih dahulu kepada pihak-pihak yang berkaitan.



Perkara yang perlu dipatuhi adalah seperti berikut:

- (i) Merancang dan menyediakan pelan keseluruhan pusat data termasuk ruang peralatan komputer, ruang percetakan dan ruang atur pejabat;
- (ii) Melengkapi semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;
- (iii) Memasang peralatan perlindungan di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
- (iv) Menyimpan bahan mudah terbakar di luar kawasan kemudahan penyimpanan aset ICT;
- (v) Meletakkan semua bahan cecair di tempat yang bersesuaian dan berjauhan dari aset ICT khususnya di dalam pusat data;
- (vi) Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer;
- (vii) Menyemak dan menguji semua peralatan perlindungan sekurang-kurangnya satu (1) kali setahun. Aktiviti dan keputusan ujian perlu direkodkan bagi tujuan rujukan dan tindakan;
- (viii) Mematuhi peraturan yang telah ditetapkan oleh pihak berkuasa seperti Jabatan Bomba dan Penyelamat (BOMBA), Jabatan Kerja Raya (JKR) dan sebagainya; dan
- (ix) Melengkapkan premis dengan sistem penggera kebakaran automatik. Pemasangan sistem pengesan kebakaran perlu mendapat kelulusan pihak berkuasa tempatan serta perlu diperiksa dan diselenggara secara berkala sekurang-kurangnya sekali setahun. Alat pemadam api mudah alih perlu diletakkan di tempat yang strategik dan tidak terlindung. Langkah-langkah penggunaan peralatan juga perlu dipaparkan.



(b) Bekalan Kuasa

- (i) Melindungi semua peralatan ICT dari kegagalan bekalan elektrik dengan menyalurkan bekalan kuasa yang bersesuaian;
- (ii) Menggunakan peralatan sokongan seperti UPS dan penjana (*generator*) bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan; dan
- (iii) Menyemak dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.

(c) Prosedur Kecemasan

- (i) Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan oleh Pegawai Keselamatan JPS;
- (ii) Melaporkan insiden kecemasan persekitaran kepada Pegawai Keselamatan JPS;
- (iii) Mengadakan, menguji dan mengemas kini pelan kecemasan dari semasa ke semasa; dan
- (iv) Mengadakan latihan kecemasan bencana sekurang-kurangnya setahun sekali.

(d) Keselamatan Rangkaian

Kabel elektrik dan telekomunikasi yang menyalurkan data atau menyokong sistem penyampaian perkhidmatan hendaklah dilindungi daripada pencerobohan dan kerosakan.

Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

- (i) Melabel dan menggunakan kabel mengikut spesifikasi yang telah ditetapkan;
- (ii) Melindungi kabel daripada kerosakan;



- (iii) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan
- (iv) Membuat pelabelan kabel.

## 5.5 Penyelenggaraan Peralatan

Perkakasan hendaklah disenggarakan berdasarkan peraturan-peraturan semasa bagi memastikan kebolehsediaan, kerahsiaan dan integriti.

Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

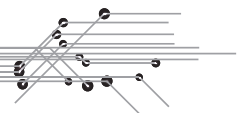
- (a) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;
- (b) Memastikan perkakasan hanya diselenggara oleh Pegawai atau pihak yang dibenarkan sahaja;
- (c) Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan; dan
- (d) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

## 5.6 Peminjaman Peralatan

Peralatan yang dipinjam hendaklah mendapat kelulusan mengikut peraturan yang telah ditetapkan oleh JPS.

Langkah-langkah perlu diambil termasuklah seperti berikut:

- (a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh JPS bagi membawa keluar peralatan bagi tujuan yang dibenarkan;
- (b) Melindungi dan mengawal peralatan sepanjang masa;
- (c) Merekodkan aktiviti peminjaman dan pemulangan peralatan; dan
- (d) Menyemak peralatan ketika peminjaman dan pemulangan dilakukan.



## 5.7 Pengendalian Peralatan Luar yang Dibawa Masuk / Keluar

Langkah keselamatan yang perlu diambil dalam mengendalikan peralatan luar yang dibawa masuk/keluar adalah seperti berikut:

- (a) Memastikan peralatan yang dibawa masuk/keluar tidak mengancam keselamatan ICT JPS; dan
- (b) Mendapatkan kelulusan agensi mengikut peraturan yang telah ditetapkan.

## 5.8 Pelupusan Peralatan

Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan Kerajaan.

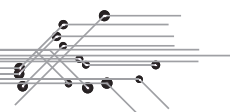
Langkah-langkah hendaklah diambil termasuklah menghapuskan semua kandungan peralatan khususnya maklumat rahsia rasmi sebelum dilupuskan.

## 5.9 *Clear Desk* dan *Clear Screen*

*Clear Desk* bermaksud tidak mendedahkan sebarang maklumat yang sensitif di tempat kerja. Manakala *Clear Screen* bermaksud tidak memaparkan sebarang maklumat sensitif di atas skrin atau yang seumpama dengannya tanpa pengawasan.

Dasar *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat yang tersimpan di dalam media storan tidak mengalami kerosakan, kecurian dan kehilangan:

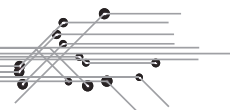
- (a) Menggunakan kemudahan seperti *password screen saver* atau *logout* apabila meninggalkan komputer. *Password screen saver* akan diaktifkan secara automatik di dalam tempoh tidak melebihi sepuluh (10) minit;
- (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan
- (c) Memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimile dan mesin fotostat.



#### **5.10 Melaporkan Kehilangan atau Kecurian Pas Keselamatan, Kad Pengenalan Jabatan, Kad Kuasa dan Kad Pelantikan**

Kehilangan atau kecurian pas keselamatan, kad pengenalan jabatan, kad kuasa dan kad pelantikan mestilah dilaporkan serta merta oleh pemilik pas/kad kepada pihak yang mengeluarkannya.





## 6. PENGURUSAN OPERASI DAN KOMUNIKASI

Objektif:

Memastikan kemudahan pemprosesan maklumat dan komunikasi adalah berfungsi dengan baik dan selamat.

### 6.1 Pengendalian Prosedur

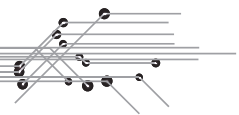
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Semua prosedur operasi yang diwujudkan, dikenal pasti dan diguna pakai hendaklah didokumenkan, disimpan dan dikawal;
- (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan
- (c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.

### 6.2 Pengurusan Penyampaian Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal, pakar runding dan pihak-pihak lain;
- (b) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pembekal, pakar runding dan pihak-pihak lain;
- (c) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan



- (d) Pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyelenggarakan dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.

### **6.3 Perancangan dan Penerimaan Sistem**

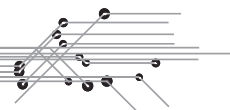
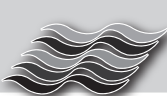
Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Penggunaan peralatan dan sistem mestilah dipantau, ditala (*tuned*) dan perancangan perlu dibuat bagi memenuhi keperluan kapasiti akan datang untuk memastikan prestasi sistem di tahap optimum;
- (b) Kriteria penerimaan untuk peralatan dan sistem baru, peningkatan dan versi baru perlu ditetapkan dan ujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem; dan
- (c) Semua urusan penerimaan dan ujian hendaklah direkodkan dengan jelas dan teratur bagi mengurangkan risiko kegagalan sistem.

### **6.4 Pengurusan dan Kawalan Perubahan**

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Perubahan atau pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;
- (b) Aktiviti-aktiviti seperti memasang, menyelenggarakan, 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;
- (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan



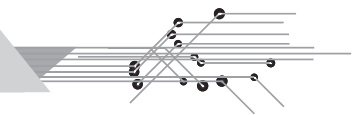
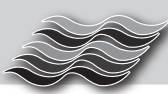
- (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

## 6.5 Perlindungan Dari *Malicious* dan *Mobile Code*

*Mobile code* ditafsirkan sebagai kod perisian yang dipindahkan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi-fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna.

Bagi tujuan perlindungan dari *malicious* dan *mobile code*, perkara yang mesti dipatuhi adalah seperti berikut:

- (a) Kawalan pencegahan, pengesanan dan pemulihan untuk melindungi integriti maklumat dan perisian daripada ancaman *malicious code* seperti *viruses*, *worms*, *trojan horses* dan *logic bombs*;
- (b) Dalam keadaan di mana *mobile code* dibenarkan, konfigurasiya hendaklah memastikan bahawa ianya beroperasi berdasarkan kepada dasar keselamatan yang jelas dan penggunaan *mobile code* yang tidak dibenarkan adalah dilarang sama sekali;
- (c) Semua penggunaan perisian hendaklah mematuhi lesen perisian dan disahkan oleh Ketua Jabatan / Ketua Bahagian. Ketua Bahagian haruslah dimaklumkan jika terdapat keperluan penggunaan perisian percuma (*freeware*) untuk tugas-tugas yang berkaitan;
- (d) Pegawai dilarang memuat turun sebarang fail atau perisian daripada sumber yang tidak diketahui (sama ada dari rangkaian luar atau sebarang media) melainkan telah diimbis bagi memastikan ianya bebas dari kod yang mencurigakan sebelum digunakan;
- (e) Penggunaan media mudah alih seperti, *tape* cakera, cakera liut, pemacu keras, CD dan DVD mestilah dikawal di dalam pusat data. Penggunaan media tersebut hanya dibenarkan untuk melaksanakan kerja yang berkaitan sahaja;
- (f) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;



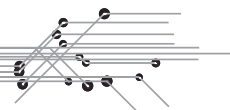
- (g) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;
- (h) Mengemas kini anti virus dengan *pattern* anti virus yang terkini;
- (i) Menyemak kandungan sistem atau maklumat mengikut keperluan bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;
- (j) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;
- (k) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;
- (l) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan
- (m) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

## 6.6 ***Backup dan Restore***

Bagi memastikan sistem dapat dipulihkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Membuat *backup* dan *restore* ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru bagi mengekalkan integriti, kesediaan dan kemudahan pemprosesan maklumat;
- (b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi menyimpan sekurang-kurangnya tiga (3) generasi *backup*. Kekerapan *backup* bergantung pada tahap kritikal maklumat;
- (c) Membuat dan menguji secara berkala sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan



- (d) Merekodkan dan menyimpan salinan *backup* di premis yang berbeza dan selamat.

## 6.7 Pengurusan Keselamatan Rangkaian

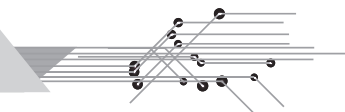
Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Memastikan perlindungan keselamatan maklumat dalam rangkaian serta infrastruktur sokongan;
- (b) Rangkaian perlu dikawal, dipantau dan diurus sebaiknya, bertujuan untuk mengawal daripada sebarang ancaman bagi menjamin keselamatan sistem dan aplikasi yang menggunakan rangkaian, termasuk maklumat yang dipindahkan melaluinya; dan
- (c) Ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian perlu dikenal pasti dan dimasukkan dalam mana-mana perjanjian perkhidmatan rangkaian sama ada perkhidmatan berkenaan disediakan secara dalaman atau melalui khidmat luar.

## 6.8 Pengendalian Peralatan Penyimpanan Maklumat

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Memastikan tidak berlaku pendedahan, pengubahsuaian, peralihan atau pemusnahan aset secara tidak sah, yang boleh mengganggu aktiviti perkhidmatan;
- (b) Prosedur perlu disediakan untuk pengurusan peralatan penyimpanan maklumat mudah alih;
- (c) Peralatan penyimpanan maklumat yang tidak digunakan perlu dilupuskan secara selamat mengikut prosedur yang telah ditetapkan;
- (d) Prosedur untuk mengendali dan menyimpan maklumat perlu diwujudkan untuk melindungi maklumat daripada didedah tanpa kebenaran atau disalah guna; dan
- (e) Dokumentasi sistem perlu dilindungi daripada capaian yang tidak dibenarkan.



## 6.9 Pertukaran Maklumat

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Polisi, prosedur dan kawalan pertukaran maklumat yang rasmi perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi dalam agensi dan mana-mana pihak terjamin;
- (b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara agensi dengan pihak luar;
- (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari agensi;
- (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan
- (e) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat agensi.

## 6.10 Perkhidmatan e-Dagang (e-Commerce)

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Maklumat yang terlibat dalam e-Dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan dalam memastikan keselamatan perkhidmatan e-dagang dan penggunaannya;
- (b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan
- (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.



## 6.11 Pemantauan

Perkara yang mesti dipatuhi termasuk yang berikut:

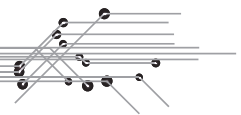
- (a) Mengesan aktiviti pemprosesan maklumat yang tidak dibenarkan dan memastikan rekod log aktiviti tidak boleh diubahsuai dan dicapai oleh pihak yang tidak dibenarkan;
- (b) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;
- (c) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala;
- (d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;
- (e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkod, dianalisis dan diambil tindakan sewajarnya; dan
- (f) Masa yang berkaitan dengan sistem pemprosesan maklumat dalam agensi atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.

## 6.12 Pengasingan Bidang Tugas

Ketua Bahagian/Ketua Seksyen/Ketua Unit hendaklah memastikan pengasingan bidang tugas terutama bagi bidang tugas yang kritikal dan sensitif seperti pemantauan aktiviti, jejak audit dan pemantauan pengurusan bagi mengelakkan konflik dan pertindihan arahan.

Kawalan capaian secara *logical* mestilah digunakan bagi membolehkan pemisahan bidang tugas dilaksanakan dan mengikut prinsip seperti berikut:

- (a) Pegawai tidak boleh mempunyai capaian untuk melakukan pengemaskinian ke atas mana-mana sistem aplikasi yang sedang beroperasi kecuali setelah mendapat kelulusan; dan
- (b) Pembangun Sistem tidak dibenarkan mempunyai akses rutin ke atas data, sistem atau perisian aplikasi yang beroperasi.



### 6.13 Pengasingan Infrastruktur Operasi dan Pembangunan

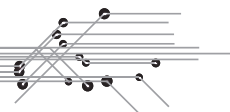
Persekitaran perisian aplikasi yang sedang dibangunkan mestilah diasingkan daripada persekitaran perisian aplikasi yang beroperasi seperti berikut:

- (a) Sekiranya infrastruktur sedia ada membolehkan pengasingan tersebut, ia perlulah diasingkan secara fizikal dengan menggunakan sistem komputer yang berasingan; dan
- (b) Sekiranya persekitaran fizikal tidak membolehkan, penggunaan direktori dan *library* dengan kawalan capaian yang sesuai perlu dilaksanakan.

### 6.14 Pelarasan Masa untuk Semua Sistem Di Dalam Pusat Data

Semua masa bagi sistem kritikal yang ditempatkan di dalam rangkaian dalaman JPS mesti diselaraskan menggunakan titik rujukan masa daripada sumber yang ditetapkan seperti menggunakan masa *Domain Controller*.





## 7. KAWALAN CAPAIAN

Objektif:

Memastikan kawalan terhadap capaian maklumat.

### 7.1 Keperluan Kawalan Capaian

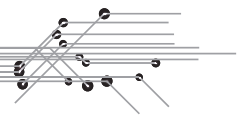
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna;
- (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;
- (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih;
- (d) Kawalan ke atas kemudahan had capaian maklumat; dan
- (e) Pengguna perlu mematuhi amalan *clear desk* dan *clear screen*.

### 7.2 Kawalan Capaian Pengguna

Perkara-perkara yang perlu dipatuhi adalah termasuk:

- (a) Mewujudkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan;
- (b) Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat;
- (c) Akaun pengguna yang diwujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran secara bertulis dan direkodkan; dan
- (d) Tindakan pengemaskinian dan/atau pembatalan pemilikan dan capaian pengguna hendaklah diambil atas sebab seperti berikut:



- (i) Pengguna tidak hadir bertugas tanpa kebenaran melebihi dari tujuh (7) hari;
- (ii) Pengguna bercuti atau bertugas di luar pejabat mengikut peraturan yang berkuat kuasa;
- (iii) Pengguna bertukar jawatan, tanggungjawab dan/atau bidang tugas. Pembatalan akan dilakukan di hari terakhir pertukaran tersebut berlaku (seperti yang dimaklumkan oleh pihak yang mengendalikan pengurusan sumber manusia);
- (iv) Pengguna yang sedang dalam prosiding dan/atau dikenakan tindakan tatatertib oleh Pihak Berkuasa Tatatertib. Pembatalan akan dilakukan serta merta apabila dimaklumkan oleh pihak yang mengendalikan pengurusan sumber manusia; dan
- (v) Pengguna bertukar, berpindah, bersara dan/atau tamat perkhidmatan. Pembatalan akan dilakukan berdasarkan tarikh arahan yang dikeluarkan oleh Bahagian Khidmat Pengurusan (BKP).

Aktiviti capaian oleh pengguna direkod, diselenggara dengan sistematik dan dikaji dari semasa ke semasa. Maklumat yang direkod termasuk identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya.

### 7.3 Pengurusan Kata Laluan

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

- (a) Pengguna tidak seharusnya menulis atau menyimpan kata laluan tanpa *encryption* di atas talian melainkan pada kes-kes tertentu di mana ia diperlukan oleh prosedur operasi seperti penyimpanan ID dasar (*root* ID) atau ID kata laluan penting bagi sistem utama. Di dalam hal ini, kata laluan haruslah dilindungi dengan menggunakan mekanisme kawalan lain seperti menyimpan kata laluan di dalam laci berkunci dan menggunakan kata laluan yang berbeza bagi capaian berbeza;



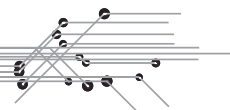
- (b) Pengguna adalah tidak digalakkan mengguna kata laluan yang sama bagi kegunaan sistem di JPS mahupun sistem yang tidak terdapat di JPS;
- (c) Pengguna hendaklah tidak mendedahkan kata laluan yang diguna pakai di JPS kepada sesiapa. Ini termasuklah ahli keluarga dan bukan ahli keluarga apabila melakukan kerja pejabat di rumah. Walau bagaimana pun, bagi ID kata laluan utama yang disimpan di dalam laci berkunci, harus diadakan satu proses mengenai tatacara memperoleh kata laluan berkenaan sekiranya berlaku ketidakhadiran pemegang kata laluan utama sewaktu ia diperlukan;
- (d) Pengguna haruslah menyimpan kata laluan mereka dengan selamat dan tidak dibenarkan berkongsi akaun dengan pengguna lain. Pengguna yang disahkan adalah bertanggungjawab ke atas kerahsiaan dan keselamatan kata laluan dan akaun mereka;
- (e) Penggunaan fungsi *Remember Password* adalah tidak dibenarkan sama sekali. Sekiranya akaun atau kata laluan disyaki telah dicerobohi, maka laporan kejadian hendaklah dilaporkan kepada Bahagian Pengurusan Maklumat dan tindakan menukar kata laluan perlu dilakukan;

Berikut adalah keperluan minimum bagi kata laluan:

- (i) Pengguna biasa – kombinasi di antara lapan (8) huruf dan nombor;
  - (ii) Pentadbir keselamatan, rangkaian dan sistem – sekurang-kurangnya kombinasi di antara lapan (8) huruf dan nombor dengan kualiti kata laluan yang kukuh; dan
  - (iii) *Screen Saver* - sekurang-kurangnya kombinasi di antara lapan (8) huruf dan nombor.
- (f) Sistem pengurusan kata laluan hendaklah menekankan pilihan kata laluan yang berkualiti. Kata laluan yang berkualiti antara lainnya mempunyai ciri-ciri seperti berikut:



- (i) Kata laluan haruslah mengandungi kedua-dua abjad huruf dan bukan huruf (seperti: 0-9, a-z, ! @ # \$ % ^ & \* ( ) - +). Pengguna juga digalakkan untuk menggunakan kombinasi antara huruf besar dan huruf kecil (contoh: p@sSWorD);
  - (ii) Kata laluan *admin/root* bagi sistem utama haruslah mengandungi kombinasi huruf besar dan huruf kecil (contoh: a-z, A-Z);
  - (iii) Kata laluan yang ditentukan oleh pengguna seharusnya tidak digunakan semula. Pengguna haruslah tidak membina kata laluan yang sama atau seakan-akan serupa seperti mana yang pernah digunakan sebelum ini di tempat lain; dan
  - (iv) Kesukaran untuk meneka kata laluan perlulah dipraktikkan. Kata laluan adalah bukan perkataan di dalam mana-mana bahasa, dialek, loghat dan sebagainya. Kata laluan tidak seharusnya berdasarkan maklumat peribadi, nama ahli keluarga dan seumpamanya.
- (g) Kata laluan haruslah ditukar dengan kerap bagi ke semua sistem dan di bawah syarat seperti berikut:
- (i) Kata laluan untuk pentadbir sistem harus ditukar sekurang-kurangnya setiap tiga (3) bulan untuk ke semua sistem utama; dan
  - (ii) Kata laluan untuk pengguna bagi mencapai aplikasi seperti e-mel harus ditukar sekurang-kurangnya bagi setiap enam (6) bulan.
- (h) Kata laluan haruslah ditukar mengikut syarat seperti berikut:
- (i) Daftar masuk kali pertama bagi pengguna baru;
  - (ii) Apabila terdapat kata laluan biasa (*default*) yang telah disediakan di dalam sistem atau dibekalkan oleh pihak pembekal;
  - (iii) Setiap kali pengguna mengesyaki kata laluan telah diketahui oleh orang lain; dan



- (iv) Apabila hak capaian pengguna bertukar disebabkan perubahan tanggungjawab di dalam bidang tugas.

Nota: Keperluan seperti yang dinyatakan di atas adalah bergantung kepada keupayaan sistem yang digunakan.

## 7.4 Kawalan Capaian Rangkaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

- (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian JPS, rangkaian agensi lain dan rangkaian awam;
- (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna;
- (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT;
- (d) Maklumat IP dalaman, konfigurasi dan reka bentuk dalaman setiap sistem di JPS mesti mempunyai kawalan capaian yang terhad bagi menghalang capaian dari luar JPS;
- (e) Semua rangkaian JPS mestilah mempunyai *domain logical* yang dipisahkan dan dilindungi dengan menggunakan perimeter keselamatan dan mekanisme kawalan capaian tertentu;
- (f) Untuk membolehkan JPS bertindak terhadap ancaman luar, semua aset ICT yang bersambung ke Internet mestilah dilindungi oleh *Intrusion Detection System* (IDS) atau *Intrusion Prevention System* (IPS);
- (g) Semua rangkaian dalaman JPS mesti melalui pusat kawalan capaian tertentu (contohnya *firewall*) sebelum pengguna mencapai sistem JPS;
- (h) Semua *firewall* yang digunakan untuk melindungi rangkaian dalaman JPS mesti beroperasi di dalam sistem yang tersendiri dan tidak boleh mempunyai operasi sistem selainnya; dan
- (i) Memastikan maklumat berkaitan reka bentuk dan konfigurasi sistem rangkaian JPS hanya terhad kepada pihak yang dibenarkan sahaja.



## 7.5 Kawalan Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan.

Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:

- (a) Mengesahkan pengguna yang dibenarkan;
- (b) Mewujudkan jejak audit (*audit trail*) ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*;
- (c) Memberi amaran sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem;
- (d) Menyediakan kaedah yang sesuai untuk pengesahan capaian (*authentication*); dan
- (e) Mengehadkan tempoh penggunaan mengikut kesesuaian.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log-on* yang terjamin;
- (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;
- (c) Menghadkan dan mengawal penggunaan program utiliti yang berkemampuan mengatasi sebarang kawalan sistem dan aplikasi;
- (d) Menamatkan sesuatu sesi yang tidak aktif sekiranya tidak digunakan bagi satu tempoh yang ditetapkan; dan
- (e) Mengehadkan tempoh sambungan ke sesuatu aplikasi berisiko tinggi.

## 7.6 Kawalan Capaian Aplikasi dan Maklumat

Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara berikut hendaklah dipatuhi:



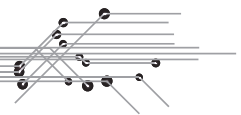
- (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;
- (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);
- (c) Menghadkan capaian sistem dan aplikasi kepada lima (5) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;
- (d) Menyediakan mekanisme perlindungan bagi menghalang capaian tidak sah ke atas aplikasi dan maklumat; dan
- (e) Mewujudkan persekitaran pengkomputeran yang khusus dan terasing untuk sistem maklumat terperingkat (sulit/rahsia).

## **7.7 Peralatan Mudah Alih dan Kerja Jarak Jauh**

Perkara yang perlu dipatuhi bagi memastikan keselamatan peralatan mudah alih dan kerja jarak jauh terjamin adalah seperti berikut:

- (a) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi;
- (b) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat;
- (c) Memastikan bahawa antivirus digunakan dan sentiasa dikemaskinikan untuk aset ICT;
- (d) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan
- (e) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.

Untuk pegawai teknikal, komunikasi dari jarak jauh untuk mengendalikan sistem di dalam pusat data mestilah menggunakan *Virtual Private Network* (VPN).



## 7.8 Penggunaan Capaian Tanpa Wayar

Pemasangan peralatan rangkaian tanpa wayar adalah tidak dibenarkan. Sekiranya ada keperluan, nasihat dan kelulusan daripada Bahagian Pengurusan Maklumat (BPM) adalah diperlukan.

Pengguna kemudahan tanpa wayar perlu mematuhi perkara berikut :

- (a) Memastikan peralatan yang digunakan mempunyai perisian antivirus yang sentiasa dikemaskini.
- (b) Memahami ancaman dan risiko yang wujud di atas penggunaan kemudahan ini dan bertanggungjawab sepenuhnya sekiranya berlaku sesuatu yang tidak diingini.

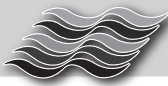
## 7.9 Tanggungjawab Pengguna

Seksyen ini bertujuan memastikan pengguna melaksanakan langkah berkesan ke atas kawalan capaian untuk menghalang penyalahgunaan, kecurian maklumat dan kemudahan proses maklumat.

Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut:

- (a) Mematuhi amalan terbaik pemilihan dan penggunaan kata laluan;
- (b) Memastikan kemudahan dan peralatan yang tidak digunakan mendapat perlindungan sewajarnya; dan
- (c) Mematuhi amalan *clear desk policy* dan *clear screen policy*.





## 8. PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

### Objektif:

Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

### 8.1 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;
- (b) Ujian keselamatan hendaklah dijalankan ke atas 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;
- (c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan
- (d) Semua sistem yang dibangunkan secara dalaman/luaran hendaklah diuji sepenuhnya bagi memenuhi keperluan keselamatan yang telah ditetapkan;

### 8.2 Kawalan Kriptografi (*Cryptography*)

Kriptografi bermaksud sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.

Tindakan melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi yang boleh dilakukan adalah seperti berikut:

- (a) Pengguna digalakkan membuat enkripsi (*encryption*) dengan menukarkan teks biasa (*plaintext*) kepada bentuk *ciphertext* ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa;



- (b) Penggunaan tandatangan digital digalakkan kepada semua pengguna yang menguruskan transaksi maklumat rahsia rasmi secara elektronik; dan
- (c) Pengurusan ke atas *Public Key Infrastructure* (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.

### 8.3 Kawalan Fail Sistem

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

### 8.4 Keselamatan Dalam Proses Pembangunan dan Sokongan

Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut:

- (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;
- (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan



tiada kesan yang buruk terhadap operasi dan keselamatan agensi;

- (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;
- (d) Mewujudkan jejak audit dalam sistem aplikasi;
- (e) Capaian kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan;
- (f) Menghalang sebarang peluang untuk membocorkan maklumat;
- (g) Pembangunan perisian secara khidmat luar (*outsourcing*) perlu diselia dan dipantau oleh pemilik sistem;
- (h) Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik JPS; dan
- (i) Kawalan yang bersesuaian dan log audit perlu di reka bentuk ke dalam sistem aplikasi. Ini termasuklah pengesahan data yang dimasukkan, data yang dihasilkan, pemprosesan dalaman, pengesahan dan integriti mesej dan sebagainya. Ukuran keselamatan mesti dititik beratkan semasa membangunkan aplikasi baru atau mengemas kini / menambah baik aplikasi sedia ada.

### 8.5 Kawalan Teknikal Keterdedahan (*Vulnerability*)

Keterdedahan adalah bermaksud sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman.

Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan adalah seperti berikut:

- (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;
- (b) Menilai tahap keterdedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan
- (c) Mengambil langkah kawalan untuk mengatasi risiko berkaitan.



## 9. PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

### Objektif:

- Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.
- Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

### 9.1 Pengurusan Pengendalian Insiden Keselamatan

ICTSO bertanggungjawab mengurus dan mengendalikan insiden keselamatan ICT termasuk perkara-perkara berikut:

- (a) Menguruskan tindakan ke atas insiden yang berlaku sehingga keadaan pulih; dan
- (b) Menentukan sama ada sesuatu insiden perlu dilaporkan kepada agensi penguatkuasaan undang-undang/keselamatan.

### 9.2 Insiden Keselamatan

Insiden keselamatan bermaksud musibah (*adverse event*) yang berlaku ke atas sistem maklumat dalam pelbagai keadaan seperti:

- (a) Percubaan (sama ada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran (*probing*);
- (b) Serangan kod jahat (*malicious code*) seperti virus, *trojan horse*, *worms* dan seumpamanya;
- (c) Gangguan yang disengajakan (*intended disruption*) atau penafian penyampaian perkhidmatan (*denial of service*);
- (d) Menggunakan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran (*unauthorised access*); dan
- (e) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak.



### 9.3 Melaporkan Insiden

Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada *Government Computer Emergency Response Team* (GCERT) dan dimaklumkan kepada NRECert. Semua maklumat adalah SULIT dan tidak boleh didedahkan tanpa kebenaran daripada ICTSO.

### 9.4 Menentukan Keutamaan Tindakan Ke Atas Insiden

Tindakan ke atas insiden yang dilaporkan akan dibuat berasaskan tahap kritikal sesuatu insiden. Keutamaan akan ditentukan seperti berikut:

#### **Keutamaan 1:**

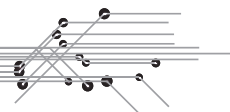
Aktiviti yang berkemungkinan mengancam nyawa atau keselamatan negara.

#### **Keutamaan 2:**

- (a) Pencerobohan atau percubaan penceroboh melalui infrastruktur Internet ke atas peralatan rangkaian;
- (b) Penyebaran penafian penyampaian perkhidmatan (*distributed denial of service*);
- (c) Serangan atau pendedahan keterdedahan terbaru (*new vulnerabilities*); atau

Lain-lain insiden seperti:

- (a) Pencerobohan melalui pemalsuan identiti;
- (b) Pengubahsuaian laman web, perisian, atau mana-mana komponen sistem tanpa pengetahuan, arahan atau persetujuan pihak yang berkenaan; dan
- (c) Gangguan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran.



## 9.5 Pengendalian Insiden

Sekiranya berlaku insiden kritikal di bawah Keutamaan 1, agensi seperti yang disenaraikan di bawah boleh dihubungi:

**(a) Ketua Pengarah JPS Malaysia**

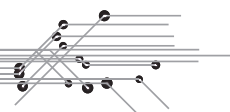
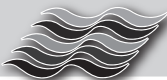
Alamat : Ketua Pengarah  
Jabatan Pengairan dan Saliran Malaysia  
Jalan Sultan Salahuddin  
50626 Kuala Lumpur  
Malaysia  
Telefon: 03 -2616 1501 (Waktu Pejabat)  
Faks : 03 - 2697 2411 (Waktu Pejabat)  
E-mel : kp@water.gov.my

**(b) Ketua Pegawai Maklumat (CIO)**

Alamat : Pengarah Kanan  
Jabatan Pengairan dan Saliran Malaysia  
Jalan Sultan Salahuddin  
50626 Kuala Lumpur  
Malaysia  
Telefon: 03 -2616 1504 (Waktu Pejabat)  
Faks : 03 - 2697 2484 (Waktu Pejabat)  
E-mel : pk@water.gov.my

**(c) Pegawai Keselamatan ICT (ICTSO)**

Alamat : Pengarah Pengurusan Maklumat  
Jabatan Pengairan dan Saliran Malaysia  
Jalan Sultan Salahuddin  
50626 Kuala Lumpur  
Malaysia  
Telefon: 03 - 2616 1518 (Waktu Pejabat)  
Faks : 03 - 2697 2600 (Waktu Pejabat)  
E-mel : ppm@water.gov.my

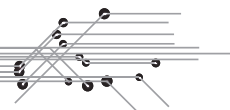


(d) ***Government Computer Emergency Response Team (GCERT)***

Alamat : Unit Pemodenan Tadbiran dan Perancangan  
Pengurusan Malaysia, (MAMPU)  
Jabatan Perdana Menteri  
Aras 5, Blok B1  
Kompleks Jabatan Perdana Menteri  
Pusat Pentadbiran Kerajaan Persekutuan  
62502 Putrajaya  
Malaysia  
Telefon: 03 - 8872 5138 (Waktu Pejabat)  
Faks : 03 - 8890 4253 (Waktu Pejabat)  
E-mel : [gcert@mampu.gov.my](mailto:gcert@mampu.gov.my)  
Web : <http://gcert.mampu.gov.my>

(e) ***NRE Computer Emergency Response Team (NRE Cert)***

Alamat : Kementerian Sumber Asli dan Alam Sekitar  
Bahagian Pengurusan Maklumat  
Aras 4 & 5, Wisma Sumber Asli  
No 25, Persiaran Perdana, Presint 4  
Pusat Pentadbiran Kerajaan Persekutuan  
62574 Putrajaya  
Malaysia  
Telefon: 03 - 8886 1041 (Waktu Pejabat)  
Faks : 03 - 8889 4821 (Waktu Pejabat)  
SMS : NRE ADUAN [Aduan Anda] dan hantar ke 15888  
E-mel : [jksec\\_cert@nre.gov.my](mailto:jksec_cert@nre.gov.my)  
Web : <http://www.nre.gov.my>



## 10. PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

### Objektif:

Menjamin operasi perkhidmatan dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

### 10.1 Kesenambungan Perkhidmatan

Ketua Jabatan atau Ketua Bahagian bertanggungjawab memastikan perkhidmatan tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

### 10.2 Pelan Kesenambungan Perkhidmatan

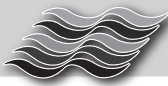
Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk mengekalkan kesinambungan perkhidmatan bagi memastikan tiada gangguan di dalam penyediaan perkhidmatan agensi. Pelan ini mestilah diperakui oleh pengurusan JPS dan perkara-perkara berikut perlu diberi perhatian:

- (a) Mengenal pasti dan mendokumenkan semua tanggungjawab dan prosedur kecemasan atau pemulihan;
- (b) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
- (c) Mengadakan program kesedaran dan latihan kepada pengguna mengenai prosedur kecemasan;
- (d) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali;
- (e) Membuat *backup*.

### 10.3 Perubahan atau Pengecualian *Business Continuity Plan* (BCP)

- (a) Jika pengecualian / pertukaran / kemas kini BCP diperlukan, permintaan secara bertulis termasuk keterangan dan kebenaran untuk pengecualian / perubahan hendaklah dikemukakan kepada Ketua Jabatan atau Ketua Bahagian;





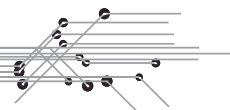
- (b) Salinan pelan kesinambungan perkhidmatan mestilah disimpan di lokasi berasingan bagi mengelakkan kerosakan akibat bencana di lokasi utama. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan;
- (c) Ujian pelan kesinambungan perkhidmatan hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan; dan
- (d) JPS hendaklah memastikan salinan pelan kesinambungan perkhidmatan sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

#### **10.4 Program Latihan dan Kesedaran Terhadap BCP**

Semua kakitangan JPS perlu mempunyai kesedaran dan mengetahui peranan masing-masing terhadap BCP. Ketua Jabatan atau Ketua Bahagian bertanggung jawab dalam memastikan latihan dan program kesedaran terhadap BCP dilaksanakan setiap tahun.

#### **10.5 Pengujian BCP**

*Disaster Recovery Plan* (DRP) perlu diuji satu (1) kali setahun (atau selepas perubahan utama, atau yang mana terdahulu) bagi memastikan kakitangan JPS mengetahui bagaimana ianya dilaksanakan. Komponen BCP yang lain perlu diuji sekali setahun atau selepas perubahan utama, atau yang mana terdahulu.



## 11. PEMATUHAN

Objektif:

Untuk menghindar pelanggaran undang-undang jenayah dan sivil, *statutory*, peraturan atau ikatan kontrak dan sebarang keperluan keselamatan lain.

### 11.1 Pematuhan Dasar

Adalah menjadi tanggungjawab Ketua Jabatan untuk memastikan bahawa pematuhan dan sebarang pelanggaran dielakkan.

Langkah-langkah perlu bagi mengelakkan sebarang pelanggaran perundangan termasuklah memastikan setiap pengguna membaca, memahami dan mematuhi Dasar Keselamatan ICT JPS dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.

### 11.2 Keperluan Perundangan

Senarai perundangan dan peraturan yang berkuat kuasa dari semasa ke semasa perlu dipatuhi oleh semua pengguna di JPS adalah seperti di **LAMPIRAN B**.

### 11.3 Perlindungan dan Privasi Data Peribadi

Pegawai JPS perlu sedar bahawa data kegunaan peribadi yang dijana dalam aset ICT adalah milik JPS. Pihak pengurusan tidak menjamin kerahsiaan data peribadi yang disimpan dalam aset ICT.

Untuk tujuan keselamatan dan penyelenggaraan rangkaian, pegawai yang diberi kuasa perlu mengawasi peralatan, sistem dan rangkaian. Pihak pengurusan JPS berhak mengaudit rangkaian dan sistem secara berkala bagi memastikan ia mematuhi dasar ini.

JPS menggalakkan dasar privasi yang adil. Pihak pengurusan perlu bertanggungjawab bagi memastikan semua maklumat peribadi digunakan berdasarkan keperluan untuk mengelakkan penyalahgunaan maklumat.

Pendedahan maklumat peribadi tentang pegawai JPS kepada pihak ketiga tidak sepatutnya berlaku kecuali:



- (a) Dikehendaki oleh undang-undang atau peraturan;
- (b) Dengan persetujuan yang jelas dan nyata daripada pegawai tersebut; atau
- (c) Setelah menerima persetujuan bertulis daripada pihak ketiga di mana maklumat akan dilindungi dengan tahap keselamatan dan privasi yang mencukupi seperti yang ditentukan oleh Pegawai Undang-undang serta perjanjian jelas diperoleh daripada pengurusan sumber manusia.

#### **11.4 Semakan Keselamatan Maklumat**

Semakan keselamatan maklumat mestilah diambil kira seperti berikut:

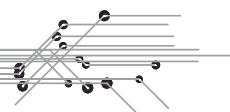
- (a) Pematuhan pemeriksaan ke atas dasar keselamatan maklumat, piawaian dan prosedur perlu dilakukan secara tahunan. Pemeriksaan ini mestilah melibatkan usaha bagi menentukan kawalan yang mencukupi dan dipatuhi;
- (b) Ujian penembusan bagi sistem yang kritikal mestilah dilaksanakan sekurang-kurangnya setahun sekali atau bila ada keperluan. Tujuan ujian penembusan ini adalah untuk memastikan pematuhan terhadap piawaian keselamatan ICT; dan
- (c) Perkara (a) dan (b) di atas mestilah dilaksanakan oleh pihak yang tidak terlibat dalam pelaksanaan aktiviti keselamatan ICT tersebut.

#### **11.5 Pelanggaran Perundangan**

Mengambil tindakan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuai, kelalaian dan pelanggaran keselamatan termasuk dasar keselamatan ICT yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972. Antara tindakan yang boleh diambil terhadap pihak ketiga adalah penamatan kontrak.

#### **11.6 Surat Akuan Pematuhan Dasar Keselamatan ICT**

Adalah menjadi tanggungjawab Ketua Jabatan dan Ketua Bahagian untuk memastikan setiap pegawai di dalam JPS menandatangani Surat Akuan Pematuhan Dasar Keselamatan Teknologi Maklumat dan Komunikasi (DKICT) seperti di **LAMPIRAN A**.



## PENGHARGAAN

Puan Norizan Binti Harun

Tuan Haji Mohd Shah Bin Rahman

Cik Rosminah binti Ahmad

Encik Muhammad Arif Bin Amir

Puan Nor Fazlinda Binti Mohd Puad

Cik Siti Sarah Binti Mohd Ismail

Puan Hanisah Binti Taib

Cik Norazlina Binti Osman

Puan Maziana Binti Mustafa



**SURAT AKUAN PEMATUHAN  
DASAR KESELAMATAN TEKNOLOGI MAKLUMAT  
DAN KOMUNIKASI (DKICT)  
JABATAN PENGAIRAN DAN SALIRAN MALAYSIA (JPS)**



Nama (Huruf Besar) : .....  
 No. Kad Pengenalan : .....  
 Jawatan : .....  
 Bahagian : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

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

Tandatangan : .....

Tarikh : .....

**Pengesahan**

.....  
 ( )  
 Pengarah Bahagian  
 Jabatan Pengairan dan Saliran Malaysia

Tarikh : .....

## SENARAI PERUNDANGAN DAN PERATURAN

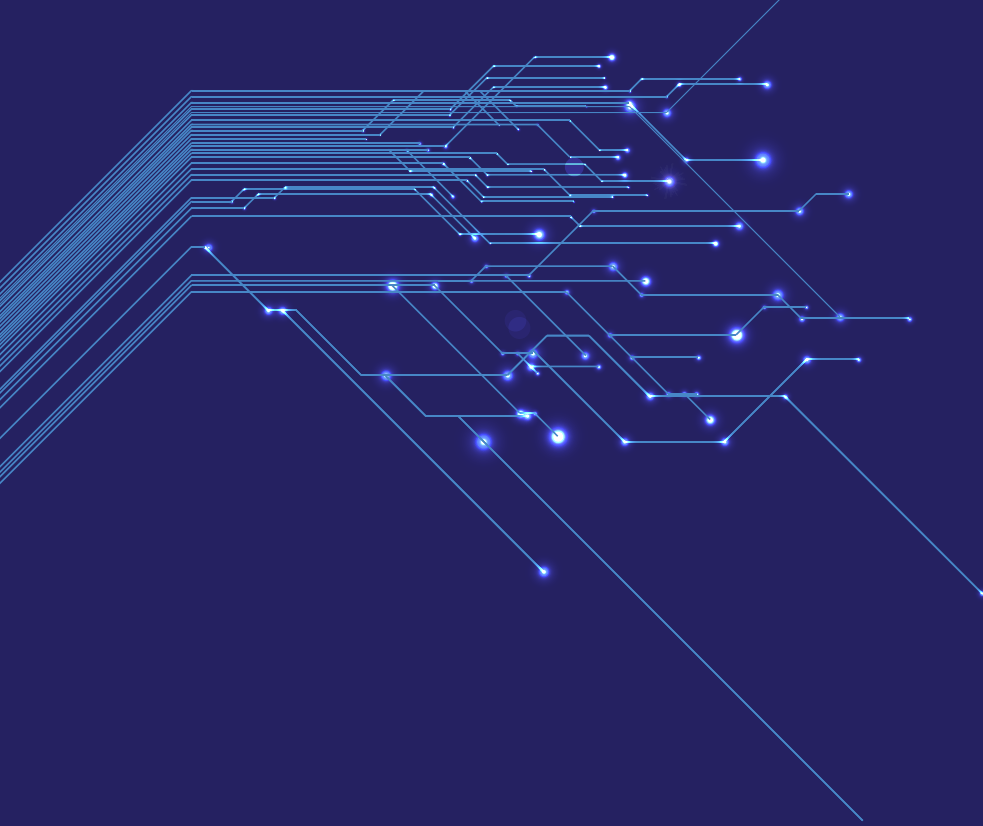
1. Arahan Keselamatan;
2. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
3. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
4. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
5. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
6. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
7. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
8. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
9. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
10. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
11. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
12. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
13. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;

14. Akta Tandatangan Digital 1997;
15. Akta Rahsia Rasmi 1972;
16. Akta Jenayah Komputer 1997;
17. Akta Hak Cipta (Pindaan) Tahun 1997;
18. Akta Komunikasi dan Multimedia 1998;
19. Perintah-Perintah Am;
20. Arahan Perbendaharaan;
21. Arahan Teknologi Maklumat 2007;
22. Garis Panduan Keselamatan MAMPU 2004;
23. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
24. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesenambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.









**Bahagian Pengurusan Maklumat  
Jabatan Pengairan dan Saliran Malaysia  
Jalan Sultan Salahuddin  
50626 Kuala Lumpur**

**Telefon : 03 - 2616 1400 / 1500 (*General Line*)  
Faks : 03 - 2697 2600  
<http://www.water.gov.my>**