

**Jabatan Akauntan Negara Malaysia**

**Prosedur Keselamatan Komunikasi dan Teknologi Maklumat  
(ICT)**

**Versi 1.0 / 2010**

## KANDUNGAN

<b>PERKARA</b>	<b>MUKA SURAT</b>
GLOSARI .....	vi
OBJEKTIF .....	1
SASARAN .....	1
<b>BAB 01: PENGURUSAN KESELAMATAN ICT .....</b>	<b>3</b>
1.1 Struktur Fungsi Organisasi Pengurusan Keselamatan ICT JANM ..	3
1.2 Pentadbir Sistem ICT .....	3
1.2.1 Pentadbir Perkakasan/Perisian ICT dan Pusat Data ( Data Centre)	3
1.2.2 Pentadbir E-mel dan Laman Web/Portal.....	5
1.2.3 Pentadbir Rangkaian.....	6
1.2.4 Pentadbir Perkakasan Keselamatan ICT .....	7
1.2.5 Pentadbir Sistem.....	8
1.3 GCERT Jabatan.....	9
<b>BAB 02: PROSEDUR PENGENDALIAN INSIDEN.....</b>	<b>11</b>
2.1 Pengurusan Pengendalian Insiden Keselamatan ICT.....	11
2.1.1 Mekanisme Pelaporan Insiden.....	11
2.1.2 Prosedur Pengurusan Insiden.....	12
<b>BAB 03: PROSEDUR KESELAMATAN SUMBER MANUSIA .....</b>	<b>14</b>
3.1 Kakitangan JANM .....	14
3.2 Pihak Ketiga.....	15
<b>BAB 04: PROSEDUR KESELAMATAN DATA DAN MAKLUMAT .....</b>	<b>17</b>
4.1 Pengelasan Data dan Maklumat .....	17
4.1.1 Aktiviti Pengelasan Data dan Maklumat.....	17
4.2 Pengendalian Data dan Maklumat.....	17
4.3 Keselamatan Dokumentasi .....	18
<b>BAB 05: PROSEDUR KESELAMATAN FIZIKAL DAN PERSEKITARAN. 20</b>	
5.1 Keselamatan Kawasan .....	20
5.1.1 Kawalan Kawasan.....	20
5.1.2 Kawalan Masuk Fizikal.....	21

5.1.3	Kawasan Larangan .....	21
5.2	Keselamatan Kawalan Persekitaran .....	21
5.2.1	Keselamatan Data Centre .....	22
<b>BAB 06:</b>	<b>PROSEDUR KESELAMATAN PERKAKASAN .....</b>	<b>25</b>
6.1	Keselamatan Perkakasan .....	25
6.1.1	Server .....	25
6.1.2	Media Storan.....	25
6.1.3	Media Tandatangan Digital .....	26
6.1.4	Media Perisian Dan Aplikasi .....	27
6.1.5	Komputer Dan Notebook.....	27
6.2	Pengagihan Perkakasan .....	28
6.3	Perlupusan Perkakasan .....	31
<b>BAB 07:</b>	<b>PROSEDUR KESELAMATAN PERISIAN .....</b>	<b>34</b>
7.1	Pengendalian Dokumen Perisian .....	34
7.2	Prosedur Pemasangan Perisian.....	34
7.3	Perlindungan Daripada Perisian Berbahaya/Tidak Sah .....	34
7.4	Penyelenggaraan Perisian .....	35
<b>BAB 08:</b>	<b>PROSEDUR KESELAMATAN OPERASI DAN KOMUNIKASI....</b>	<b>37</b>
8.1	Pengendalian Dokumen Prosedur .....	37
8.2	Backup dan Restore.....	37
8.3	Keselamatan Media .....	38
8.4	Keselamatan E-mel.....	38
8.4.1	Kategori E-mel .....	38
8.4.2	Pemakaian Dan Penggunaan E-mel Yang Betul.....	39
8.4.3	Peraturan Menggunakan E-mel .....	40
8.4.4	Penyelenggaraan E-mel.....	41
8.4.5	Tanggungjawab Pengguna E-mel.....	41
8.5	Pemantauan.....	42
8.5.1	Pengauditan dan Forensik ICT .....	42
8.5.2	Jejak Audit .....	43
8.5.3	Sistem Log .....	43

8.5.4	Pemantauan Log.....	44
<b>BAB 09</b>	<b>PROSEDUR KESELAMATAN RANGKAIAN.....</b>	<b>46</b>
9.1	Keselamatan Rangkaian.....	46
9.1.1	Infrastruktur Rangkaian.....	46
9.1.2	Pelaporan Kerosakan.....	47
<b>BAB 10</b>	<b>PROSEDUR KESELAMATAN KAWALAN CAPAIAN.....</b>	<b>49</b>
10.1	Kawalan Capaian Pengguna.....	49
10.1.1	Akaun Pengguna.....	49
10.1.2	Keselamatan Kata Laluan.....	50
10.1.3	Keselamatan Penggunaan Kad Pintar.....	51
10.2	Kawalan Capaian Rangkaian.....	52
10.2.1	Keselamatan Capaian Rangkaian.....	52
10.2.2	Keselamatan Capaian Internet.....	52
10.3	Kawalan Capaian Sistem Pengoperasian.....	53
10.4	Kawalan Capaian Aplikasi dan Maklumat.....	54
10.5	Prosedur Kawalan Capaian Perbankan Internet (Online Banking).....	54
<b>BAB 11</b>	<b>PROSEDUR PEROLEHAN, PEMBANGUNAN DAN</b>	
	<b>PENYELENGGARAAN SISTEM.....</b>	<b>57</b>
11.1	Keselamatan Dalam Membangunkan Sistem Dan Aplikasi.....	57
11.1.1	Keperluan Keselamatan Sistem Maklumat.....	57
11.1.2	Pengesahan Data Input Dan Output.....	57
11.2	Kawalan Kriptografi.....	58
11.2.1	Enkripsi.....	58
11.3	Keselamatan Fail Sistem.....	58
11.3.1	Kawalan Fail Sistem.....	58
11.4	Keselamatan Dalam Proses Pembangunan Dan Sokongan.....	58
11.4.1	Prosedur Kawalan Perubahan.....	58
11.4.2	Pembangunan Perisian Secara Outsource.....	59
11.5	Kawalan Teknikal Keterdedahan (Vulnerability).....	59
11.5.1	Kawalan dari Ancaman Teknikal.....	59

<b>BAB 12: PROSEDUR</b>	<b>PENGURUSAN</b>	<b>KESINAMBUNGAN</b>	
<b>PERKHIDMATAN</b>			<b>61</b>
Lampiran A: Struktur Organisasi Pengurusan Keselamatan ICT JANM			62
Lampiran B: Surat Akuan Pematuhan			63
Lampiran C: Proses Kerja Pelaporan Insiden Rujukan MAMPU			64
Lampiran D: Contoh Format E-Mel Bukan Rahsia Rasmi			68
Lampiran E: Contoh Format E-Mel Rahsia Rasmi			69
Lampiran F: Amalan Baik Keselamatan Kata Laluan			70
<b>RUJUKAN</b>			<b>71</b>

## GLOSARI

Aset ICT	Data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang berada di bawah tanggungjawab JANM.
CIO	Chief Information Officer. Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi;
Dokumen	Semua himpunan atau kumpulan bahan atau dokumen yang disimpan dalam bentuk media cetak, salinan lembut ( <i>soft copy</i> ), elektronik, dalam talian, kertas lutsinar, risalah atau slaid.
E-mel	Mel elektronik atau e-mel adalah merupakan aplikasi yang membolehkan pengguna berkomunikasi antara satu sama lain dalam bentuk mesej elektronik. Aplikasi e-mel ini digunakan secara meluas dan membenarkan komunikasi lebih daripada dua hala dengan cara yang pantas dan lebih sesuai untuk penulisan yang ringkas
GCERT	Government Computer Emergency Response Team. GCERT di MAMPU bertanggungjawab menangani semua laporan insiden keselamatan ICT yang melibatkan sektor awam.
ICTSO	ICT Security Officer. Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.

Insiden Keselamatan	Musibah ( <i>adverse event</i> ) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Kad Pintar	Kad pintar bermaksud kad yang mempunyai cip mikro yang menjadikannya seperti komputer mikro. Cip mikro ini menyimpan maklumat pengenalan pemilik kad tersebut.
Kata laluan	Kata laluan merupakan kata kunci atau nombor PIN untuk membolehkan pengguna memasuki atau menggunakan infrastruktur ICT sama ada perkakasan, sistem atau aplikasi.
Media storan	Perkakasan yang berkaitan dengan penyimpanan data dan maklumat seperti disket, kartrij, cakera padat, cakera mudah alih, pita, cakera keras dan pemacu pena.
Modem	Modem / NTU ( <i>Network Termination Unit</i> ) adalah merupakan peralatan yang digunakan untuk mengirim dan menerima data komputer melalui talian komunikasi
Pentadbir Sistem ICT	Pegawai-pegawai yang dipertanggungjawabkan dalam melaksanakan tugas-tugas pentadbiran sistem ICT di Bahagian-bahagian JANM, Negeri/Cawangan dan JMS
Perisian Sistem	Pemrograman pelbagai ( <i>Multi-tasking</i> ) iaitu keupayaan satu-satu komputer melaksanakan arahan-arahan ,dari beberapa program/ aplikasi secara serentak pada satu masa. Selain itu, pemprosesan pelbagai melibatkan penyambungan beberapa unit pemprosesan pusat bagi tujuan operasi pemprosesan data.

Perisian Aplikasi	Program-program yang direkabentuk khas untuk komputer bagi melaksanakan sesuatu tugas, masalah, ataupun kerja-kerja automasi bagi memenuhi keperluan pengguna
Peralatan perlindungan	Peralatan yang berfungsi untuk pengawalan, pencegahan dan pengurusan tampalan ( <i>patches</i> ) seperti <i>firewall</i> , <i>router</i> , <i>proxy</i> , antivirus, dan lain-lain.
<i>Router</i>	<i>Router</i> adalah peralatan yang digunakan untuk mengirim dan menerima data komputer melalui talian komunikasi seperti bagi talian komunikasi <i>EG*Net</i> dan <i>Leased Line</i> ;
<i>Switch</i>	<i>Switch</i> merupakan peralatan yang digunakan untuk menyambung peralatan komputer bagi membolehkannya berhubung di antara satu sama lain yang dikenali dengan nama rangkaian kawasan setempat ( <i>Local Area Network</i> );
Virus	Atur cara yang bertujuan merosakkan data dan sistem aplikasi;

## **PENDAHULUAN**

Penggunaan ICT dalam tugas harian di JANM semakin meningkat setelah pelaksanaan aplikasi penting GFMAS, eSPKB dan lain-lain lagi. Untuk memastikan maklumat-maklumat penting JANM bebas daripada sebarang ancaman, pengguna dinasihatkan untuk mematuhi prosedur keselamatan ICT yang telah ditetapkan. Pengguna adalah tertakluk kepada garis panduan yang telah dikeluarkan oleh MAMPU dan undang-undang lain yang berkaitan. Keselamatan ICT adalah merangkumi semua data, peralatan, perisian, rangkaian dan kemudahan ICT yang lain seperti dinyatakan dalam Pekeliling Am Bil. 3 Tahun 2000 dan Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003

## **OBJEKTIF**

Prosedur Keselamatan ICT JANM ini adalah sebagai panduan untuk menjamin keselamatan infrastruktur ICT dan maklumat penting JANM. Garis panduan dalam prosedur tersebut akan membolehkan pengguna mengetahui dengan jelas peraturan dan juga batasan apabila menggunakan peralatan dan perisian ICT semasa menjalankan tugas.

## **SASARAN**

Dokumen ini disasarkan kepada setiap anggota JANM, pegawai yang bertugas di pejabat perakaunan, pembekal, pakar runding dan penjawat awam yang menggunakan sistem JANM serta pihak-pihak lain yang terlibat.

# **BAB 01: PENGURUSAN KESELAMATAN ICT**

## **BAB 01: PENGURUSAN KESELAMATAN ICT**

Bab 01 ini secara keseluruhannya adalah merujuk kepada Bahagian 2.0 di dalam Dokumen Polisi Keselamatan ICT Versi 1.0/2008.

### **1.1 Struktur Fungsi Organisasi Pengurusan Keselamatan ICT JANM**

Struktur formal Organisasi Pengurusan Keselamatan ICT JANM seperti di Lampiran A diwujudkan untuk mengurus segala aspek keselamatan ICT Jabatan. Penekanan yang diberikan di dalam Bab 01 ini adalah tanggungjawab dan tatacara pentadbiran setiap pentadbir sistem ICT. Pentadbir sistem ICT terdiri daripada Pentadbir Perkakasan/Perisian ICT Dan Pusat Data (*Data Centre*), Pentadbir E-mel dan Laman Web/Portal, Pentadbir Rangkaian, Pentadbir Perkakasan Keselamatan ICT dan Pentadbir Sistem.

### **1.2 Pentadbir Sistem ICT**

#### **1.2.1 Pentadbir Perkakasan/Perisian ICT dan Pusat Data ( *Data Centre* )**

##### **(i) Pentadbir Perkakasan/Perisian ICT**

Kakitangan JANM yang dilantik sebagai pentadbir perkakasan dan perisian perlu mematuhi perkara-perkara seperti berikut:

- a) Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan;
- b) Semua perkakasan hanya boleh diselenggarakan secara berjadual oleh pentadbir perkakasan dan perisian atau kontraktor bertauliah yang dibenarkan sahaja;
- c) Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan;
- d) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT Jabatan/Pengurus ICT setiap cawangan berkenaan;

- e) Semua aktiviti penyelenggaraan perlu direkodkan di dalam borang hartamodal yang diuruskan oleh Pentadbir Aset Bahagian/Jabatan;
- f) Sebarang peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pentadbir perkakasan/perisian dan tertakluk kepada tujuan yang dibenarkan;
- g) Sebarang aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan;
- h) Semua perisian dan aplikasi hendaklah di *upgrade* dari semasa ke semasa bagi memastikan versi yang sesuai digunapakai; dan
- i) Semua perolehan perkakasan/perisian/aplikasi hendaklah mengikut prosedur Tatacara Perolehan ICT (Surat Pekeliling Am Bil. 2 Tahun 2009).

## **(ii) Pentadbir *Data Centre***

Kakitangan JANM yang dilantik sebagai pentadbir *data centre* perlu mematuhi perkara-perkara berikut bagi memastikan pengoperasian *data centre* berjalan dengan lancar:

- a) Memastikan semua peralatan perlu berada dalam keadaan baik dan sentiasa boleh guna, selamat dari segi logikal dan fizikal serta mempunyai ruang yang mencukupi untuk menempatkan peralatan, perkakasan dan kabel;
- b) Memastikan semua permohonan penempatan, peralihan dan pengeluaran sebarang peralatan dalam *data centre* perlu mendapat kelulusan pentadbir *data centre*. Pentadbir *data centre* perlu sentiasa mengemaskini *layout* yang baru dan didokumentasikan;
- c) Memantau dan memastikan bahawa pegawai-pegawai lain, vendor, kakitangan syarikat atau kontraktor perlu mendapatkan kebenaran daripada pentadbir *data centre* dan dikehendaki merekod maklumat ke dalam Log Keluar/Masuk *Data Centre*;
- d) Memastikan Log Keluar / Masuk di *Data Centre* diselenggara oleh pentadbir *data centre*;
- e) Melaporkan sebarang kerosakan pada peralatan di dalam *Data Centre* kepada Meja Bantuan (*helpdesk*);

- f) Pentadbir *data centre* atau wakilnya hendaklah sentiasa berada di *Data Centre* semasa kerja pemasangan atau penyenggaraan yang dilakukan oleh kontraktor, kakitangan syarikat atau vendor;
- g) Memastikan *Data Centre* perlu disenggarakan mengikut jadual yang telah ditetapkan; dan
- h) Menyemak dan menguji semua peralatan sokongan bekalan kuasa (*UPS* dan *Gen-set*) sekurang-kurangnya setahun sekali.

### **1.2.2 Pentadbir E-mel dan Laman Web/Portal**

#### **(i) Pentadbir *Emel***

Bagi memastikan pengendalian e-mel JANM beroperasi dengan sempurna dan berkesan, pentadbir e-mel JANM adalah bertanggungjawab:

- a) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Ketua Seksyen/Ketua Unit;
- b) Pegawai pentadbir e-mel setiap bahagian/pejabat perakaunan bertanggungjawab memaklumkan dengan segera kepada Pentadbir e-mel Jabatan mana-mana pegawai yang tamat perkhidmatan atau bertukar ke Bahagian/ Jabatan;
- c) Menamatkan akaun dengan segera (pengguna yang berhenti, bertukar dan melanggar dasar atau tatacara JANM) atas tujuan keselamatan maklumat menggunakan Borang Penutupan Akaun E-mel;
- d) Menamatkan akaun e-mel yang tidak aktif selama tiga bulan berturut-turut kecuali bagi kakitangan yang menyambung pelajaran (*disactive*);
- e) Menjalankan pemantauan dan penapisan kandungan fail elektronik dan e-mel secara berkala jika difikirkan perlu tanpa terlebih dahulu merujuk kepada pengguna;
- f) Memantau log dan backup e-mel secara berkala bagi memastikan sistem keluar/masuk e-mel berjalan lancar;

- g) Melaksanakan jadual penstoran dan pengarkiban e-mel JANM. Penyimpanan media storan sama ada di luar atau di dalam kawasan mestilah mempunyai ciri-ciri keselamatan fizikal yang terjamin;
- h) Melaksanakan penyelenggaraan ke atas sistem e-mel dengan baik dan menentukan segala patches terkini yang disediakan oleh pihak pembekal perisian dipasang dan berfungsi dengan sempurna; dan
- i) Memaklumkan kepada Ketua Jabatan sekiranya mengalami insiden keselamatan seterusnya pentadbir e-mel perlu mengurus dan menangani insiden yang berlaku dengan segera serta sistematik sehingga keadaan kembali pulih.

#### **(ii) Pentadbir Laman Web/Portal**

Perkara-perkara berikut perlu dipatuhi oleh pentadbir laman web/portal bagi memastikan kelancaran capaian laman web JANM:

- a) Menyelia dan menyelaras laman web/portal di JANM dengan merujuk kepada Pekeliling Am Bil.1 Tahun 2006 - Pengurusan Laman Web/Portal Sektor Awam;

#### **1.2.3 Pentadbir Rangkaian**

Bagi memastikan pengendalian rangkaian JANM beroperasi dengan sempurna dan berkesan, pentadbir rangkaian JANM adalah bertanggungjawab untuk mematuhi perkara-perkara seperti berikut:

- a) Memastikan perhubungan rangkaian GFMS antara Ibu Pejabat dengan rangkaian GFMS di Cawangan dan Pejabat Mengakaun Sendiri (SAD) sentiasa beroperasi dengan baik;
- b) Memberikan khidmat nasihat dalam hal ehwal berkaitan infrastruktur rangkaian di Ibu Pejabat dan 36 Pejabat Perakaunan;
- c) Memastikan semua peralatan rangkaian seperti *VLAN, ATM Switch, DMZ Zone, server farm, port* dan trafik rangkaian berfungsi dengan baik;

- d) Memastikan semua peralatan rangkaian ditempatkan di rak yang selamat dan berkunci;
- e) Memastikan tiada sebarang pemasangan *wireless/broadband* di rangkaian JANM kecuali dengan kebenaran;
- f) Memastikan pengagihan alamat IP adalah secara DHCP kecuali dengan kebenaran.
- g) Mengenalpasti dan menyenggara kerosakan teknikal bagi semua peralatan teknikal rangkaian; dan
- h) Melaporkan sebarang masalah rangkaian kepada pihak yang bertanggungjawab.

#### **1.2.4 Pentadbir Perkakasan Keselamatan ICT**

Kakitangan JANM yang dilantik sebagai pentadbir keselamatan ICT perlu mematuhi perkara –perkara berikut:

##### **(i) Pengendalian *Firewall***

Perkara-perkara seperti berikut hendaklah dipatuhi :

- a) Memastikan semua trafik keluar dan masuk ke *server farm* / VLAN *user* hendaklah melalui *firewall*;
- b) Memastikan permohonan membuka sebarang *service* dan *port* di *firewall* hendaklah dengan mengisi borang yang disediakan;
- c) Memastikan hanya Pentadbir Keselamatan ICT JANM Ibu Pejabat sahaja dibenarkan untuk mencapai dan melaksanakan perubahan ke atas polisi di semua *firewall* GFMAS (Cawangan dan Pejabat Mengakaun Sendiri); dan
- d) Melaksanakan pemantauan ke atas log *firewall* perlu dibuat secara berterusan.

##### **(ii) Pengendalian *Intrusion Prevention System (IPS)* / *Intrusion Detection System (IDS)***

Perkara-perkara seperti berikut hendaklah dipatuhi :

- a) Melaksanakan pemantauan *log traffic* di *IPS / IDS* Ibu Pejabat , Cawangan dan Pejabat Mengakaun Sendiri (SAD);
- b) Melakukan aktiviti pencegahan di *IPS / IDS* dan melaporkan kepada TP(SPICT) sekiranya berlaku aktiviti yang mencurigakan; dan
- c) Melakukan tindakan keselamatan ICT yang di cadangkan oleh PRISMA, MAMPU berdasarkan penemuan daripada *IDS* PRISMA, MAMPU.

### (iii) Pemantauan Perisian Antivirus

Perkara-perkara seperti berikut hendaklah dipatuhi :

- a) Memastikan ke semua komputer dan server di Ibu Pejabat dan Pejabat Perakaunan mempunyai perisian antivirus yang berdaftar dan sah;
- b) Memastikan *pattern* antivirus yang digunakan pada setiap komputer dan server sentiasa mendapat *update* terkini daripada server antivirus;
- c) Memantau *console management antivirus* secara berkala seterusnya menyimpan laporan berkenaan *virus attack* melalui fail log antivirus tersebut;
- d) Memutuskan sambungan rangkaian komputer telah sah dijangkiti virus sementara waktu bagi mengelakkan penyebaran virus pada komputer lain melalui talian rangkaian JANM;
- e) Melaporkan kepada pihak ketiga dengan segera sekiranya terdapat serangan virus yang luar biasa dan tidak boleh di *clean up* menggunakan versi antivirus sedia ada; dan
- f) Mendapatkan maklumat terkini mengenai maklumat dan virus terbaru melalui laman web antivirus yang digunakan di JANM.

### 1.2.5 Pentadbir Sistem

Kakitangan JANM yang dilantik sebagai pentadbir sistem perlu mematuhi perkara – perkara berikut bagi memastikan pengoperasian semua sistem di JANM berjalan dengan lancar:

- a) Mengambil tindakan dengan segera apabila dimaklumkan mengenai kakitangan JANM yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;
- b) Memantau aktiviti capaian harian sistem aplikasi pengguna;
- c) Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dengan membatalkan atau memberhentikannya dengan serta merta;
- d) Menganalisis dan menyimpan rekod jejak audit dalam tempoh yang ditetapkan serta menyediakan laporan jika perlu ; dan
- e) Menyediakan laporan mengenai aktiviti capaian secara berkala.

### **1.3 GCERT Jabatan**

Secara amnya tugas GCERT jabatan adalah seperti berikut

- a) Menerima dan mengambil tindakan susulan ke atas insiden keselamatan yang dilaporkan;
- b) Menyebarkan maklumat bagi membantu pengukuhan keselamatan ICT JANM dari semasa ke semasa;
- c) Menyediakan khidmat nasihat kepada JANM dalam mengesan, mengenalpasti dan menangani sesuatu insiden keselamatan ICT; dan
- d) Menjadi penyelaras dengan pihak-pihak yang terlibat seperti GCERT MOF dan MAMPU.

## **BAB 02: PROSEDUR PENGENDALIAN INSIDEN**

## **BAB 02: PROSEDUR PENGENDALIAN INSIDEN**

Bab 02 ini secara keseluruhannya adalah merujuk kepada Bahagian 3.0 di dalam Dokumen Polisi Keselamatan ICT Versi 1.0/2008.

### **2.1 Pengurusan Pengendalian Insiden Keselamatan ICT**

Tanggungjawab Pengurus ICT dalam pengendalian insiden keselamatan ICT adalah seperti berikut:

- a) Pengurus ICT adalah bertanggungjawab untuk memastikan arahan pengurusan pengendalian insiden keselamatan ICT di bawah kawalan masing-masing dipatuhi; dan
- b) Pengurus ICT dan setiap pegawai serta kakitangan yang terlibat hendaklah memastikan bahan-bahan bukti berkaitan insiden keselamatan ICT dapat disediakan, disimpan, disenggarakan dan mempunyai perlindungan keselamatan. Penyediaan bahan-bahan bukti seperti jejak audit, backup secara berkala, media *backup offline* ini hendaklah mengikut amalan terbaik yang disarankan oleh Kerajaan dari semasa ke semasa.

#### **2.1.1 Mekanisme Pelaporan Insiden**

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO, Wakil GCERT Jabatan dan GCERT MAMPU dengan kadar segera:

- a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;
- b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;
- c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;
- d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
- e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.

Prosedur pelaporan insiden keselamatan ICT berdasarkan:

- a) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan
- b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam. Carta bagi proses kerja pelaporan insiden adalah seperti di Lampiran C.

### **2.1.2 Prosedur Pengurusan Insiden**

Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:

- a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;
- b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;
- c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;
- d) Menyediakan tindakan pemulihan segera; dan
- e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

**BAB 03: PROSEDUR KESELAMATAN SUMBER  
MANUSIA**

### **BAB 03: PROSEDUR KESELAMATAN SUMBER MANUSIA**

Bab 03 – Bab 09 ini secara keseluruhannya adalah merujuk kepada Bahagian 4.0 di dalam Dokumen Polisi Keselamatan ICT Versi 1.0/2008.

#### **3.1 Kakitangan JANM**

##### **i. Mula Perkhidmatan**

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- a) Mematuhi dan memahami polisi dan prosedur keselamatan ICT, JANM;
- b) Mengisi dan menandatangani Surat Akuan Pematuhan Polisi Keseleamatan ICT, JANM seperti di Lampiran B sebelum memulakan tugas di JANM; dan
- c) Menjalani tapisan keselamatan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan
- d) Mematuhi semua terma dan syarat perkhidmatan awam yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian ditetapkan.

##### **ii. Dalam Perkhidmatan**

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- a) Menghadiri dan menjalani kursus mengenai keselamatan ICT yang dijalankan secara berkala bagi memantapkan pengetahuan serta kedah pengendalian aset ICT dengan kaedah yang betul; dan
- b) Tindakan disiplin dan/atau undang-undang yang boleh dikenakan sekiranya berlaku pelanggaran dengan perundangan serta peraturan ditetapkan oleh JANM.

##### **iii. Tamat atau Bertukar Perkhidmatan**

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- a) Mengembalikan semua aset ICT kepada JANM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan;
- b) Hendaklah memastikan kebenaran capaian sistem dan aplikasi serta kemudahan proses maklumat di batalkan mengikut peraturan yang ditetapkan oleh JANM

- dan/atau terma perkhidmatan; dan
- c) Memulangkan kembali pas keselamatan kepada JANM bagi menyekat sistem keluar/masuk Jabatan.

### **3.2 Pihak Ketiga**

#### **i. Mula Perkhidmatan**

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- a) Mematuhi dan memahami polisi dan prosedur keselamatan ICT, JANM;
- b) Mengisi dan menandatangani Surat Akuan Pematuhan Polisi Keselematan ICT, JANM sebelum memulakan tugas di JANM; dan
- c) Mengemukakan surat sokongan dari pihak yang terlibat sekiranya di lantik oleh JANM bagi menjalankan tugas di mana-mana Pejabat Perakaunan atau Jabatan Mengakauntan Sendiri.

#### **ii. Dalam Perkhidmatan**

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- a) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian ditetapkan; dan
- b) Tindakan disiplin dan/atau undang-undang yang boleh dikenakan sekiranya berlaku pelanggaran dengan perundangan serta peraturan ditetapkan oleh JANM.

#### **iii. Tamat Perkhidmatan**

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- d) Mengembalikan semua aset ICT ( jika ada) kepada JANM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan;
- e) Hendaklah memastikan kebenaran capaian sistem dan aplikasi serta kemudahan proses maklumat di batalkan mengikut peraturan yang ditetapkan oleh JANM dan/atau terma perkhidmatan; dan
- f) Memulangkan kembali pas keselamatan kepada JANM bagi menyekat sistem keluar/masuk Jabatan.

**BAB 04: PROSEDUR KESELAMATAN DATA  
DAN MAKLUMAT**

## **BAB 04: PROSEDUR KESELAMATAN DATA DAN MAKLUMAT**

### **4.1 Pengelasan Data dan Maklumat**

Data dan Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut Dokumen Arahan Keselamatan.

Setiap data dan maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut:

- a) Rahsia Besar;
- b) Rahsia;
- c) Sulit; dan
- d) Terhad.

#### **4.1.1 Aktiviti Pengelasan Data dan Maklumat**

Aktiviti bagi menentukan pengelasan data dan maklumat bagi para 4.1 perlu dilaksanakan oleh setiap bahagian yang berkenaan.

### **4.2 Pengendalian Data dan Maklumat**

Aktiviti pengendalian data/maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut:

- a) Menghalang pendedahan data/maklumat kepada pihak yang tidak dibenarkan;
- b) Melakukan penglabelan dan sistem fail ke atas maklumat terperingkat mengikut klasifikasi keselamatan seperti di dalam Dokumen Arahan Keselamatan;

- c) Memberi perhatian kepada maklumat terperingkat terutama semasa pengwujudan, pemprosesan, pengwujudan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;
- d) Memeriksa data/maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
- e) Melindungi media yang mengandungi data/maklumat dengan menggunakan *firewall* bagi mengelak daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari JANM;
- f) Mewujudkan perjanjian untuk pertukaran maklumat dan perisian di antara JANM dengan agensi luar;
- g) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; dan
- h) Menggunakan enkripsi ke atas data/maklumat terperingkat yang disediakan dan dihantar secara elektornik.

### **4.3 Keselamatan Dokumentasi**

Perkara-perkara yang perlu dipatuhi adalah:

- a) Setiap dokumen hendaklah difail dan dilabel mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;
- b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan;
- c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan;
- d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan
- e) Dokumentasi yang hilang hendaklah dilaporkan dengan segera kepada pegawai bertanggungjawab untuk tindakan selanjutnya.

**BAB 05: PROSEDUR KESELAMATAN FIZIKAL  
DAN PERSEKITARAN**

## **BAB 05: PROSEDUR KESELAMATAN FIZIKAL DAN PERSEKITARAN**

### **5.1 Keselamatan Kawasan**

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

#### **5.1.1 Kawalan Kawasan**

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;
- b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
- c) Memasang alat penggera atau kamera;
- d) Menghadkan jalan keluar masuk;
- e) Mengadakan kaunter kawalan;
- f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat;
- g) Mewujudkan perkhidmatan kawalan keselamatan;
- h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;
- i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;
- j) Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana;
- k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan

- l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.

### **5.1.2 Kawalan Masuk Fizikal**

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- a) Setiap kakitangan JANM hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;
- b) Semua pas keselamatan hendaklah diserahkan balik kepada JANM apabila kakitangan bertukar atau tamat perkhidmatan;
- c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama JANM. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan
- d) Kehilangan pas mestilah dilaporkan dengan segera.

### **5.1.3 Kawasan Larangan**

Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut.

- a) Kawasan larangan di JANM adalah bilik Akauntan Negara Malaysia, bilik Timbalan Akauntan Negara Malaysia, bilik Pengarah Bahagian, bilik Timbalan Pengarah Bahagian, stor komputer dan Bilik Operasi/Pusat Data (*Data Centre*).

## **5.2 Keselamatan Kawalan Persekitaran**

Perkara-perkara berikut hendaklah dipatuhi:

- a) Merancang dan menyediakan pelan keseluruhan susun atur *data centre* (bilik percetakan dan peralatan komputer) dengan teliti;
- b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;
- c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian,

- mudah dikenali dan dikendalikan;
- d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT;
  - e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT;
  - f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer;
  - g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan
  - h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.

### 5.2.1 Keselamatan *Data Centre*

Server utama JANM perlu diletakkan di dalam *Data Centre* bagi memastikan ia dapat dikawal secara berpusat dari segi keselamatan dan juga keperluan utiliti dan diwartakan sebagai kawasan larangan.

Perkara yang perlu dipatuhi termasuk yang berikut :

- a) *Data Centre* hanya boleh dimasuki atau digunakan oleh pegawai yang dipertanggungjawabkan sahaja;
  - Log Keluar / Masuk hendaklah ditempatkan di *Data Centre* dan diselenggara oleh pentadbir *data centre*.
- b) Memastikan semua pintu dan tingkap di *data centre* perlu dikunci setiap masa serta memantau media log keluar/masuk berfungsi dengan baik;
- c) *Data Centre* perlu dilengkapi dengan *Uninterruptible Power Supply (UPS)*, bekalan kuasa elektrik sekunder (*Generator-Set*), Voltage Stabilizer, sistem penghawa dingin dengan suhu di antara 19°C hingga 21°C dan kelembapan pada tahap 60% hingga 70%, sistem pencegahan kebakaran, sistem pengesan asap serta haba dan sistem keselamatan pintu utama; dan

- d) Mempunyai sistem pendawaian yang kemas, selamat dan mengikut spesifikasi yang dibenarkan.

**BAB 06: PROSEDUR KESELAMATAN  
PERKAKASAN**

## **BAB 06: PROSEDUR KESELAMATAN PERKAKASAN**

### **6.1 Keselamatan Perkakasan**

Setiap aset perlu dikenal pasti, dikelaskan, didokumenkan dan disenggarakan untuk memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT.

Berikut adalah senarai aset yang perlu dikendalikan mengikut aturan prosedur keselamatan ICT JANM:

#### **6.1.1 Server**

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Server hendaklah ditempatkan di dalam *Data Centre* dan dilindungi oleh *Firewall* dan peralatan perlindungan yang lain seperti *IPS*, *IDS* dan penyahvirus (antivirus);
- b) Server untuk capaian umum perlu ditempatkan dalam segmen *DMZ* manakala server lain ditempatkan di luar segmen *DMZ*;
- c) Semua server yang berada di luar segmen *DMZ* adalah tidak dibenarkan sama sekali untuk laluan capaian ke internet;
- d) Kemasukan sebarang server ke dalam *Data Centre* hendaklah dilakukan pengauditan terlebih dahulu oleh pentadbir *data centre*;
- e) Server *name* adalah mengikut *convention* yang ditetapkan iaitu <lokasi/nama aplikasi> contoh : HODEV, HODNAR1 atau <bahagian aplikasi> contoh : SPEKSDBASE
- f) Sebarang *patches* yang hendak dipasang pada server hendaklah diuji terlebih dahulu sebelum di *install* ke persekitaran *live server* ; dan
- g) Server perlu disenggarakan mengikut jadual yang telah ditetapkan.

#### **6.1.2 Media Storan**

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Aksesori tersebut adalah untuk kegunaan rasmi sahaja;
- b) Tidak dibenarkan meminjamkan kepada orang lain yang tidak berkenaan;
- c) Nyahvirus (virus scan) *thumb-drive*/disket terlebih dahulu untuk mengelakkan serangan virus;
- d) Untuk keselamatan jangan mencabut *thumb-drive* secara terus dari *USB port* kerana boleh menyebabkan kerosakan dan data *corrupted*;
- e) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
- f) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;
- g) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;
- h) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;
- i) Akses dan pergerakan media storan hendaklah direkodkan;
- j) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal;
- k) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data;
- l) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan
- m) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.

### **6.1.3 Media Tandatangan Digital**

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media dan tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;
- b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan

- c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.

#### 6.1.4 Media Perisian Dan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan kakitangan JANM;
- b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT;
- c) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada *CD-ROM, disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan
- d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.

#### 6.1.5 Komputer Dan Notebook

Pengguna hendaklah sentiasa mematuhi garis panduan berikut:

- a) Mempunyai kata laluan *login*;
- b) Menggunakan perisian Antivirus yang tulen;
- c) Menggunakan *password screen saver* dan *wallpaper* JANM;
- d) *Log-off* dan *power-off* apabila meninggalkan pejabat;
- e) Menggunakan komputer atau *notebook* untuk urusan rasmi sahaja;
- f) Keselamatan fizikal komputer adalah tanggungjawab pengguna;
- g) Tidak dibenarkan menukar komponen atau konfigurasi komputer;
- h) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;
- i) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Perkakasan dan Perisian;

- j) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;
- k) Peralatan ICT yang hendak dibawa keluar dari premis JANM, perlulah mendapat kelulusan Pentadbir Perkakasan/Perisian dan direkodkan bagi tujuan pemantauan;
- l) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;
- m) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;
- n) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Perkakasan dan Perisian;
- o) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Perkakasan dan Perisian untuk di baik pulih dengan mengisi Borang Aduan Kerosakan;
- p) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;
- q) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;
- r) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Perkakasan dan Perisian;
- s) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan
- t) Memastikan *plug* dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.

## 6.2 Pengagihan Perkakasan

Memastikan pengagihan perkakasan dan perisian ICT yang disediakan mencukupi dan operasi perkhidmatan dilaksanakan dengan cekap dan berkesan. Pengagihan selain dari yang dinyatakan di dalam prosedur hendaklah mengikut keperluan kerja

dan kapasiti semasa dengan perakuan daripada pengarah bahagian masing-masing dan mendapat kelulusan Pengarah BPTM.

### **6.2.1 Komputer Desktop (PC)**

Pengagihan PC:

- a. Pegawai kumpulan pengurusan tertinggi;
- b. Pegawai kumpulan pengurusan dan profesional;
- c. Kakitangan sokongan gred 17 ke atas; dan
- d. Selainnya, pengagihan adalah mengikut keperluan kerja seperti tugas pentadbiran, ICT dan teknikal dengan perakuan pengarah bahagian masing-masing dan kelulusan Pengarah BPTM.

### **6.2.2 Komputer Riba**

Pengagihan komputer riba:

- a. Pegawai kumpulan pengurusan tertinggi;
- b. Pengarah Negeri; dan
- c. Setiap Unit/Seksyen di JANM (secara gunasama).

### **6.2.3 Pencetak**

Pengagihan pencetak:

- a. Pegawai kumpulan pengurusan tertinggi layak dan boleh dibekalkan pencetak warna;
- b. Pegawai kumpulan pengurusan dan profesional gred 48 dan ke atas dibekalkan dengan pencetak hitam putih *ligh duty*;
- c. Pegawai kumpulan pengurusan dan profesional gred 44 dan ke bawah dibekalkan dengan pencetak hitam putih *light duty* secara gunasama;

- d. Setiap bahagian di Ibu Pejabat dan setiap pejabat perakaunan JANM boleh dibekalkan dengan pencetak hitam putih berkapasiti tinggi; dan
- e. Setiap bahagian di Ibu Pejabat dan setiap pejabat perakaunan JANM boleh dibekalkan pencetak warna berkapasiti tinggi.

Pengagihan pencetak (d) dan (e) adalah mengikut keperluan kerja dengan perakuan pengarah bahagian masing-masing dan kelulusan Pengarah BPTM.

#### **6.2.4 Pengimbas (*Scanner*)**

Pengagihan pengimbas:

- a. Pejabat pengurusan atasan, bahagian dan pejabat perakaunan JANM layak dibekalkan pengimbas bersaiz A3/A4; dan
- b. Pengimbas berteknologi tinggi dibekalkan mengikut keperluan tugas rasmi dan dengan perakuan pengarah bahagian masing-masing.

#### **6.2.5 Perisian-Perisian ICT**

Perisian-perisian ICT yang disokong dan diluluskan oleh BPTM:

##### **Sistem Pengoperasian:**

- i. Microsoft Windows
- ii. RedHat

##### **Aplikasi Desktop:**

- i. Microsoft Office 2003/2007
- ii. Microsoft Office Visio
- iii. Microsoft Project
- iv. Adobe Photoshop

- v. Micromedia Director
- vi. Dewan Eja Pro

**Komunikasi:**

- i. Web based emel
  - ii. Internet Explorer/ Mozilla Firefox
- 
- a. Pegawai dan kakitangan yang terlibat dengan kerja-kerja seperti urusan pentadbiran, kewangan dan pembangunan projek layak dibekalkan dengan perisian Microsoft Office;
  - b. Setiap bahagian di Ibu Pejabat dan setiap pejabat perakaunan JANM dibekalkan dengan perisian Microsoft Office Visio;
  - c. Setiap bahagian di Ibu Pejabat dan setiap pejabat perakaunan JANM dibekalkan dengan perisian Microsoft Project;
  - d. Setiap bahagian di Ibu Pejabat dan setiap pejabat perakaunan JANM dibekalkan dengan perisian Dewan Eja;
  - e. Perisian grafik Adobe Photoshop hanya dibekalkan kepada pegawai dan kakitangan yang terlibat dengan kerja-kerja penyuntingan dan pembangunan multi media; dan
  - f. Perisian Micromedia Director hanya dibekalkankan kepada unit yang terlibat dalam pembangunan aplikasi web.

**6.3 Perlupusan Perkakasan**

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding*, *grinding*, *degauzing* atau pembakaran;

- b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;
- c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;
- d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;
- e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;
- f) Pegawai aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT;
- g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan
- h) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:
  - Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya;
  - Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di JANM;
  - Memindah keluar dari JANM mana-mana peralatan ICT yang hendak dilupuskan;
  - Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.

## **BAB 07: PROSEDUR KESELAMATAN PERISIAN**

## **BAB 07: PROSEDUR KESELAMATAN PERISIAN**

### **7.1 Pengendalian Dokumen Perisian**

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Semua dokumen perisian yang diwujudkan, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; dan
- b) Semua dokumen perisian hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.

### **7.2 Prosedur Pemasangan Perisian**

Prosedur pemasangan perisian ialah:

- a) Perisian yang dibenarkan sahaja oleh JANM sahaja boleh dipasang pada peralatan ICT;
- b) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada *CD-ROM, disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak;
- c) Mana-mana aplikasi/sistem yang tidak dapat menyokong mana-mana aplikasi sistem yang lain, dan tidak seiring dengan perkembangan teknologi masa terkini, maka ia boleh difikirkan untuk ditingkatkan atau dilupuskan;
- d) Latihan perlu diberikan kepada pengguna perisian aplikasi yang baru; dan
- e) Perisian aplikasi perlu ditingkatkan (*upgrade*) mengikut keperluan dan diselenggarakan dengan baik dari semasa ke semasa.

### **7.3 Perlindungan Daripada Perisian Berbahaya/Tidak Sah**

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) 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;
- b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;
- c) Mengimbas semua perisian atau sistem dengan anti virus sebelum

menggunakannya dan melakukan pengemaskinian anti virus dengan pattern antivirus yang terkini; dan

- d) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

#### **7.4 Penyelenggaraan Perisian**

Perisian hendaklah diselenggara dengan betul bagi memastikan ia dapat berfungsi dengan baik dan lancar.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

- a) Setiap perisian perlu bebas daripada kelemahan, keterdedahan, virus dan aturcara tidak sah;
- b) Sebarang peningkatan atau kemaskini patches daripada perisian sedia ada perlu dilaksanakan sebaik mungkin dan perisian berfungsi mengikut standard yang ditetapkan;
- c) Penyelenggaraan pencegahan yang dinyatakan dalam kontrak penyelenggaraan termasuklah kerja-kerja memeriksa, service, membaiki atau mengganti komponen perisian secara teratur mengikut jadual yang ditetapkan. Tujuan utama ialah untuk mengurangkan kerosakan sistem supaya ianya dapat beroperasi dengan cekap secara berterusan.
- d) Setiap perisian perlu mempunyai tahap keselamatan yang tinggi; dan
- e) Setiap penyelenggaraan perisian oleh pihak luar termasuk tempoh penyelenggaraan hendaklah dipersetujui oleh pihak pengurusan. Salinan kontrak hendaklah diteliti termasuk sokongan perisian dengan kos yang telah dipersetujui.

**BAB 08: PROSEDUR KESELAMATAN  
OPERASI DAN KOMUNIKASI**

## **BAB 08: PROSEDUR KESELAMATAN OPERASI DAN KOMUNIKASI**

### **8.1 Pengendalian Dokumen Prosedur**

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- c) Semua prosedur pengurusan operasi yang diwujudkan, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal;
- d) 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
- e) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.

### **8.2 Backup dan Restore**

Bagi memastikan keselamatan data dan sistem, *backup* hendaklah menggunakan media yang bersesuaian berdasarkan kepada Arahan Kerja Dan Prosedur Kerja.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;
- b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi;
- c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan;
- d) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan
- e) Backup perlu dibuat dalam 2 salinan. Salinan pertama disimpan di dalam Bilik Media backup manakala salinan kedua di simpan di lokasi berlainan;
- f) Manual mengenai prosedur *back-up*, *restore* dan penyenggaraan *server* hendaklah disediakan sebanyak dua salinan.
- g) Tempat penyimpanan media *backup* hendaklah dipastikan selamat dengan suhu di antara 19°C – 22°C; dan
- h) Semua media *backup* hendaklah dilabelkan.

### **8.3 Keselamatan Media**

Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut:

- a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;
- b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;
- c) Menghadkan pendedaran data atau media untuk tujuan yang dibenarkan sahaja;
- d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;
- e) Menyimpan semua media di tempat yang selamat; dan
- f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.

### **8.4 Keselamatan E-mel**

Penggunaan e-mel di JANM hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003, Surat Arahan Ketua Pengarah MAMPU bertajuk “Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan” bertarikh 1 Jun 2007 dan Surat Arahan Ketua Pengarah MAMPU bertajuk “Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-Agensi Kerajaan” bertarikh 23 November 2007.

#### **8.4.1 Kategori E-mel**

Semua kakitangan Jabatan mempunyai e-mel rasmi yang digunakan untuk tujuan rasmi dan didaftarkan dibawah agensi Kerajaan. E-mel rasmi boleh dibahagikan kepada dua kategori iaitu e-mel rahsia rasmi dan e-mel bukan rasmi.

- a) E-mel Rahsia Rasmi

E-mel yang mengandungi maklumat atau perkara rahsia rasmi yang mesti diberi perlindungan untuk keselamatan yang dikelaskan mengikut pengelasannya sama ada *Terhad, Sulit, Rahsia* atau *Rahsia Besar*; dan

b) E-mel Bukan Rahsia Rasmi

E-mel yang tidak mengandungi maklumat atau perkara rahsia rasmi.

#### 8.4.2 Pemakaian Dan Penggunaan E-mel Yang Betul

Perkara-perkara seperti berikut perlu di patuhi dalam penggunaan e-mel JANM:

- a) Akaun e-mel JANM adalah untuk kegunaan rasmi dan urusan pejabat sahaja. Tidak boleh digunakan untuk tujuan peribadi;
- b) Permohonan akaun e-mel JANM hendaklah dengan menggunakan Borang Permohonan E-mel yang boleh diperolehi dari laman web JANM ([www.anm.gov.my](http://www.anm.gov.my));
- c) Semua kakitangan JANM di Ibu Pejabat dan cawangan hendaklah menggunakan e-mel rasmi JANM *@anm.gov.my* dalam sebarang urusan rasmi;
- d) Penggunaan e-mel luar seperti e-mel *Yahoo, Gmail, TMNet* bagi sebarang urusan rasmi adalah tidak dibenarkan;
- e) Webmail JANM ([mail.anm.gov.my](mailto:mail.anm.gov.my)) digalakkan untuk dicapai oleh semua pengguna ingin membuat capaian e-mel;
- f) Penggunaan *mobile access* digalakkan;
- g) Menggunakan format e-mel bukan rahsia rasmi adalah seperti di dalam Lampiran D dan format e-mel rahsia rasmi adalah seperti di Lampiran E;
- h) Penggunaan huruf besar kandungan e-mel adalah tidak digalakkan dan dianggap tidak beretika sebaliknya menggunakan bahasa yang ringkas, betul dan sopan;
- i) Memastikan bahawa subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;

- j) Penghantar boleh menggunakan kemudahan 'salinan kepada (cc)' sekiranya e-mel tersebut perlu dimaklumkan kepada penerima lain. Bagaimanapun, penggunaan 'blind cc' (bcc) tidak digalakkan; dan
- k) Sebagai amalan baik, e-mel penghantar hendaklah **dijawab selewat-lewatnya 4 hari** dari tarikh e-mel berkenaan diterima. Kemudahan penghantaran e-mel jawab automatik semasa berada di luar pejabat bagi tempoh waktu yang panjang adalah digalakkan.

### 8.4.3 Peraturan Menggunakan E-mel

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Rahsiakan dan kukuhkan katalaluan e-mel mengikut prosedur kawalan capaian;
- b) Pengguna e-mel perlu membuka e-mel sekurang-kurangnya 2 kali setiap hari;
- c) Memberi *respon* ke atas email dengan cepat dan mengambil tindakan dengan segera;
- d) Tidak dibenarkan memberikan akaun e-mel dengan sesuka hati kepada orang yang tidak berkenaan kerana dikhuatiri menggalakkan penyebaran virus, e-mel sampah, *spamming* dan sebagainya;
- e) Tidak menggunakan e-mel untuk menyebarkan bahan-bahan yang dilarang seperti gambar lucah, memfitnah, menghasut, gangguan seksual dan sebagainya yang ternyata menyalahi undang-undang atau untuk tujuan politik, perjudian serta perniagaan;
- f) Sistem e-mel membuat tapisan untuk e-mel yang mengandungi fail kepilang (*attachment file*) seperti \*.scr, \*.com, \*.exe, \*.dll, \*.pif, \*.vbs, \*.bat, \*.asd, \*.chm, \*.ocx, \*.hlp, \*.hta, \*.js, \*.shb, \*.shs, \*.vb, \*.vbe, \*.wsf, \*.wsh, \*.reg, \*.ini, \*.diz, \*.cpp, \*.cpl, \*.vxd, \*.sys dan \*.cmd. Ia berkemungkinan akan menyebarkan virus apabila dibuka; dan
- g) Jangan membuka e-mel dari penghantar yang tidak dikenali.

#### 8.4.4 Penyelenggaraan E-mel

Perkara-perkara berikut perlu dilakukan oleh pemilik e-mel JANM bagi memastikan e-mel berjalan lancar:

- a) Pengguna hendaklah membuat salinan dan menyimpan fail ke dalam satu *folder* berasingan dari setiap e-mel yang penting bagi tujuan *backup* jika berlaku sebarang masalah kepada cakera keras komputer;
- b) Lakukan imbasan (*scanning*) ke atas semua fail dan fail kepilan bagi mengenal pasti fail-fail yang diserang virus dengan perisian anti virus *Symantec* atau yang lain;
- c) Bagi pengguna webmail JANM, mana-mana e-mel yang telah dibaca atau diambil tindakan hendaklah dipadam atau diarkib agar saiz storan di dalam e-mel server tidak melebihi 1 *Giga byte (1GB)*. Ini bertujuan untuk menjamin prestasi e-mel *server* dan terus dapat beroperasi dengan baik; dan
- d) Semua e-mel yang rasmi perlu dicetak dan difailkan untuk mengelakkan kehilangan maklumat penting apabila berlaku kerosakan kepada cakera keras komputer.

#### 8.4.5 Tanggungjawab Pengguna E-mel

Peranan dan tanggungjawab pengguna adalah seperti berikut:

- a) Menggunakan akaun e-mel yang diperuntukkan oleh JANM;
- b) Memaklumkan kepada pentadbir e-mel dengan segera sekiranya mengesyaki akaun telah disalahgunakan;
- c) Menggunakan kata laluan yang baik dengan ciri-ciri keselamatan yang bersesuaian dengan merujuk kepada Amalan Baik Keselamatan Kata Laluan di **Lampiran F**;
- d) Memastikan setiap fail yang dimuat turun bebas daripada virus sebelum digunakan;
- e) Bertanggungjawab sepenuhnya terhadap semua kandungan fail elektronik termasuk e-mel dalam akaun sendiri;

- f) Berhenti dan memutuskan talian dengan serta-merta sekiranya kakitangan menerima dan disambungkan ke laman Internet yang mengandungi unsur-unsur tidak menyenangkan;
- g) Mengadakan salinan atau penduaan pada media storan kedua elektronik seperti *thumb drive* dan sebagainya bagi tujuan keselamatan;
- h) Memastikan kemudahan e-mel digunakan dan dibiarkan aktif pada keseluruhan waktu bekerja supaya e-mel yang dialamatkan sampai tepat pada masanya dan tindakan segera ke atasnya dapat disegerakan; dan
- i) Memaklumkan kepada pentadbir e-mel sekiranya berada diluar pejabat dalam tempoh waktu yang lama, bercuti atau bertukar tempat kerja bagi memudahkan penyelenggaraan dilakukan.

## 8.5 Pemantauan

Pemantauan secara sistematik perlu dilakukan bagi memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan dapat dikenalpasti.

### 8.5.1 Pengauditan dan Forensik ICT

ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut:

- a) Sebarang percubaan pencerobohan kepada sistem ICT JANM;
- b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*);
- c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;
- d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;
- e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;
- f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian;
- g) Aktiviti penyalahgunaan akaun e-mel; dan

- h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.

### 8.5.2 Jejak Audit

Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.

Jejak audit hendaklah mengandungi maklumat-maklumat berikut:

- a) Rekod setiap aktiviti transaksi;
- b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;
- c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan
- d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.

### 8.5.3 Sistem Log

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:

- a) Memastikan fail log bagi server dan aplikasi di JANM di aktifkan:
  - i. Fail log sistem pengoperasian;
  - ii. Fail log servis (laman web, ftp,e-mel);
  - iii. Fail log aplikasi (audit trail);
  - iv. Fail log rangkaian ( switch,firewall, router, IDS/IPS); dan
  - v. Fail log backup.
- b) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;
- c) Menyimpan fail log untuk tempoh **sekurang-kurangnya 6 bulan** di tempat

- selamat dan dikemukakan kepada MAMPU apabila diperlukan untuk pengendalian insiden keselamatan ICT;
- d) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan
  - e) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.

#### **8.5.4 Pemantauan Log**

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;
- b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala;
- c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;
- d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;
- e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan
- f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam JANM atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.

**BAB 09: PROSEDUR KESELAMATAN  
RANGKAIAN**

## **BAB 09      PROSEDUR KESELAMATAN RANGKAIAN**

### **9.1      Keselamatan Rangkaian**

Keselamatan rangkaian adalah merupakan satu langkah keselamatan utama untuk mengawal aset ICT JANM dari dicerobohi.

#### **9.1.1    Infrastruktur Rangkaian**

Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.

Perkara-perkara seperti berikut mestilah dipatuhi:

- a) Rekabentuk infrastruktur rangkaian perlu mempunyai ciri-ciri keselamatan terbaik dari segi tahap keselamatan dengan dilindungi oleh mekanisma keselamatan rangkaian meliputi *Firewall*, *Intrusion Prevention System (IPS)* / *Intrusion Detection System (IDS)*, dan Antivirus;
- b) Maklumat berkaitan rangkaian JANM seperti *network address*, konfigurasi, rekabentuk adalah tidak dibenarkan sama sekali didedahkan kepada pihak luar;
- c) Pemantauan perlu dilakukan sepanjang masa untuk memastikan keselamatan rangkaian dan server JANM di dalam *DMZ zone*, *server farm* dan lain-lain sentiasa berada di dalam keadaan baik dan selamat;
- d) Perisian *sniffer* atau *network analyzer* adalah dilarang sama sekali di pasang di mana-mana PC / *notebook*;
- e) Pengguna luar yang melakukan capaian rangkaian di dalam JANM perlu mendapat kebenaran Pentadbir Rangkaian;
- f) PC yang dibenarkan sahaja dibenarkan untuk membuat sambungan *Virtual Area Network (VLAN)* yang telah ditetapkan; dan
- g) Semua pengguna hanya dibenarkan menggunakan rangkaian JANM sahaja dan penggunaan media lain (*modem*, *wireless*, *broadband*) adalah dilarang sama sekali.

### 9.1.2 Pelaporan Kerosakan

Perkara-perkara seperti berikut hendaklah dipatuhi :

- a) Sebarang kerosakan pada kabel *UTP*, *network point* dan *network port* pada mana-mana *switch* hendaklah dilaporkan kepada pegawai teknikal sistem masing-masing.

**BAB 10: PROSEDUR KESELAMATAN  
KAWALAN CAPAIAN**

## **BAB 10      PROSEDUR KESELAMATAN KAWALAN CAPAIAN**

### **10.1 Kawalan Capaian Pengguna**

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 hendaklah mengikut keperluan keselamatan dan peranan pengguna;
- b) Kawalan capaian ke atas perkhidmatan rangkaian sama ada dalaman dan luaran;
- c) Keselamatan maklumat yang dicapai hendaklah menggunakan kemudahan atau peralatan mudah alih; dan
- d) Kawalan ke atas kemudahan pemrosesan maklumat.

#### **10.1.1 Akaun Pengguna**

Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:

- a) Penggunaan akaun yang diperuntukkan oleh JANM sahaja boleh digunakan;
- b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;
- c) Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;
- d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan JANM. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;
- e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah

- dilarang; dan
- f) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut:
- i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu;
  - ii. Bertukar bidang tugas kerja;
  - iii. Bertukar ke agensi lain;
  - iv. Bersara; atau
  - v. Ditamatkan perkhidmatan.

### 10.1.2 Keselamatan Kata Laluan

Katalaluan mesti dijaga dengan selamat agar tidak dicerobohi oleh pengguna lain. Sila pastikan perkara-perkara berikut:

- a) Kata laluan hendaklah dirahsiakan;
- b) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;
- c) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;
- d) Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara, angka dan aksara khusus;
- e) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;
- f) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;
- g) Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;
- h) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula;
- i) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;
- j) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian

- sistem) dan selepas had itu, sesi ditamatkan secara automatik;
- k) Kata laluan hendaklah ditukar **selepas 90 hari** atau selepas tempoh masa yang bersesuaian;
  - l) Mengelakkan penggunaan semula kata laluan yang telah digunakan; dan
  - m) Jangan menggunakan nama pengguna (*userid*) sebagai katalaluan.

### 10.1.3 Keselamatan Penggunaan Kad Pintar

Peraturan berikut hendaklah dipatuhi bagi pengguna menggunakan kad pintar dan *PKI* dengan lebih cekap dan selamat:

- a) Permohonan kad pintar boleh dilakukan dengan mengisi borang daripada Pentadbir Sistem;
- b) Pemilik kad pintar akan diberi tahap capaian mengikut tahap kelayakan contohnya pegawai penyemak hanya boleh melakukan penyemakan sahaja dan tidak boleh melakukan pengesahan bagi sebarang urusan GFMAS dan eSPKB;
- c) Kad pintar dan kata laluan bagi kad pintar hendaklah di simpan di tempat selamat dan sukar dicapai oleh pihak luar;
- d) Pemilik kad pintar hendaklah menghafal kata laluan;
- e) Pemilik kad pintar tidak dibenarkan meminjamkan kad tersebut kepada orang lain yang tidak berkenaan;
- f) Penggunaan tandatangan berdigital dalam melakukan sebarang kelulusan hanya akan diberikan kepada pegawai yang telah disahkan oleh JANM;
- g) Pemilik kad pintar dilarang memohon bantuan pihak lain bagi melakukan tandatangan berdigital; dan
- h) Kad pintar hendaklah berdaftar dengan pihak berkuasa pensijilan digital Malaysia yang sah iaitu DigiCert (kad pintar GFMAS) atau MIMOS (kad pintar eSPKB).

## 10.2 Kawalan Capaian Rangkaian

### 10.2.1 Keselamatan Capaian Rangkaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

- a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian JANM, rangkaian agensi lain dan rangkaian awam;
- b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan
- c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

### 10.2.2 Keselamatan Capaian Internet

Perkara-Perkara Yang Dilarang Semasa Menggunakan Internet

- a) Menghantar, menyimpan atau menerima sebarang bahan atau pesanan-pesanan yang menjadi kesalahan dan sensitif kepada perkauman, kebudayaan atau seksual;
- b) Memuat turun, menyebarkan dan menyimpan sebarang imej, video serta audio yang berbentuk pornografi, berunsurkan fitnah dan perkauman;
- c) Memuat turun apa jua perisian dengan sesuka hati sebagai contoh *screen saver, games, perisian chatting*;
- d) Menyalin bahan-bahan yang dipaten atau Hak Milik Terpelihara, termasuk teks, kod aturcara/program, data atau apa jua bahan tanpa kebenaran daripada pemilik bahan-bahan tersebut;
- e) Menyebarkan pesanan atau maklumat palsu, ugutan atau gangguan seksual, atau menyebarkan dengan niat apa jua bahan yang boleh merosakkan kepentingan awam;
- f) Melayari laman web yang tidak beretika/bermoral atau mengakses bahan-bahan yang mengandungi unsur-unsur lucah, *gay, lesbian* dan sebagainya;
- g) Menggunakan perisian seperti KAZA, *BitTorrent movie, game* dan lain-lain dengan menggunakan kemudahan Kerajaan;

- h) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan;
- i) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; dan
- j) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan.

### 10.3 Kawalan Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi:

- a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan
- b) Merekodkan capaian yang berjaya dan gagal.

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

- a) Mengesahkan pengguna yang dibenarkan;
- b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan
- c) Menjana amaran (*alert*) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin;
- b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;
- c) Menghadkan dan mengawal penggunaan program; dan
- d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

#### **10.4 Kawalan Capaian Aplikasi dan Maklumat**

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

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

- a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;
- b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);
- c) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;
- d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan
- e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.

#### **10.5 Prosedur Kawalan Capaian Perbankan Internet (*Online Banking*)**

Prosedur berikut bertujuan melindungi sistem perbankan internet (*online banking*) JANM dari sebarang bentuk capaian yang tidak dibenarkan di mana boleh menyebabkan pencerobohan dan apa jua jenayah cyber.

Bagi memastikan kawalan capaian perbankan internet adalah kukuh, perkara-perkara berikut hendaklah dipatuhi:

- a) Pihak bank perlu mematuhi polisi dan garis panduan yang telah ditetapkan oleh Bank Negara Malaysia (*Minimum Guidelines on the Provision of Internet Banking Services*) di dalam pelaksanaan perbankan Internet khususnya dari segi keselamatan perbankan;
- b) Bagi memastikan tahap keselamatan perbankan internet di tahap optimum, pihak bank perlulah menggunakan *Public Key Infrastructure (PKI)* bagi proses *authorization*;
- c) Mewujudkan satu capaian khas yang selamat dari Pejabat Perakaunan ke Bank dan sebaliknya;
- d) Pihak bank perlu melaksanakan amalan terbaik (*best practice*) terhadap host perbankan internet seperti penggunaan screen server berpassword, mempunyai *antivirus pattern* terkini, *update patch*, *disable default service* yang tidak digunakan dan lain-lain lagi; dan
- e) JANM perlu memastikan bahawa Firewall perlu diletakkan di antara *host* perbankan internet dengan sistem GFMAS bagi tujuan pemantauan dan keselamatan.

**BAB 11: PROSEDUR PEROLEHAN,  
PEMBANGUNAN DAN PENYELENGGARAAN  
SISTEM**

## **BAB 11 PROSEDUR PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM**

### **11.1 Keselamatan Dalam Membangunkan Sistem Dan Aplikasi**

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

#### **11.1.1 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 sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.

#### **11.1.2 Pengesahan Data Input Dan Output**

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan
- b) Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.

## **11.2 Kawalan Kriptografi**

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

### **11.2.1 Enkripsi**

Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.

## **11.3 Keselamatan Fail Sistem**

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

### **11.3.1 Kawalan Fail Sistem**

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah 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.

## **11.4 Keselamatan Dalam Proses Pembangunan Dan Sokongan**

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

### **11.4.1 Prosedur Kawalan Perubahan**

Perkara-perkara yang perlu dipatuhi adalah seperti 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. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor;

- c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;
- d) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan
- e) Menghalang sebarang peluang untuk membocorkan maklumat.

#### **11.4.2 Pembangunan Perisian Secara Outsource**

Pembangunan perisian secara outsource perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik JANM.

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

Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.

#### **11.5.1 Kawalan dari Ancaman Teknikal**

Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan.

Perkara yang perlu dipatuhi adalah seperti berikut:

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

**BAB 12: PROSEDUR PENGURUSAN  
KESINAMBUNGAN PERKHIDMATAN**

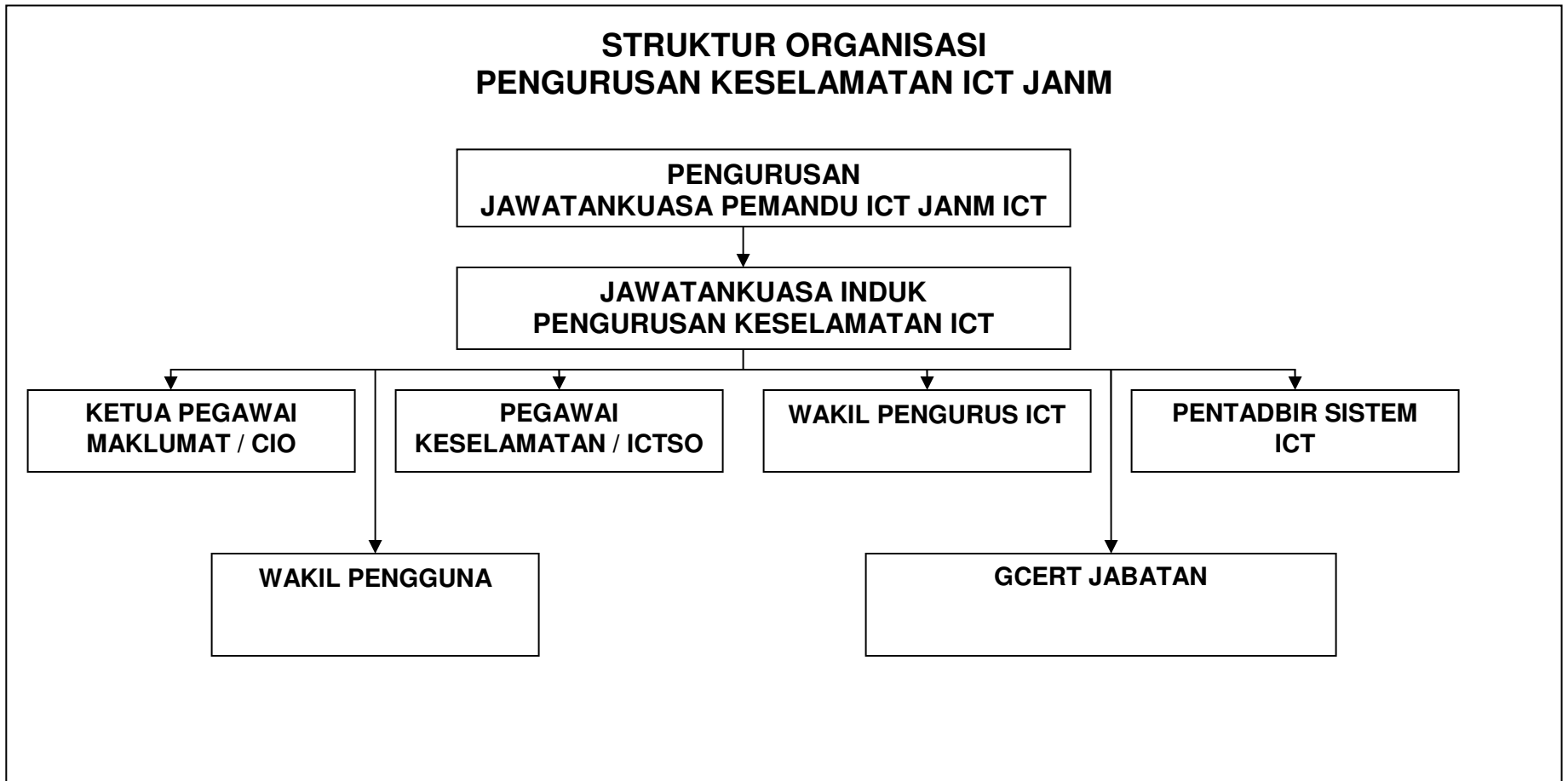
## **BAB 12: PROSEDUR PENGURUSAN KESINAMBUNGAN PERKHIDMATAN**

Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi.

Pengurusan kesinambungan perkhidmatan JANM hendaklah mematuhi Rancangan Pengurusan Kesinambungan Perkhidmatan JANM yang akan dihasilkan kelak.

**LAMPIRAN**

**Lampiran A: Struktur Organisasi Pengurusan Keselamatan ICT JANM**



**Lampiran B: Surat Akuan Pematuhan**

**POLISI KESELAMATAN ICT JANM**

Nama	:	.....
No. Kad Pengenalan	:	.....
Jawatan	:	.....
Kementerian/Jabatan	:	.....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

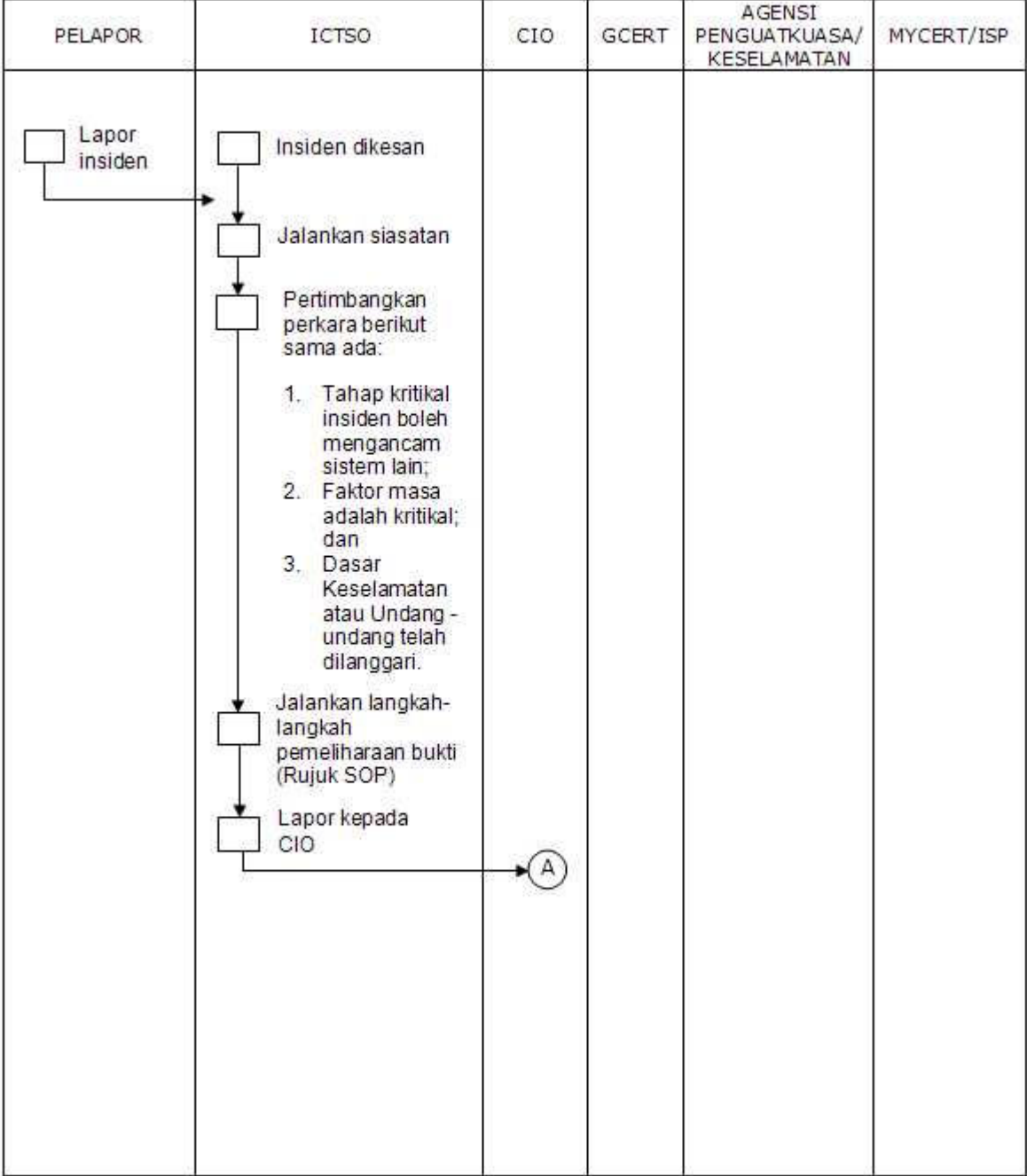
.....  
(Tanda Tangan Pegawai )

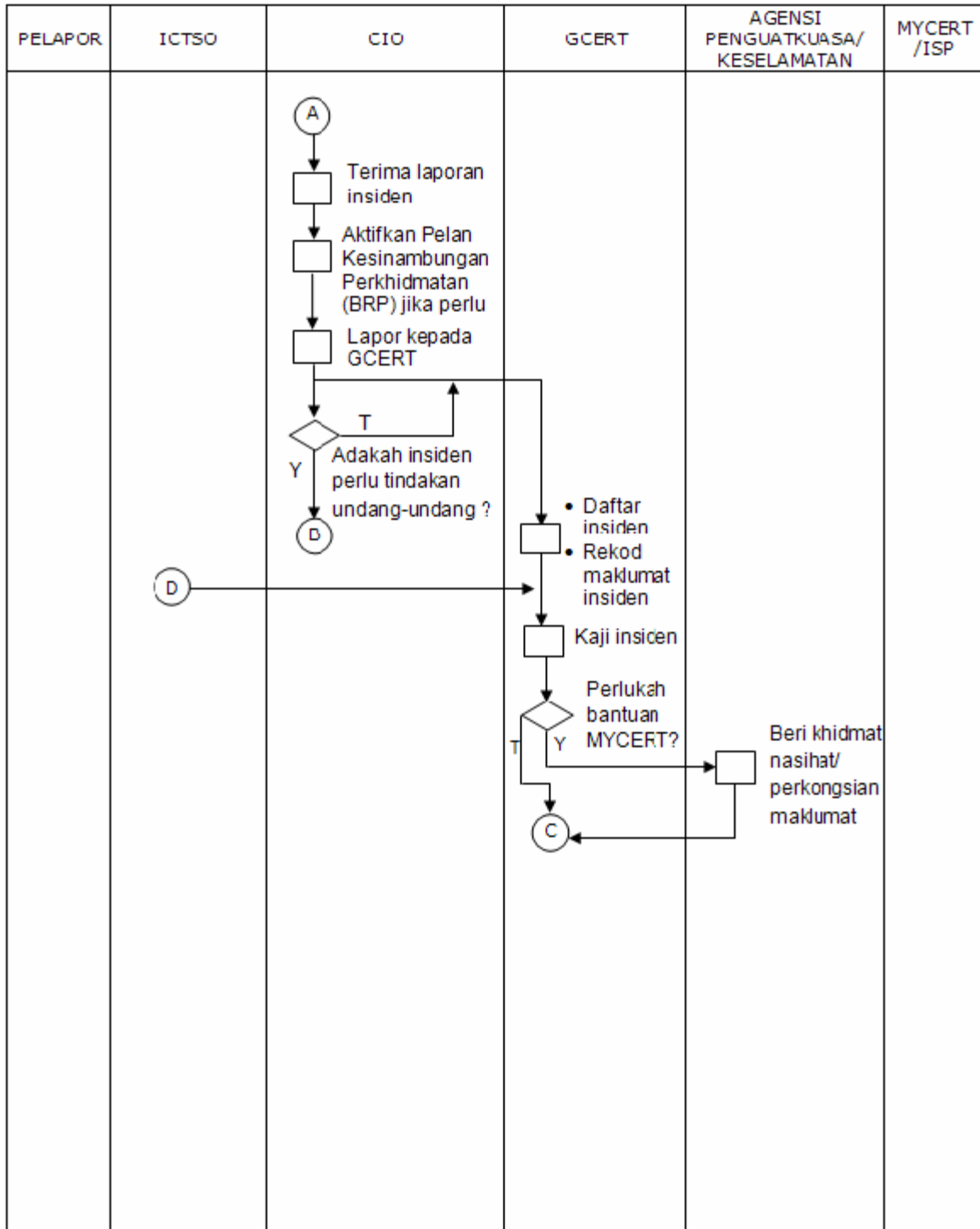
Tarikh : .....  
Pengesahan Pegawai Keselamatan ICT

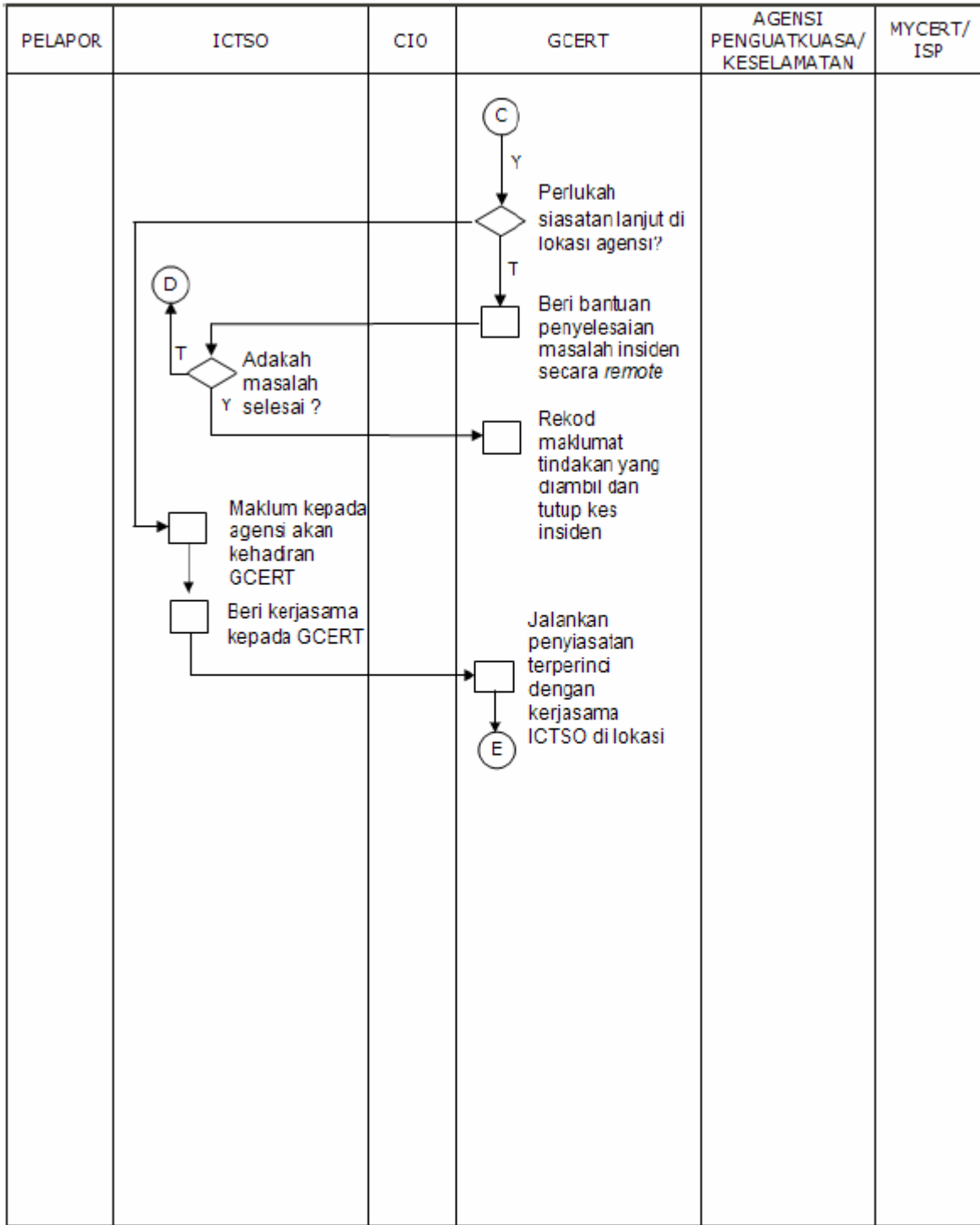
.....  
( Nama Pegawai Keselamatan ICT )  
b.p Ketua Pengarah  
Kementerian / Jabatan  
Tarikh : .....

**Lampiran C: Proses Kerja Pelaporan Insiden Rujukan MAMPU**

**Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT MAMPU**





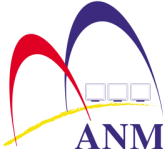


PELAPOR	ICTSO	CIO	GCERT	AGENSI PENGUATKUASA/ KESELAMATAN	MYCERT/ ISP
			<p data-bbox="711 310 760 359">E</p> <p data-bbox="711 470 760 518">↓</p> <p data-bbox="711 443 760 491">Tindakan IRH di lokasi:-</p> <ul data-bbox="760 499 992 1045" style="list-style-type: none"> <li>• Kawal kerosakan</li> <li>• Baikpulih minima dengan segera</li> <li>• Siasat Insiden dengan terperinci</li> <li>• Analisa Impak (Business Impact Analysis)</li> <li>• Hasilkan laporan Insiden</li> <li>• Bentang dan kemukakan laporan kepada agensi</li> <li>• Selaraskan tindakan di antara agensi dan Agensi Penguatkuasa/ Keselamatan (jika berkenaan)</li> </ul> <p data-bbox="711 1052 760 1100">↓</p> <p data-bbox="711 1052 760 1100">Rekod laporan dan tutup kes insiden</p>	<p data-bbox="1024 310 1073 359">B</p> <p data-bbox="1024 365 1073 413">↓</p> <p data-bbox="1024 386 1224 659">Ambil tindakan ke atas insiden yang menyalahi undang-undang dan peraturan berkaitan</p> <p data-bbox="1024 688 1224 827">(Kerjasama dengan GCERT di lokasi jika perlu)</p>	

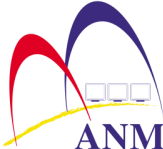
**Penunjuk :**

SOP - *Standard Operating Procedure*

## Lampiran D: Contoh Format E-Mel Bukan Rahsia Rasmi

From	: ali@anm.gov.my
To	: abu@anm.gov.my
Cc	: bakar@anm.gov.my
Subjek	: Kursus Pengenalan Komputer      No. Ruj : ANM/BPTM/003/2 (24)
	JABATAN AKAUNTAN NEGARA MALAYSIA Aras 1-8, Kompleks Kementerian Kewangan, No.1, Persiaran Perdana, Precint 2, 62594 PUTRAJAYA.
<b>"BERKHIDMAT UNTUK NEGARA"</b>  <b>ALI BIN AHMAD</b> Pegawai Teknologi Maklumat Bahagian Pengurusan Teknologi Maklumat Jabatan Akauntan Negara Malaysia Tel: 03-8882 0088 Fax: 03-8882 0089	

## Lampiran E: Contoh Format E-Mel Rahsia Rasmi

From	: ali@anm.gov.my
To	: abu@anm.gov.my
Cc	: bakar@anm.gov.my
Subjek	: Kursus Asas Microsoft Word 2007 No. Ruj : ANM/BPTM/003/2 (24)
	JABATAN AKAUNTAN NEGARA MALAYSIA Aras 1-8, Kompleks Kementerian Kewangan, No.1, Persiaran Perdana, Precint 2, 62594 PUTRAJAYA.
<b>RAHSIA</b>	
<b>RAHSIA</b>	
<b>"BERKHIDMAT UNTUK NEGARA"</b>	
<b>ALI BIN AHMAD</b> Pegawai Teknologi Maklumat Bahagian Pengurusan Teknologi Maklumat Jabatan Akauntan Negara Malaysia Tel: 03-8882 0088 Fax: 03-8882 0089	

## Lampiran F: Amalan Baik Keselamatan Kata Laluan

1. Rahsiakan kata laluan anda dari pengetahuan orang lain. Pendedahan kepada yang tidak berhak adalah satu kesalahan di bawah Akta Jenayah Komputer 1997;
2. Sekiranya kata laluan telah dikompromi atau disyaki dikompromi, hendaklah dilaporkan kepada pentadbir e-mel dan kata laluan sedia ada diubah dengan serta merta;
3. Kata laluan hendaklah diubah sekurang-kurangnya sekali dalam 30 hari;
4. Kata laluan hendaklah mempunyai saiz sekurang-kurangnya lapan (8) aksara dengan gabungan alphanumerik dan simbol khas. Contoh kata laluan yang baik adalah "j2yU!pA\*";
5. Elakkan diri menggunakan semula empat (4) kata laluan yang terdahulu; dan
6. Kata laluan hendaklah dihafal dan jangan sekali-kali disalin di mana-mana media.

## RUJUKAN

Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di Jabatan termasuklah seperti berikut:

- 1) Pekeliling Am Bil. 3 tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan
- 2) Pekeliling Am Bil.1 Tahun 2001 –Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)
- 3) Pekeliling Am Bil.1 Tahun 2006 – Pengurusan Laman Web/Portal Sektor Awam
- 4) Pekeliling Kemajuan Perkhidmatan Awam Bil 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.
- 5) Surat Ketua Pengarah MAMPU (MAMPU.702-1/1/7 Jld.3 (48)) – Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-Agensi Kerajaan.
- 6) Surat Ketua Pengarah MAMPU (UPTM 159/526/9 Jld. 4 (59) ) – Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan.
- 7) Surat Ketua Pengarah MAMPU (UPTM 159/526/9 Jld. 4 (60) ) – Langkah-Langkah Pemantapan Perlaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan.
- 8) Surat Ketua Pengarah MAMPU (MAMPU .eKL.700.2/10 (2) ) – Panduan Penyediaan Dan Penyiaran Berita Online Di Laman Web Agensi-Agensi Kerajaan.

- 9) Arahan Keselamatan
- 10) Arahan Teknologi Maklumat dan Akta Aktiviti Kerajaan Elektronik (Akta 680)
- 11) Akta Rahsia Rasmi 1972
- 12) Akta Komunikasi dan Multimedia Malaysia (AKM), 1998;
- 13) Akta Kawasan Larangan dan Tempat Larangan 1959
- 14) *Computer Crime Act 1997*
- 15) *Digital Signature Act 1997*
- 16) *Communications and Multimedia Act 1998*
- 17) *Malaysian Communications and Multimedia Commission act 1998*
- 18) *Malaysian Public Sector Management of Information and Communication Technology Security Handbook (MyMIS).*
- 19) Undang-Undang Malaysia Akta 680 (Akta Aktiviti Kerajaan Elektronik 2007)