

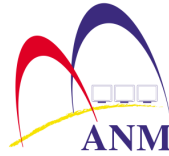
**POLISI KESELAMATAN ICT**  
**JABATAN AKAUNTAN NEGARA MALAYSIA**  
**Versi 1.0 / 2008**



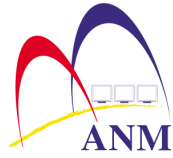
## PERKARA

## MUKA SURAT

<b>GLOSARI.....</b>	<b>5</b>
<b>SINGKATAN.....</b>	<b>9</b>
<b>PENDAHULUAN .....</b>	<b>10</b>
<b>OBJEKTIF .....</b>	<b>10</b>
<b>SASARAN .....</b>	<b>11</b>
<b>BAHAGIAN 1.0: PENYATAAN POLISI KESELAMATAN ICT .....</b>	<b>12</b>
1.1    Penyataan Polisi Keselamatan ICT .....	12
1.1.1    Keperluan Keselamatan .....	12
1.2    Prinsip-prinsip polisi .....	13
1.3    Objektif Polisi Keselamatan ICT JANM .....	16
1.4    Skop.....	17
1.5    Pelanggaran.....	18
1.6    Pindaan Dan Kemaskini .....	18
1.7    Maklumat lanjut.....	19
<b>BAHAGIAN 2.0: PENGURUSAN KESELAMATAN ICT.....</b>	<b>20</b>
2.1    Pengurusan Keselamatan ICT .....	20
2.2    Struktur Organisasi Pengurusan Keselamatan ICT JANM.....	21
2.2.1    Jawatankuasa Induk Pengurusan .....	21
2.2.2    Jawatankuasa Pengurusan Keselamatan ICT .....	22
2.3    Agensi Luar .....	28
2.3.1    Jabatan Audit Negara (Sistem Perakaunan) .....	28
2.4    Pihak Luar.....	29
<b>BAHAGIAN 3.0 : PENGURUSAN PENILAIAN RISIKO DAN INSIDEN .....</b>	<b>30</b>



3.1	Pengurusan Penilaian Risiko Keselamatan ICT .....	30
3.1.1	Tanggungjawab Melaksanakan Penilaian Risiko Keselamatan ICT.....	30
3.1.2	Skop Penilaian Risiko .....	31
3.1.3	Analisa Risiko .....	31
3.1.4	Penentuan Tindakan Pengendalian Risiko .....	32
3.1.5	Kawalan Risiko .....	32
3.2	Pengurusan Pengendalian Insiden Keselamatan ICT .....	33
3.2.1	Insiden Keselamatan ICT .....	33
3.2.2	Mekanisme Pelaporan Insiden .....	35
<b>BAHAGIAN 4.0 : PENGURUSAN KESELAMATAN SUMBER .....</b>		<b>36</b>
4.1	Pengurusan Keselamatan Aset .....	36
4.1.1	Tanggungjawab Ke Atas Aset .....	36
4.2	Pengurusan Data Dan Maklumat .....	36
4.2.2	Keselamatan Maklumat.....	37
4.3	Pengurusan Keselamatan Sumber Manusia .....	37
4.4	Pengurusan Keselamatan Premis, Peralatan Dan Persekitaran.....	37
4.5	Pengurusan Keselamatan Perisian .....	37
4.6	Pengurusan Keselamatan Operasi Dan Komunikasi .....	38
4.7	Pengurusan Keselamatan Kawalan Capaian .....	38
4.8	Pengurusan Keselamatan Didalam Perolehan, Pembangunan Dan Penyelenggaraan Sistem Maklumat .....	38
<b>BAHAGIAN 5.0 : PENGURUSAN KESINAMBUNGAN PERKHIDMATAN .....</b>		<b>39</b>
5.1	Pengurusan Kesinambungan Perkhidmatan .....	39
<b>BAHAGIAN 6.0 : PEMATUHAN .....</b>		<b>39</b>
6.1	Pematuhan Keperluan Perundangan .....	39
6.2	Keperluan Perundangan .....	39
6.3	Tanggungjawab.....	41
6.3.1	Tanggungjawab Pengguna ICT .....	41
6.3.2	Tanggungjawab Ketua Jabatan, Pegawai Keselamatan ICT, Pengurus ICT dan Pentadbir Sistem.....	41

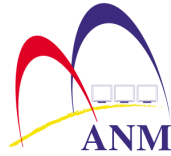


## **SENARAI LAMPIRAN**

### **LAMPIRAN**

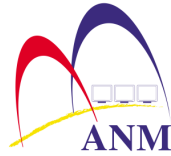
### **PERKARA**

Lampiran A	Struktur Organisasi Pengurusan Keselamatan ICT JANM
Lampiran B	Surat Akuan Pematuhan Polisi Keselamatan ICT JANM

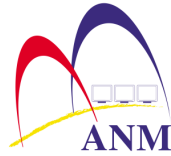


## GLOSARI

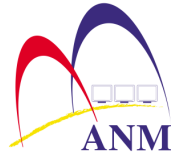
Ancaman	Bermaksud apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah.
Aset ICT	Data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang berada di bawah tanggungjawab JANM.
Dokumen	Semua 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.
Ibu Pejabat JANM	Bermaksud Ibu Pejabat Jabatan Akauntan Negara Malaysia Putrajaya.
Insiden Keselamatan	Musibah ( <i>adverse event</i> ) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Kerentanan ( <i>Vulnerability</i> )	Bermaksud sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman.
Ketua Jabatan	Merujuk kepada maksud Timbalan Akauntan Negara JANM (Korporat)



Media storan	Perkakasan yang berkaitan dengan penyimpanan data dan maklumat seperti disket, kartrij, cakera padat, cakera mudah alih, pita, cakera keras dan pemacu pena.
Pejabat Perakaunan	Bermaksud merangkumi Pejabat Cawangan Negeri dan Jabatan Mengakaun Sendiri.
Penilaian Risiko	Bermaksud penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.
Pengguna ICT	Anggota JANM, pegawai yang bertugas di pejabat perakaunan, pembekal, pakar runding dan penjawat awam yang menggunakan sistem JANM serta pihak-pihak lain yang terlibat.
Pengurus ICT	Pengarah-pengarah Bahagian di JANM, Pengarah-pengarah JANM Negeri dan Cawangan serta Ketua Akauntan JMS.
Pentadbir Sistem ICT	Pegawai-pegawai yang dipertanggungjawabkan dalam melaksanakan tugas-tugas pentadbiran sistem ICT di Bahagian-bahagian JANM, Negeri/Cawangan dan JMS



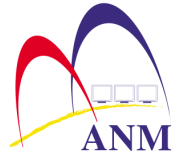
Perisian Sistem	Pemrograman pelbagai (Multi-tasking) iaitu keupayaan satu-satu komputer melaksanakan arahan-arahan ,dari beberapa program/ aplikasi secara serentak pada satu masa. Selain itu, pemprosesan pelbagai melibatkan penyambungan beberapa unit pemprosesan pusat bagi tujuan operasi pemprosesan 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> , <i>antivirus</i> , dan lain-lain.
Rahsia Besar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia , hendaklah diperingkatkan Rahsia Besar. [ Rujukan : Dokumen Arahan Keselamatan ]
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada



sesebuah kuasa asing hendaklah diperingkatkan Rahsia.

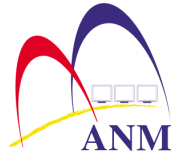
[ Rujukan : Dokumen Arahan Keselamatan ]

Risiko	Bermaksud kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian
Sistem JANM	Semua sistem yang digunakan di JANM serta sistem-sistem yang dibangunkan dan/atau digunapakai di JANM dan Pejabat Perakaunan.
Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing hendaklah diperingkatkan Sulit. [ Rujukan : Dokumen Arahan Keselamatan ]
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakan juga diberi satu tahap perlindungan keselamatan hendaklah diperingkatkan Terhad. [ Rujukan : Dokumen Arahan Keselamatan ]



## SINGKATAN

ICT	Singkatan perkataan <i>Information, Communication and Technology</i> atau bidang Teknologi Maklumat dan Komunikasi
JANM	Singkatan perkataan Jabatan Akauntan Negara Malaysia
JMS	Singkatan perkataan Jabatan Mengakaun Sendiri.
SPICT	Seksyen Pengurusan Komunikasi dan Operasi ICT.



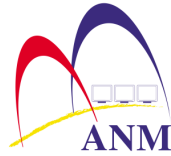
## **PENDAHULUAN**

Penggunaan ICT dalam tugas harian di JANM semakin meningkat setelah pelaksanaan aplikasi penting GFMAS, eSPKB, HRMIS dan lain-lain lagi. Bilangan pengguna e-mel dan internet di kalangan pegawai dan kakitangan JANM telah bertambah selaras dengan pertambahan perjawatan dan galakan daripada pengurusan untuk menggunakan kemudahan ICT untuk memudahkan dalam menjalankan tugas seharian. Untuk memastikan maklumat-maklumat penting JANM bebas daripada sebarang ancaman, pengguna dinasihatkan untuk mematuhi polisi 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**

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

Polisi ini juga diharapkan dapat menjamin keselamatan maklumat Jabatan di samping untuk mencegah salahguna atau kecurian sumber serta aset ICT Jabatan.

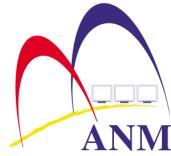


Aspek keselamatan ICT adalah:

- Menjamin aset ICT dilindungi dari hilang, disalahguna atau diseleweng;
- Menjamin urusan ICT berjalan lancar;
- Melindungi kepentingan pihak-pihak yang bergantung kepada sistem daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti dan kebolehsediaan maklumat dan komunikasi.

## **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.



## **BAHAGIAN 1.0: PENYATAAN POLISI KESELAMATAN ICT**

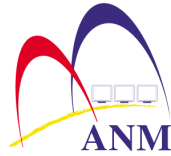
### **1.1 Penyataan Polisi Keselamatan ICT**

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyediakan dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan.

Polisi Keselamatan ICT JANM adalah untuk melindungi aset ICT dan maklumat elektronik dengan meminimumkan kesan insiden keselamatan ICT bagi menjamin keselamatan pengoperasian Jabatan dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ini adalah bertujuan untuk menjamin kesinambungan urusan dengan menekankan aspek kepenggunaan aset ICT serta prosedur keselamatan yang perlu diikuti seperti yang telah ditetapkan.

#### **1.1.1 Keperluan Keselamatan**

Aspek keselamatan yang telah dikenal pasti, dipersetujui dan didokumen pada setiap peringkat perolehan, pembangunan dan penyelenggaraan adalah dipatuhi. Ini termasuk keperluan kawalan jaminan keselamatan bagi sistem maklumat baru atau penambahbaikan ke atas sistem sedia ada.



## 1.2 Prinsip-prinsip polisi

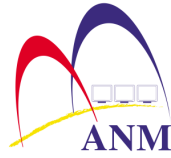
Prinsip-prinsip yang menjadi asas kepada Polisi Keselamatan ICT adalah seperti berikut:

### (a) Akses atas dasar “perlu mengetahui”

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan akses di bawah prinsip ini adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut:

#### i. Klasifikasi Maklumat

Keselamatan ICT Kerajaan hendaklah mematuhi “Arahan Keselamatan” perenggan 53, muka surat 15, di mana maklumat dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad. Data, bahan atau maklumat rasmi yang sensitif atau bersifat terperingkat perlu dilindungi dari pendedahan, di manipulasi atau diubah semasa dalam penghantaran. Penggunaan kod dan/atau tandatangan digital mesti digunapakai bagi melindungi data yang dikirim secara elektronik. Dasar kawalan akses ke atas aplikasi atau sistem juga hendaklah mengikut klasifikasi maklumat yang sama, iaitu sama ada rahsia besar, rahsia, sulit atau terhad; dan



## ii. Tapisan Keselamatan Pengguna

Polisi Keselamatan ICT adalah mematuhi prinsip bahawa pengguna boleh diberi kebenaran mengakses kategori maklumat tertentu setelah siasatan latar belakang menunjukkan tiada sebab atau faktor untuk menghalang pengguna daripada berbuat demikian.

### (b) Hak akses

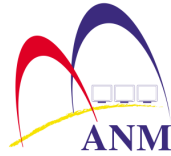
Kelulusan khas adalah diperlukan untuk membolehkan pengguna akses pada tahap-tahap yang ditetapkan untuk membaca, melihat, mewujudkan, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu data atau maklumat.

### (c) Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT.

### (d) Pengasingan

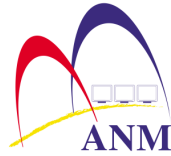
- i. Prinsip pengasingan bermaksud bahawa kombinasi tugas-tugas mewujudkan, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah dilakukan oleh orang yang berlainan. Ia bertujuan untuk mengelak akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat, dimanipulasi dan seterusnya, mengekalkan integriti dan kebolehsediaan; dan



- ii. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. Ia bertujuan untuk mengasingkan akses kepada domain kedua-dua kumpulan tersebut seperti akses kepada fail data, fail program, kemudahan sistem dan komunikasi, manakala pemisahan antara domain pula adalah untuk mengawal dan mengurus perubahan pada konfigurasi dan keperluan sistem.

(e) *Audit trail*

- i. *Audit trail* adalah kemudahan yang disediakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall*, dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*. Pentingnya *audit trail* ini menjadi semakin ketara apabila wujud keperluan untuk mengenal pasti punca masalah atau ancaman kepada keselamatan ICT. Oleh itu, rekod *audit trail* hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta-merta; dan
- ii. *Audit trail* boleh juga dalam bentuk rekod-rekod manual seperti dokumen operasi, nota serah tugas, kelulusan keluar pejabat, memorandum, borang kebenaran, surat kuasa, senarai inventori dan kemudahan akses log. Ini adalah kerana dalam kes-kes tertentu, dokumen ini diperlukan untuk menyokong *audit trail* sistem komputer.



(f) Pematuhan

Polisi Keselamatan ICT JANM hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

(g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan.

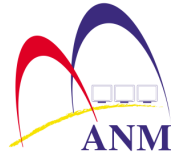
(h) Saling bergantung

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

### 1.3 Objektif Polisi Keselamatan ICT JANM

Objektif utama Polisi Keselamatan ICT JANM ialah seperti berikut:

- (a) Memastikan kelancaran operasi JANM dan meminimumkan kerosakan atau kemusnahan;
- (b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

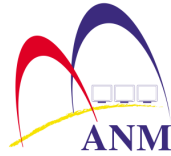


(c) Mencegah salah guna atau kecurian aset ICT JANM.

#### 1.4 Skop

Polisi ini meliputi semua sumber atau aset ICT yang digunakan seperti:

- i. Data dan Maklumat – Semua data dan maklumat yang disimpan atau digunakan pada pelbagai media atau peralatan ICT.
- ii. Perisian – Semua perisian yang digunakan untuk mengendali, memproses, menyimpan, menjana dan menghantar maklumat. Ini meliputi semua perisian utiliti, perisian rangkaian, program aplikasi, pangkalan data, fail program dan fail data.
- iii. Perkakasan ICT – Semua peralatan komputer dan periferal seperti komputer peribadi, *workstation*, pelayan dan semua alat-alat prasarana ICT.
- iv. Media Storan – Semua media storan dan peralatan yang berkaitan seperti disket, katrij, CDROM, pita, cakera, pemacu cakera, pemacu pita dan pemacu luaran.
- v. Komunikasi dan Peralatan Rangkaian – Semua peralatan komunikasi dan rangkaian seperti pelayan rangkaian, *gateway*, *router*, *switch*, *firewall* dan lain-lain.
- vi. Dokumentasi – Semua dokumentasi yang mengandungi maklumat berkaitan dengan penggunaan dan pemasangan peralatan dan



perisian. Ia juga meliputi data dalam semua bentuk media seperti salinan kekal, salinan elektronik, risalah dan *slides*.

- vii. Manusia – Semua pengguna yang dibenarkan termasuk pentadbir dan pengurus serta mereka yang bertanggungjawab terhadap keselamatan ICT.

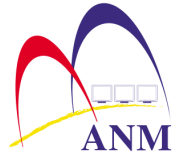
Polisi ini adalah terpakai oleh semua anggota JANM, pegawai yang bertugas di pejabat perakaunan, pembekal, pakar runding dan penjawat awam yang menggunakan sistem JANM serta pihak-pihak lain yang terlibat di dalam mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT JANM.

## **1.5 Pelanggaran**

Pengguna yang tidak mematuhi Polisi Keselamatan ICT JANM akan dikenakan tindakan tatatertib mengikut Peraturan-peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993 [Pindaan 2002], Akta Rahsia Rasmi 1972 dan akta-akta lain yang berkaitan.

## **1.6 Pindaan Dan Kemaskini**

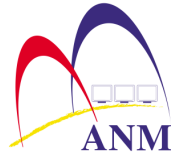
Polisi Keselamatan ICT JANM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Polisi ini hendaklah dibaca bersama dokumen-dokumen mengenai standard, garis panduan, prosedur dan langkah-langkah keselamatan ICT JANM yang akan dikeluarkan dari masa ke semasa.



## 1.7 Maklumat lanjut

Sebarang kemusykilan atau pertanyaan berkaitan Polisi Keselamatan ICT JANM ini, sila hubungi Unit Keselamatan SPICT, Bahagian Pengurusan Teknologi Maklumat.

Emel : [keselamatan@anm.gov.my](mailto:keselamatan@anm.gov.my)  
Talian/Meja Bantuan : 03-8882 1307  
Faksimili : 03-8882 1049



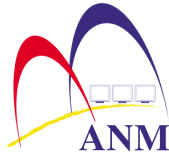
## **BAHAGIAN 2.0: PENGURUSAN KESELAMATAN ICT**

### **2.1 Pengurusan Keselamatan ICT**

Satu rangka kerja pengurusan keselamatan ICT diwujudkan bagi memastikan keselamatan ICT dilaksanakan dengan lebih sistematik, lancar dan berkesan.

Ketua Jabatan adalah bertanggungjawab untuk:

- (a) Membaca, memahami dan mematuhi Polisi Keselamatan ICT JANM;
- (b) Mewujud dan mengetuai jawatankuasa pengurusan keselamatan ICT JANM;
- (c) Memastikan semua pengguna ICT memahami dan mematuhi Polisi Keselamatan ICT JANM;
- (d) Memastikan semua keperluan keselamatan ICT (sumber kewangan, kakitangan dan perlindungan keselamatan) adalah mencukupi;
- (e) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT Kerajaan; dan



- (f) Menandatangani “Surat Akuan Pematuhan” bagi mematuhi Polisi Keselamatan ICT JANM (rujuk **Lampiran B**).

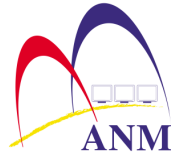
## **2.2 Struktur Organisasi Pengurusan Keselamatan ICT JANM**

Struktur formal Organisasi Pengurusan Keselamatan ICT JANM seperti di **Lampiran A** diwujudkan untuk mengurus keselamatan ICT. Ia terbahagi kepada Jawatankuasa Induk Pengurusan dan Jawatankuasa Pengurusan Keselamatan ICT.

### **2.2.1 Jawatankuasa Induk Pengurusan.**

Peranan dan tanggungjawab Jawatankuasa Induk Pengurusan dijelaskan seperti berikut:

- (a) Organisasi Pengurusan Keselamatan ICT JANM diketuai oleh Akauntan Negara Malaysia bagi memastikan keselamatan ICT dilaksanakan dengan aktif dan telus;
- (b) Menyelaras aktiviti pengurusan keselamatan ICT yang diketuai oleh Pengarah-pengarah Bahagian, Pengarah-pengarah Negeri dan Cawangan serta Ketua Akauntan JMS dari semua peringkat Bahagian, Negeri/Cawangan dan JMS berdasarkan peranan masing-masing;
- (c) Menjelaskan peranan dan tanggungjawab semua pengguna ICT JANM berhubung pengurusan keselamatan ICT JANM;



- (d) Mengenalpasti keperluan untuk pengurusan kerahsiaan maklumat, dilaksana dan dikaji secara berkala;
- (e) Memastikan jalinan perhubungan/komunikasi dengan pihak yang relevan dipelihara; dan
- (f) Memastikan kajian semula ke atas keselamatan maklumat dijalankan mengikut peraturan yang ditetapkan.

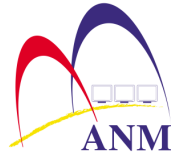
### **2.2.2 Jawatankuasa Pengurusan Keselamatan ICT**

Peranan dan tanggungjawab ahli Jawatankuasa Pengurusan Keselamatan ICT dijelaskan seperti berikut:

- (a) Ketua Pegawai Maklumat (CIO) – Timbalan Akauntan Negara Malaysia (Korporat)

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Polisi Keselamatan ICT JANM;
- ii. Membantu Akauntan Negara dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT JANM;
- iii. Menentukan keperluan keselamatan ICT JANM;
- iv. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT JANM; dan

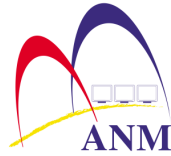


- v. Menandatangani “Surat Akuan Pematuhan” bagi mematuhi Polisi Keselamatan ICT JANM (**Lampiran B**).

(b) Pegawai Keselamatan ICT (ICTSO)

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Polisi Keselamatan ICT JANM;
- ii. Mengurus keseluruhan program-program keselamatan ICT JANM;
- iii. Menguatkuasakan Polisi Keselamatan ICT JANM;
- iv. Memberi penerangan dan pendedahan berkenaan Polisi Keselamatan ICT JANM kepada semua pengguna;
- v. Mewujudkan garis panduan dan prosedur selaras dengan keperluan Polisi Keselamatan ICT JANM;
- vi. Melaksanakan pengurusan risiko;
- vii. Melaksanakan pengauditan, mengkaji semula, merumus tindak balas berdasarkan hasil penemuan dan menyediakan laporan mengenainya;

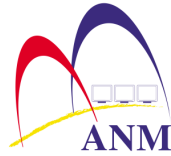


- viii. Memberi amaran kepada bahagian/Pejabat Perakaunan terhadap kemungkinan berlakunya ancaman keselamatan ICT seperti virus dan penggadam serta memberi khidmat nasihat dan bantuan teknikal bagi menyediakan langkah-langkah perlindungan yang bersesuaian;
- ix. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT Kementerian Kewangan dan GCERT MAMPU serta memaklukkannya kepada Akauntan Negara, CIO, Pengurus ICT berkenaan dan Pengarah BPTM;
- x. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;
- xi. Memberi perakuan tindakan tatatertib ke atas pengguna yang melanggar Polisi Keselamatan ICT JANM;
- xii. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan
- xiii. Menandatangani “Surat Akuan Pematuhan” bagi mematuhi Polisi Keselamatan ICT JANM (**Lampiran B**).

(c) Pengurus ICT

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Polisi Keselamatan ICT JANM;

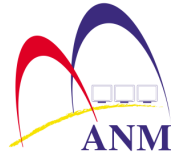


- ii. Memastikan kajian semula dan pelaksanaan kawalan keselamatan ICT selaras dengan keperluan Jabatan;
- iii. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO untuk tindakan;
- iv. Memastikan penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Jabatan dilaksanakan;
- v. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai Pentadbir Sistem ICT yang berhenti, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas; dan
- vi. Menandatangani “Surat Akuan Pematuhan” pematuhan Polisi Keselamatan ICT JANM (**Lampiran B**).

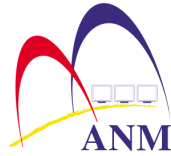
(d) Pentadbir Sistem ICT

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Polisi Keselamatan ICT;
- ii. Menjaga kerahsiaan kata laluan;
- iii. Menjaga kerahsiaan konfigurasi aset ICT;



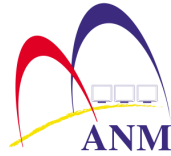
- iv. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai semua pengguna ICT JANM yang digantung kerja, berhenti, bersara, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas;
- v. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna luar dan pihak ketiga yang berhenti atau tamat projek;
- vi. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan;
- vii. Memantau aktiviti capaian harian pengguna;
- viii. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran; membatalkan atau memberhentikanannya dengan serta merta; dan memaklumkan kepada Pengurus ICT untuk tindakan selanjutnya;
- ix. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala;
- x. Menyimpan dan menganalisis rekod *audit trail*; dan
- xi. Menandatangani “Surat Akuan Pematuhan” bagi mematuhi Polisi Keselamatan ICT JANM (**Lampiran B**).



(e) Pengguna ICT JANM

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Polisi Keselamatan ICT JANM;
- ii. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;
- iii. Menjaga kerahsiaan maklumat JANM yang meliputi maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;
- iv. Menjaga kerahsiaan kata laluan;
- v. Memastikan maklumat berkaitan adalah tepat dan lengkap dari masa ke semasa;
- vi. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum;
- vii. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan
- viii. Menandatangani “Surat Akuan Pematuhan” bagi mematuhi Polisi Keselamatan ICT JANM (**Lampiran B**).



## 2.3 Agensi Luar

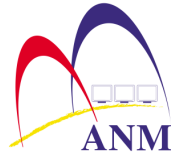
Peranan dan tanggungjawab Agensi Luar yang mencapai sistem JANM adalah seperti berikut:

- (a) Membaca, mematuhi dan memahami Polisi Keselamatan ICT JANM;
- (b) Memastikan data dan maklumat yang hendak disalurkan ke sistem JANM adalah sah dan *encrypted* berdasarkan persetujuan kedua-dua belah pihak;
- (c) Tidak menyalahgunakan data yang disalurkan oleh sistem JANM;
- (d) Memastikan tahap keselamatan data yang bersesuaian ke atas data yang disalurkan oleh sistem JANM; dan
- (e) Melaporkan kepada Meja Bantuan dengan serta merta sekiranya berlaku sebarang pelanggaran polisi keselamatan JANM.

### 2.3.1 Jabatan Audit Negara (Sistem Perakaunan)

Peranan dan tanggungjawab Jabatan Audit Negara yang melakukan pengauditan ke atas sistem perakaunan adalah seperti berikut:

- (a) Membaca, mematuhi dan memahami Polisi Keselamatan ICT JANM;
- (b) Tidak menyalahgunakan data yang disalurkan oleh sistem JANM;

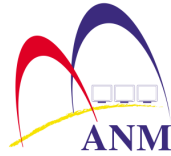


- (c) Memastikan tahap keselamatan data yang bersesuaian ke atas data yang disalurkan oleh sistem JANM; dan
- (d) Melaporkan kepada Meja Bantuan dengan serta merta sekiranya berlaku sebarang pelanggaran Polisi Keselamatan ICT JANM.

## **2.4 Pihak Luar**

Pengurus ICT atas nasihat ICTSO hendaklah memastikan penggunaan aset ICT oleh pihak luar/asing adalah dikawal seperti berikut:

- (a) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian ke atas aset ICT;
- (b) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan aset ICT;
- (c) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai.
  - i. Rangka Dasar Keselamatan ICT Kerajaan;
  - ii. Tapisan Keselamatan;
  - iii. Perakuan Akta Rahsia Rasmi 1972; dan
  - iv. Hak Harta Intelekt;



## **BAHAGIAN 3.0 : PENGURUSAN PENILAIAN RISIKO DAN INSIDEN**

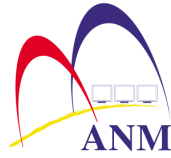
### **3.1 Pengurusan Penilaian Risiko Keselamatan ICT**

Penilaian risiko keselamatan aset ICT bertujuan membolehkan Jabatan mengukur, menyenarai kemungkinan risiko, menganalisis tahap risiko aset ICT dan seterusnya mengambil tindakan untuk merancang dan mengawal risiko.

#### **3.1.1 Tanggungjawab Melaksanakan Penilaian Risiko Keselamatan ICT**

Ketua Jabatan adalah bertanggungjawab untuk:

- (a) Memastikan penilaian risiko keselamatan ICT dilaksanakan secara berkala dan berterusan sekurang-kurangnya setahun sekali. Keperluan melaksanakan penilaian risiko bergantung kepada perubahan ke atas persekitaran Jabatan.
- (b) Mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.
- (c) Melaksanakan penilaian risiko mengikut peraturan atau prosedur yang ditetapkan oleh JANM dan Kerajaan dari semasa ke semasa.



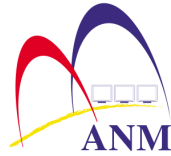
### **3.1.2 Skop Penilaian Risiko**

Skop penilaian risiko keselamatan ICT ke atas sistem maklumat di Jabatan termasuklah:

- (a) Aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur yang dikendalikan oleh Jabatan; dan
- (b) Premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

### **3.1.3 Analisa Risiko**

ICTSO JANM perlu melaksanakan analisa risiko dari semasa ke semasa ke atas aset ICT jabatan bertujuan untuk memastikan ancaman, kerentanan dan risiko keselamatan ICT di Jabatan berada di tahap yang paling minimum.



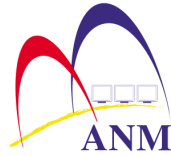
### **3.1.4 Penentuan Tindakan Pengendalian Risiko**

Untuk mengenal pasti tindakan yang wajar diambil bagi menghadapi kemungkinan risiko terjadi termasuklah seperti berikut :

- (a) mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
- (b) menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan Jabatan;
- (c) mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
- (d) memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

### **3.1.5 Kawalan Risiko**

Pengurusan kawalan risiko keselamatan ICT di JANM perlu dipantau oleh Pengurus ICT secara berterusan dan prosedur kawalan adalah mengikut penentuan tahap risiko yang telah ditetapkan bagi memastikan risiko dapat dikawal dengan baik.



### **3.2 Pengurusan Pengendalian Insiden Keselamatan ICT**

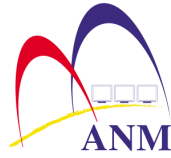
Semua insiden keselamatan ICT yang berlaku di Pejabat Perakaunan dan Bahagian-bahagian JANM mestilah dilaporkan dengan serta-merta dan dikendalikan mengikut peraturan atau prosedur pengurusan pengendalian insiden keselamatan ICT JANM dan Kerajaan yang ditetapkan.

Pengurus ICT adalah bertanggungjawab untuk memastikan arahan pengurusan pengendalian insiden keselamatan ICT di bawah kawalan masing-masing dipatuhi.

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.

#### **3.2.1 Insiden Keselamatan ICT**

Insiden keselamatan ICT bermaksud musibah (adverse event) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut seperti:



**a) Perlanggaran Dasar (Violation of Policy)**

Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar Dasar.

**b) Penghalangan Penyampaian Perkhidmatan (Denial of Service)**

Ancaman ke atas keselamatan sistem komputer di mana perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal.

**c) Pencerobohan (Intrusion)**

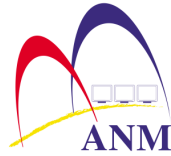
Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak.

**d) Pemalsuan**

Pemalsuan dan penyemaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat dan penipuan.

**e) Kehilangan Fizikal**

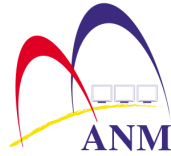
Kehilangan yang disebabkan oleh gangguan elektrik, kehilangan komunikasi data, kebocoran air, kebakaran, banjir, ancaman bom dan rusuhan atau mogok yang akan mengganggu perkhidmatan.



### **3.2.2 Mekanisme Pelaporan Insiden**

Semua insiden keselamatan ICT yang berlaku mesti dilaporkan serta merta kepada ICTSO untuk tindakan pengendalian insiden keselamatan ICT Kerajaan mengikut tahap ancaman yang telah ditetapkan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan.

Sebarang kerentanan (vulnerability) yang diperhatikan atau disyaki terdapat dalam perkhidmatan dan sistem maklumat Jabatan hendaklah dilaporkan dengan segera kepada ICTSO.



## **BAHAGIAN 4.0 : PENGURUSAN KESELAMATAN SUMBER**

### **4.1 Pengurusan Keselamatan Aset**

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

#### **4.1.1 Tanggungjawab Ke Atas Aset**

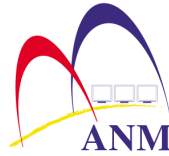
Memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.

### **4.2 Pengurusan Data Dan Maklumat**

Memastikan keselamatan serta integriti data dan maklumat yang diselenggara / diuruskan oleh JANM.

#### **4.2.1 Keselamatan Data**

Data yang sensitif perlu dilindungi daripada sebarang pendedahan, dimanipulasi, capaian dan ekstrak tanpa kebenaran serta semua bentuk kemusnahan. Semua capaian, ekstrak dan pelupusan ke atas data perlu mendapat kebenaran dari pihak yang diberi kuasa.



#### **4.2.2 Keselamatan Maklumat**

Memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan tahap kerahsiaan dan tahap kritikal kepada Kerajaan.

#### **4.3 Pengurusan Keselamatan Sumber Manusia**

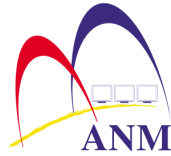
Peranan dan tanggungjawab pengguna ICT JANM hendaklah dinyatakan dengan jelas dan didokumenkan dengan sempurna. Polisi Keselamatan ICT adalah merangkumi pengguna ICT JANM sebelum memulakan tugas, semasa bertugas dan sebelum tamat bertugas.

#### **4.4 Pengurusan Keselamatan Premis, Peralatan Dan Persekitaran**

Premis dan peralatan memproses maklumat yang kritikal dan sensitif hendaklah ditempatkan di kawasan yang selamat dan dilindungi dari sebarang ancaman fizikal dan persekitaran.

#### **4.5 Pengurusan Keselamatan Perisian**

Semua perisian sistem dan perisian aplikasi yang digunakan hendaklah terdiri daripada perisian yang tulen dan sah. Perlindungan yang mampan dan bersesuaian hendaklah diwujudkan bagi menjauhi sebarang ancaman, kelemahan dan risiko kegagalan serta kehilangan.



#### **4.6 Pengurusan Keselamatan Operasi Dan Komunikasi**

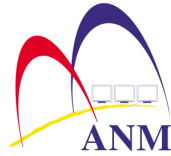
Dokumen pengurusan operasi dan komunikasi yang lengkap hendaklah disenggarakan dan mudah didapati.

#### **4.7 Pengurusan Keselamatan Kawalan Capaian**

Maklumat dan kemudahan-kemudahan pemprosesan maklumat hendaklah dilindungi dari pencerobohan dan penyebaran maklumat yang tidak sah.

#### **4.8 Pengurusan Keselamatan Didalam Perolehan, Pembangunan Dan Penyelenggaraan Sistem Maklumat**

Keperluan kawalan keselamatan hendaklah dikenalpasti dan diambilkira dalam pengurusan perolehan, pembangunan dan penambahbaikan serta penyelenggaraan sistem maklumat, dokumentasi dan perkhidmatan termasuk sistem pengoperasian, infrastruktur, sistem aplikasi serta perisian.



## **BAHAGIAN 5.0 : PENGURUSAN KESINAMBUNGAN PERKHIDMATAN**

### **5.1 Pengurusan Kesinambungan Perkhidmatan**

Pengurusan kesinambungan perkhidmatan JANM hendaklah mematuhi Rancangan Pengurusan Kesinambungan Perkhidmatan JANM.

## **BAHAGIAN 6.0 : PEMATUHAN**

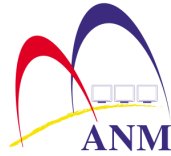
### **6.1 Pematuhan Keperluan Perundangan**

Polisi Keselamatan ICT disediakan selari dengan peruntukan-peruntukan perundangan dan peraturan semasa Kerajaan Malaysia yang berkuatkuasa.

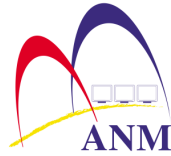
### **6.2 Keperluan Perundangan**

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

- (a) Pekeliling Am Bil. 3 tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan
- (b) Pekeliling Am Bil.1 Tahun 2001 –Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)



- (c) Pekeliling Kemajuan Perkhidmatan Awam Bil 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.
- (d) Arahan Keselamatan
- (e) Akta Rahsia Rasmi 1972
- (f) Akta Kawasan Larangan dan Tempat Larangan 1959
- (g) *Computer Crime Act 1997*
- (h) *Digital Signature Act 1997*
- (i) *Communications and Multimedia Act 1998*
- (j) *Malaysian Communications and Multimedia Commission act 1998*
- (k) *Malaysian Public Sector Management of Information and Communication Technology Security Handbook (MyMIS).*
- (l) Undang-Undang Malaysia Akta 680 (Akta Aktiviti Kerajaan Elektronik 2007)



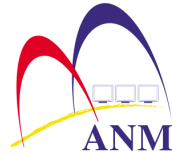
## **6.3 Tanggungjawab**

### **6.3.1 Tanggungjawab Pengguna ICT**

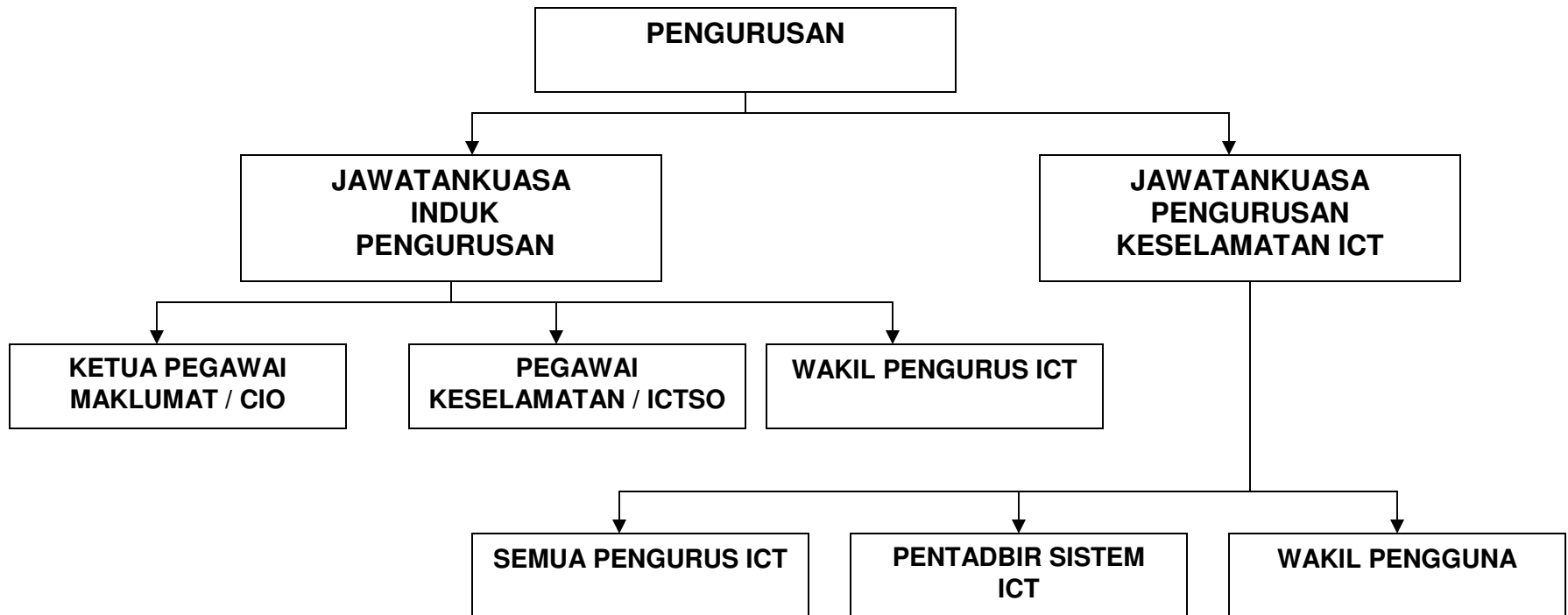
Pengguna ICT adalah bertanggungjawab mematuhi polisi keselamatan ICT JANM dan tindakan boleh diambil sekiranya didapati gagal mematuhi mana-mana peruntukan dibawah polisi tersebut.

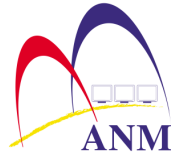
### **6.3.2 Tanggungjawab Ketua Jabatan, Pegawai Keselamatan ICT, Pengurus ICT dan Pentadbir Sistem.**

Ketua Jabatan, Pegawai Keselamatan ICT, Pengurus ICT dan Pentadbir Sistem adalah bertanggungjawab melaksanakan polisi keselamatan ICT JANM dan tindakan boleh diambil sekiranya didapati gagal melaksanakan mana-mana peruntukan dibawah polisi tersebut.



## STRUKTUR ORGANISASI PENGURUSAN KESELAMATAN ICT JANM





**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 Polisis 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 : .....